UNIWERSYTET W BIAŁYMSTOKU
Wydział Prawa
Zakład Prawa Międzynarodowego Publicznego

CYBERPRZESTRZEŃ A PRAWO MIĘDZYNARODOWE
STATUS QUO I PERSPEKTYWY

mgr Joanna Worona

Rozprawa doktorska
przygotowana pod kierunkiem naukowym
dr. hab. Macieja Perkowskiego, prof. UwB

Białystok 2017

Spis treści

Wykaz skrótów

A2B	— administracja z przedsiębiorcą (ang. *Administration to Business)*
ACTA	— Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi (ang. *Anti-Counterfeiting Trade Agreement*)
ARPA	— Agencja Zaawansowanych Projektów Badawczych (ang. *Advanced Research Projects Agency*)
ARPANET	— Sieć Agencji Zaawansowanych Projektów Badawczych (ang. *The Advanced Research Projects Agency Network*)
B2B	— przedsiębiorca z przedsiębiorcą (ang. *Business to Business*)
B2E	— przedsiębiorca z pracownikiem (ang. *Business to Employee*)
BGH	— Federalny Trynunał Sprawiedliwości Niemiec (niem. *Bundesgerichtshof*)
BTA	— Podstawowe Porozumienie Telekomunikacyjne (ang. *Basic Telecommunication Agreement)*
C2B	— konsument z przedsiębiorcą (ang. *Consumer to Business*)
C2C	— konsument z konsumentem (ang. *Consumer to Consumer*)
CBMD	— Urząd NATO do spraw Zarządzania Cyberobroną (ang. *The Cyber Defence Management Board*)
CC	— Creative Commons
CCD COE	— Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi (ang. *Cooperative Cyber Defence Centre of Excellence*)
CERT	— Zespoły Reagowania na Incydenty Komputerowe (ang. *Computer Emergency Response Team*)
CIGF	— Forum Zarządzania Internetem Brytyjskiej Wspólnoty Narodów (ang. *Commonwealth Intenet Governance Forum*)
CSNET	— Naukowa Sieć Komputerowa (ang. *Computer Science Network*)

DARPA — Agencja Zaawansowanych Projektów Badawczych do spraw Obrony (ang. *Defence Advanced Research Project Agency*)

DCA — Agencja Komunikacji Obronnej (ang. *Defence Communications Agency*)

DDoS — rozproszona odmowa usługi (ang. *Distributed Denial of Service*)

DDSOC — Strategia Działania w Cyberprzestrzeni Departamentu Obrony Stanów Zjednoczonych Ameryki (ang. *Department of Defense Strategy for Operating in Cyberspace*)

DNS — System Nazw Domenowych (ang. *Domain Name System*)

DoS — odmowa usługi (ang. *Denial of Service*)

DRDoS — rozproszona odwrócona odmowa usługi (ang. *Distributed Reflected Denial of Service*)

EC3 — Europejskie Centrum do spraw Walki z Cyberprzestępczością (ang. *European Cybercrime Centre*)

EDL CU — Estońska Liga Cyberobrony (ang. *Estonian Defence League's Cyber Unit*)

EKPC — Europejska Konwencji o Ochronie Praw Człowieka

ENISA — Europejska Agencja Bezpieczeństwa Sieci i Informacji (ang. *European Network and Information Security Agency*)

ETPCz — Eurpejski Trybunał Praw Człowieka

ETS — Europejski Trybunał Sprawiedliwości

GCA — Globalna Agenda Cyberbezpieczeństwa (ang. *Global Cybersecurity Agenda*)

GIC — Światowa Rada ds. Internetu (ang. *Global Internet Council*)

GIGF — Światowe Forum ds. Zarządzania Internetem (ang. *Global Internet Governance Forum*)

GIPC — Światowa Rada Polityki Internetu (ang. *The Global Internet Policy Council*)

HLEG — Grupa Ekspertów Wysokiego Poziomu (ang. *High -Level Expert Group*)

IaS — infrastruktura jako usługa (ang. *Infrastructure as a Service)*

ICANN — Internetowa Korporacja ds. Nadanych Nazw i Numerów (ang. *The Internet Corporation for Assigned Names and Numbers*)

ICCP — Komitet do spraw Informacji, Informatyki i Polityki Komunikacyjnej (ang. *Commitee for Information, Computer and Communications Policy)*

ICT — Technologie informacyjne i komunikacyjne (ang. *Information and Communication Technologies*)

IGCI — Globalny Zespół Innowacji Interpolu (ang. *Interpol Global Complex for Innovation*)

IGF — Forum Zarządzania Internetem (ang. *Internet Governance Forum*)

IIC — Międzynarodowa Rada do spraw Internetu (ang. *International Internet Council*)

IMPACT — Międzynarodowe Wielostronne Partnerstwo Przeciwko Zagrożeniom Internetowym (ang. *International Multilateral Partnership Against Cyber Threats*)

INWG — Międzynarodowa Grupa Robocza do spraw Sieci (ang. *International Network Working Group*)

IPC3 — Centrum Koordynacji przeciwko Przestępstwom Własności Intelektualnej (ang. *Intellectual Property Crime Coordination Centre*)

ISIS — Państwo Islamskie (ang. *Islamic State of Iraq and Syria*)

ISS — Międzynarodowa Stacja Komiczna (ang. *International Space Station*)

IT — technologia informacyjna (ang. *Information Technology*)

ITA — Porozumienie o Technologiach Informacyjnych (ang. *Information Technology Agreement)*

ITU — Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union*)

J-CAT — EU Joint Cybercrime Action Taskforce

k.c. — kodeks cywilny

k.k.- — kodeks karny

LAN — sieć lokalna (ang. *Local Area Networks*)

MAN — sieć miejska (ang. *Metropolitan Area Networks*)

MILNET — sieć wojskowa (ang. *Millitary Network*)

MIT — Massachusetts Institute of Technology

MPPOiP — Międzynarodowy Pakt Praw Obywatelskich i Politycznych

MŚP — Małe i Średnie Przedsiębiorstwa

MTKJ — Międzynarodowy Trybunał Karnym dla byłej Jugosławii

MTS — Międzynarodowy Trybunał Sprawiedliwości

NASK — Naukowa i Akademicka Sieć Komputerowa

NATO — Sojusz Północnoatlantycki (ang. *North Atlantic Treaty Organization*)

NIK — Najwyższa Izba Kontroli

NSF — Narodowa Fundacja Nauki (ang. *The National Science Foundation*)

NSFNET — Krajowa Sieć Fundacji Nauki (ang. The *National Science Foundation Network*)

NWG — Sieciowa Grupa Robocza (ang. *Network Working Group*)

OECD — Organizacja Współpracy Gospodarczej i Rozwoju (ang. *Organisation for Economic Cooperation and Development*)

ONZ — Organizacja Narodów Zjednoczonych

P2P — usługi *peer - to - peer*

PaS — platforma jako usługa (ang. *Platform as a Service)*

PE — Parlament Europejski

PRNET — sieć radiowa

RE — Rada Europy

SaS — oprogramowanie jako usługa (ang. *Software as a Service)*

SATNET — sieć satelitarna

TCP/IP — protokół komunikacyjny (ang. *Transmission Control Protocol/ Internet Protocol*)

T-CY — Komitet Konwencji o cyberprzestępczości (ang. *Cybercrime Convention Committee*)

TDS — Sektor Rozwoju Telekomunikacji (ang. *Telecommunication Development Sector*)

TS UE — Trybunał Sprawiedliwości Unii Europejskiej

UE — Unia Europejska

UNCITRAL — Komisja Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego (ang. *United Nations Commission on International Trade Law*)

UNCTAD — Konferencja Narodów Zjednoczonych ds. Handlu i Rozwoju (ang. *United Nations Conference on Trade and Development*)

UNESCO — Organizacja Narodów Zjednoczonych do spraw Oświaty, Nauki i Kultury (ang. *United Nations Educational, Scientific and Cultural Organization*)

UNODC — Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (ang. *United Nations Office on Drugs and Crime*)

WHOA — Ogranizacja ds. Walki z Przemocą Cyfrową (ang. *Working to Halt Online Abuse*)

WGIG — Grupa Robocza ds. Zarządzania Internetem (ang. *Working Group on Internet Governance*)

WIPO — Światowa Organizacja Własności Intelektualnej (ang. *World Intellectual Property Organization*)

WSIS — Światowy Szczyt Społeczeństwa Informacyjnego (ang. *The World Summit on the Information Society)*

WPPT — Traktat WIPO o artystycznych wykonaniach i fonogramach (ang. *WIPO Performances and Phonograms Treaty*)

WTC	— Traktat WIPO o prawie autorskim (ang. *WIPO Copyright Treaty)*
WTO	— Światowa Organizacja Handlu (ang. *World Trade Organisation*)
WWW	— ogólnoświatowa sieć (ang. *World Wide Web*)
ZO ONZ	— Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych

Wstęp

Cyberprzestrzeń, nazywana również Internetem, przestrzenią cyfrową lub wirtualną, jest swoistym medium, które bez wątpienia zrewolucjonizowało współczesny świat. Mimo, że geneza cyberprzestrzeni sięga lat sześćdziesiątych XX wieku, to momentem przełomowym dla globalnej sieci były lata dziewięćdziesiąte przypadające na okres komercjalizacji Internetu, ale przede wszystkim upowszechnienia komputerów osobistych. Liczba użytkowników Internetu wynosiła wówczas kilkanaście milionów[1]. Według danych witryny Internet World Stats w grudniu 2016 roku liczba internautów przekroczyła 3,6 miliarda[2]. Oznacza to, że aż 49,2% światowej populacji jest częścią globalnej wioski, położonej w nowej przestrzeni o wirtualnym, trangranicznym, aterytorialnym i ponadnarodowym charakterze. Jeszcze nigdy w historii naszego globu nie było możliwości tak łatwego, taniego i szybkiego przesyłania danych czy komunikowania się na odległość.

Intensywny rozwój systemów informacyjnych i telekomunikacyjnych w latach 1990 - 2015 sprawił, że cyberprzestrzeń stała się ważnym czynnikiem wspomagającym i stymulującym rozwój gospodarczy państw, w szczególności krajów wysoko rozwiniętych. Wysoki poziom komputeryzacji przyczynił się jednakże do wzrostu uzależnienia krajów od ich poprawnego i niezakłóconego działania. Ewolucja i postępująca ekspansja cyberprzestrzeni zdeterminowały nieznane dotąd zagrożenia takie, jak cyberprzestępczość czy cyberterroryzm. W państwie informacyjnym, którego wszelkie dziedziny życia oparte są na skoncentrowanych w systemach komputerowych źródłach informacji, zakłócenie ich funkcjonowania oznacza dezorganizację życia państwa i społeczeństwa. Konsekwentny i coraz silniejszy rozkwit koniunktury wirtualnej na przestrzeni ostatnich lat spowodował, że przestrzeń cyfrowa ma coraz silniejszy wpływ na takie dziedziny życia, jak produkcja, handel czy też edukacja i prawo.

Ogromna liczba użytkowników sieci oraz nieograniczony narodowo charakter Internetu powoduje, że stroną ulokowanego tu stosunku prawnego może być niemal co drugi mieszkaniec Ziemi. Ustawodawcy krajowi mimo podejmowanych prób nie są w stanie nadążyć za szybkimi zmianami technologicznymi, brakuje jednolitych reguł postępowania

[1] K.B. Wydro, *Internet dziś – stan i wykorzystanie*, [w:], A. Szewczyk, E. Krok (red.), *Fenomen Internetu*, t. 1, Szczecin 2008, s. 51.
[2] Dane ze strony Internetowej Internet World Stats http://www.internetworldstats.com/stats.htm [01.03.2017].

oraz unormowań podstawowych kwestii takich, jak jurysdykcja czy sposób zarządzania cyberprzestrzenią. Omawiane medium nie ma granic, fizycznego podziału, narodowości ani jednego prawa właściwego, dlatego też stanowi wyzwanie dla teoretyków i praktyków prawa. Szczególne znaczenie w procesie regulacji statusu cyberprzestrzeni mają prace organizacji międzynarodowych, które podejmują działania w kierunku harmonizacji przepisów dotyczących działalności człowieka w przestrzeni wirtualnej. Podjęta problematyka, mimo globalnego wymiaru, ma bezpośrednie i praktyczne przełożenie na codzienną rzeczywistość milionów ludzi żyjących w różnych regionach świata. Powoduje to, że wybór tematu ma tu uzasadnienie zarówno obiektywne, jak i subiektywne. Przygotowana dysertacja ma charakter interdyscyplinarny, gdyż tylko takie podejście pozwoli na gruntowne zbadanie tematu. Omówione w rozprawie zagadnienia mogą stać się przyczynkiem do dalszej dyskusji o roli prawa międzynarodowego w cyberprzestrzeni.

Celem niniejszej rozprawy doktorskiej jest weryfikacja aktualnego statusu cyberprzestrzeni w kierunku jej optymalnego uregulowania z wykorzystaniem prawa międzynarodowego. Zostanie również dokonana identyfikacja obszarów, w których istnieje konieczność unifikacji przepisów odnoszących się do cyberprzestrzeni.

Głównym problemem badawczym jest ustalenie, czy prawo międzynarodowe może udoskonalić rekonstrukcyjnie aktualny status cyberprzestrzeni.

Punkt wyjścia dla prowadzonych rozważań stanowią pytania szczegółowe sformułowane w następujący sposób:

1. Czy cyberprzestrzeń, jako przedmiot regulacji, można ująć definicyjnie?
2. Jakie reguły jurysdykcyjne są stosowane w stosunku do cyberprzestrzeni?
3. Czy i w jaki sposób oraz w jakim zakresie państwa, organizacje międzynarodowe i inne podmioty podejmują próby regulacji cyberprzestrzeni?
4. Czy prawo międzynarodowe umożliwia regulację cyberprzestrzeni?
5. W jakich płaszczyznach prawo międzynarodowe może mieć zastosowanie w stosunku do cyberprzestrzeni?
6. W jakich obszarach prawo międzynarodowe przyczynia się do unifikacji problematycznych kwestii związanych z cyberprzestrzenią?
7. Jakie są najbardziej adekwatne postulaty i propozycje rozwiązań prawnych regulacji cyberprzestrzeni?

Na tej podstawie została sformułowana teza badawcza, wedle której prawo międzynarodowe jest najbardziej predysponowane do racjonalnego i użytecznego modelowania oraz harmonizacji regulacji krajowych cyberprzestrzeni.

Biorąc pod uwagę, że rozprawa doktorska dotyczy przedmiotowo zwłaszcza prawa międzynarodowego publicznego, zastosowano w niej następujące metody badawcze:

1. Metodę dogmatyczną - w rozprawie dokonano analizy wielostronnych umów międzynarodowych, aktów prawnych uniwersalnych i regionalnych organizacji międzynarodowych oraz dokumentów tworzonych przez podmioty zajmujące się problematycznymi zagadnieniami występującymi w cyberprzestrzeni, jak na przykład cyberprzestępczość. Jej zastosowanie pozwoliło na określenie norm prawnych stosowanych w przestrzeni wirtualnej oraz identyfikację przedmiotowych obszarów, w których istnieje potrzeba regulacji i harmonizacji.
2. Metodę prawnoporównawczą - analizie zostały poddane normy prawne wybranych państw odnoszące się do cyberprzestrzeni. Pozwoliła ona poznać różnorodność obowiązujących regulacji oraz wyciągnąć wnioski w zakresie prawidłowości przyjętych rozwiązań.
3. Metodę analizy orzecznictwa i doktryny – pozwoliła ona na porównanie judykatury i określenie, w jaki sposób kształtuje się praktyka sądowa w wybranych państwach oraz jak cyberprzestrzeń winna być regulowana według znawców prawa.
4. Metodę historyczną – jej wykorzystanie było konieczne do przedstawienia genezy i ewolucji sieci pierwotnie wojskowej w globalną przestrzeń wirtualną. Pozwoliła przedstawić pierwsze dokumenty poruszające opisywane zjawisko, zrozumieć obecną formę cyberprzestrzeni oraz przewidzieć możliwe tendencje rozwoju.
5. Metodę analizy statystycznej - w rozprawie wykorzystano między innymi raporty instytucji zajmujących się monitorowaniem incydentów w cyberprzestrzeni (CERT, Norton) oraz strony internetowe, na których systematycznie są publikowane informacje o stanie ilościowym Internetu (http://www.internetworldstats.com/). Pozwoliła poznać dynamikę wzrostu liczby użytkowników cyberprzestrzeni, ilościowy rozwój przestrzeni wirtualnej, rodzaje i liczbę naruszeń występujących w sieci czy też skalę problemów takich, jak *cyberstalking*.

Przygotowana praca jest obszerna, dlatego została podzielona na trzy części. Część pierwsza *Cyberprzestrzeń a jurysdykcja* składa się z dwóch rozdziałów. W pierwszym

zatytułowanym *Cyberprzestrzeń - pojęcie i geneza* omówiono pojęcie, genezę i ewolucję historyczną cyberprzestrzeni oraz etapy rozwoju społeczeństwa informacyjnego. Opisano także kluczowe koncepcje i poglądy doktryny krajowej oraz zagranicznej na temat cyberprzestrzeni. Ukazano statystyki odnoszące się do liczby użytkowników sieci oraz etapów rozwoju sieci wirtualnej. Zasygnalizowano również zagrożenia związane z funkcjonowaniem cyberprzestrzeni.

W rozdziale drugim *Jurysdykcja państwowa a cyberprzestrzeń* ujęto rozważania wskazujące prawo właściwe do zobowiązań umownych zawieranych za pośrednictwem Internetu, deliktów elektronicznych oraz jurysdykcji w sprawach cywilnych i handlowych. Wskazano międzynarodowe oraz regionalne akty prawne, które mogą mieć zastosowanie w stosunku do umów zawieranych w przestrzeni cyfrowej. Opisano również rozwiązania prawne wybranych krajów oraz orzecznictwo poruszające kwestię prawa właściwego w stosunkach cywilno-gospodarczych w przestrzeni wirtualnej. Przedstawiono zagadnienie jurysdykcji karnej w odniesieniu do czynów przestępczych popełnionych w cyberprzestrzeni. Ponadto, ukazano model władztwa jurysdykcyjnego przyjęty w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. oraz w Decyzji ramowej Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów. Szczegółowo omówiono również kwestię jurysdykcji karnej w cyberprzestrzeni, w ujęciu prawnoporównawczym wybranych państw. Podjęto też rozważania na temat teoretycznego ujęcia zasad jurysdykcji oraz możliwości ich zastosowania w cyberprzestrzeni.

Część druga rozprawy *Prawnomiędzynarodowy wymiar cyberprzestrzeni - status quo* także składa się z dwóch rozdziałów. Rozdział, trzeci zatytułowany *Identyfikacja regulacji prawnych cyberprzestrzeni z perspektywy międzynarodowej* poświęcono wnikliwej analizie norm prawnych dotyczących cyberprzestrzeni ustanowionych przez powszechne i regionalne organizacje międzynarodowe, w tym międzynarodowe organy ścigania oraz inne instytucje zainteresowane regulacją statusu przestrzeni wirtualnej. Ponadto, ukazano, jakie regulacje prawne w odniesieniu do cyberprzestrzeni zostały przyjęte w cybermocarstwach, krajach determinowanych postępem technologicznym oraz państwach, które stały się ofiarami cyberataków. W czwartym rozdziale *Identyfikacja kluczowych zagadnień przedmiotowych prawnej regulacji cyberprzestrzeni* poruszono problem zwalczania cyberprzestępczości, obrotu gospodarczego, własności intelektualnej i innych obszarów, w których prawo międzynarodowe może mieć zastosowanie. Druga część rozprawy doktorskiej jest

najobszerniejsza, między innymi ze względu na złożoność przedstawionej problematyki. Brak jednej, uniwersalnej instytucji międzynarodowej regulującej działalność człowieka w cyberprzestrzeni powoduje fragmentację oraz rozproszenie przyjętych rozwiązań. Tym bardziej była potrzebna identyfikacja kluczowych zagadnień podlegających regulacji w przestrzeni cyfrowej.

Trzecią część rozprawy (konsekwentnie podzieloną na dwa rozdziały) zatytułowano *Koncepcja rekonstrukcji statusu prawnego cyberprzestrzeni (z wykorzystaniem prawa międzynarodowego)*. W rozdziale piątym *Identyfikacja obszarów regulacji prawnomiędzynarodowych możliwych do wykorzystania rekonstrukcyjnego wobec cyberprzestrzeni* opisano specyfikę prawa międzynarodowego oraz jego zastosowania w różnych przestrzeniach - państwowych oraz międzynarodowych. Ponadto, zidentyfikowano nowe obszary, wyłonione na skutek postępu technologicznego i ekspansji człowieka, w których prawo międzynarodowe podejmuje próbę regulacji. W rozdziale szóstym *Postulaty i propozycje rozwiązań dla cyberprzestrzeni,* przedstawiono postulaty i koncepcje zmian zarządzania i regulacji cyberprzestrzeni. W pierwszej kolejności zaprezentowano koncepcje samoregulacji przestrzeni. Następnie zaproponowano koncepcję nowego ładu cyberprzestrzeni w aspekcie podmiotowym, przedmiotowym oraz proceduralnym, a także przeprowadzono rekonstrukcję prawa cyberprzestrzeni oraz podjęto próbę jego definicji.

Niniejsza dysertacja nie wyczerpuje wszystkich aspektów działalności człowieka w cyberprzestrzeni w świetle prawa międzynarodowego, tworząc jedynie zarys problematyki, który (być może) będzie przyczynkiem do dalszych rozważań i dyskusji w doktrynie.

Problemy, które dotyczą cyberprzestrzeni, czyli cyberprzestępczość, cyberterroryzm, czy transgraniczne zawieranie umów internetowych coraz częściej są dyskutowane w doktrynie polskiej i zagranicznej. Cyberprzestrzeń stanowi wielkie wyzwanie dla prawa, nie tylko ze względu na swój transgraniczny, niematerialny charakter, ale również ze względu na fakt, że w przestrzeni tej zastosowanie znaleźć może niemal każda dziedzina prawa - prawo karne, cywilne, handlowe, prawo własności intelektualnej czy chociażby prawo bankowe. Bardzo liczne potencjalne możliwości powodują, że autorzy skupiają się zazwyczaj na jednej gałęzi prawa bądź jednym zagadnieniu przedmiotowym. Jedynie nieliczni autorzy podejmują próbę holistycznego opracowania naukowego poruszającego kwestie natury i zasad rządzących cyberprzestrzenią. Przygotowując tę rozprawę doktorską wykorzystano odpowiednie przedmiotowo monografie i artykuły zarówno w języku polskim autorstwa:

Joanny Kuleszy, Macieja Siwickiego, Piotra Sienkiewicza, Andrzeja Adamskiego, Janusza Barta i Ryszarda Markiewicza, jak i w języku angielskim na przykład: Aarona Schwabacha, Davida R. Johnsona, Davida G. Posta i Darrela G. Menthe.

Biorąc pod uwagę tematykę pracy, niezbędnych i oczywistych zasobów danych wykorzystanych w procesie twórczym dostarczył Internet. Autorka skorzystała ze stron internetowych organizacji międzynarodowych takich, jak Rada Europy, Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości czy NATO oraz oficjalnych stron międzynarodowych organów ścigania (INTERPOL, Europejskie Centrum do spraw Walki z Cyberprzestępczością). Nie mniej istotne okazały się zasoby cyberprzestrzeni w zakresie zdobywania dodatkowych informacji czy uzupełniania literatury naukowej, dostępnej również w zasobach *on-line.*

Nie rezygnując z rozwiązań tradycyjnych, autorka odbyła dwie kwerendy zagraniczne w celu zebrania podstawowej, międzynarodowej literatury przedmiotu. Pierwsza z nich została przeprowadzona w 2011 roku w Bibliotece Parlamentu Europejskiego oraz w Bibliotece Uniwersytetu w Antwerpii. W toku przygotowywania rozprawy doktorskiej zaistniała konieczność aktualizacji literatury zagranicznej, wobec czego drugą kwerendę zrealizowano w maju 2015 roku w *Peace Palace,* przy siedzibie Międzynarodowego Trybunału Sprawiedliwości w Hadze.

W trakcie przygotowań rozprawy doktorskiej nie mniej istotnym zasobem okazała się życzliwość i nieocenione wsparcie wielu osób, a w szczególności pracowników Wydziału Prawa Uniwersytetu w Białymstoku. W związku z tym wszystkim należą się serdeczne podziękowania za okazaną pomoc, rady i dobre słowa, bez których trudno byłoby niniejszą pracę zrealizować.

CZĘŚĆ I

CYBERPRZESTRZEŃ

A JURYSDYKCJA

Rozdział 1

Cyberprzestrzeń - pojęcie i geneza

W dwudziestym i dwudziestym pierwszym wieku nastąpiło zrewolucjonizowanie świata. Postęp medycyny, uprzemysłowienie, pierwsze loty samolotem, a następnie loty w kosmos spowodowały, że człowiek zaczął wkraczać w zupełnie nowe obszary, zyskując ogromy potencjał do dalszego rozwoju. Wynalezienie pionierskich, szybkich i ogólnodostępnych technik komunikacji doprowadziło do wykształcenia się globalnej wioski, w której informacja ma najwyższą wartość. Internet dał światu zupełnie nowe możliwości - powstanie nowych rynków zbytu, ułatwionej i szybkiej wymiany danych, dostępu do edukacji, pracy i rozrywki. Jest to wynalazek na miarę druku Gutenberga, który przyczynił się do szerszego dostępu do książek, a tym samym wiedzy i informacji. Słowo drukowane upowszechniło książki, dało dostęp do wiedzy, która w tamtym okresie zarezerwowana była wyłącznie dla możnych i wysoko urodzonych. Cyberprzestrzeń jednak poszła krok dalej, umożliwiła swobodne wyrażanie poglądów, dzielenie się ideami, prezentowanie swoich dokonań bez marketingowej cenzury wydawców, ścisłej kontroli rządów czy dyktatur. Obecnie ziemię zamieszkuje około 7,5 miliardów ludzi, a niemal połowa - 3,6 miliardów z nich ma dostęp do Internetu[3]. Zaledwie w ciągu kilkudziesięciu lat XX i XXI wieku wykształciła się przestrzeń, która połączyła połowę ludzkiej populacji w jednej, wirtualnej sieci. Wydaje się, że w historii globu nie było takiego fenomenu.

W niniejszym rozdziale zostanie zdefiniowany termin cyberprzestrzeń, następnie ukazana geneza i ewolucja powstania Internetu począwszy od jego zalążków w ramach sieci wojskowej przez komercjalizację i upowszechnienie aż do globalnego wykorzystania. Nieodłącznym elementem przestrzeni cyfrowej są jej użytkownicy. Powstanie cyberprzestrzeni doprowadziło do wykształcenia się społeczeństwa informacyjnego, w którym wiedza i informacja jest priorytetem. Przestrzeń cyfrowa stymulująco wpływa na rozwój gospodarki, szerszy dostęp do edukacji i wiedzy, lecz nie jest to obszar wolny od zagrożeń. Przeciwnie, cyberprzestrzeń jest wykorzystywana przez cyberprzestępców,

[3] Dane z witryny internetowej Internet World Stats: http://internetworldstats.com/stats.htm, [01.02.2017].

terrorystów, ale również przez państwa do realizacji swoich celów politycznych i wojskowych.

1.1 Pojęcie cyberprzestrzeni

Po raz pierwszy termin cyberprzestrzeń (ang. *cyberspace*) pojawił się w powieści *science fiction* Williama Gibsona *Neuromancer* (1984). Książka została osadzona w wyimaginowanej przestrzeni zbudowanej z procesów elektronicznej komunikacji[4]. William Gibson opisując ją, stwierdza, że: „Jest to cyberprzestrzeń, konsensualna, halucynacyjna, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność”[5].

Pojęcie cyberprzestrzeni nie ma jednej, ogólnie przyjętej i akceptowalnej definicji. Ze względu na swój dynamicznie zmieniający się, nieostry i niematerialny charakter prowadzi do trudności zarówno interpretacyjnych, jak i definicyjnych. Cyberprzestrzeń z psychologicznego punktu widzenia jest uznawana bardziej za stan umysłu niż fragment świata realnego. John P. Barlow twierdzi, że cyberprzestrzenią jest „każda przestrzeń, w której ludzie mogą gromadzić swoje umysły bez zabierania tam swoich ciał”[6]. Cyberprzestrzeń odnosi się do wirtualnej przestrzeni - świata komputerów, w którym pojawił się nowy wirtualny świat, połączony za pomocą globalnej sieci Internet. W tym znaczeniu cyberprzestrzeń jest „niematerialnym wymiarem rzeczywistości, bazującym na materialnej infrastrukturze sieci teleinformatycznych, w tym przede wszystkim sieci Internet”[7]. Ryszard Tadeusiewicz stoi zaś na stanowisku, iż słowo przestrzeń w terminie cyberprzestrzeń „ma konotacje semantyczne i emocjonalnie odwołującą się do ogromnego zasięgu i całkowitej

[4] K. Dobrzeniecki, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 18.
[5] P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni*, [w:] T. Jemioła, J. Kiesielnicki, K. Rajchel (red.), *Cyberterroryzm - nowe wyzwania XXI wieku*, Warszawa 2009, s 194.
[6] K. Dobrzeniecki, *Prawo …*, s. 18.
[7] Ibidem, s. 19.

swobody. Przestrzeń zachęca do wielokierunkowego przemieszczania się, do przezwyciężania barier, do inicjowania kontaktów interakcji niemożliwych w przypadku jej braku”[8].

Według koncepcji Pierre'a Levy cyberprzestrzeń to „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie”. W dyskursie humanistycznym stała się ona zatem synonimem Internetu. Dalej Levy wskazuje, iż cyberprzestrzeń ma charakter „plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzalny w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny. Uważam go za znamienną cechę cyberprzestrzeni. To nowe środowisko umożliwia współdziałanie i sprzęganie wszystkich narzędzi tworzenia informacji, rejestrowania, komunikacji i symulacji. Perspektywa powszechnej numeryzacji informacji i przekazów uczyni prawdopodobnie z cyberprzestrzeni główny kanał informacyjny i główny nośnik pamięciowy ludzkości, poczynając od pierwszych lat przyszłego stulecia”[9].

Znawcy tematu podkreślają wielowymiarowość cyberprzestrzeni, która „ma wymiar ludzki i techniczny. Do cech cyberprzestrzeni zalicza się: plastyczność, płynność, obliczalność, dokładność, powtarzalność, hipertekstowość, interaktywność, wizualność, kompatybilność, otwartość, nieograniczoność, wszechstronność, złożoność, sieciowość, przenikliwość, konwergentność, konsolidację, automatyzację i totalność. Cechy te przenoszone są na kształtowany pod jej wpływem porządek realprzestrzeni”[10]. Wymienione wyżej cechy można uzupełnić o dodatkowe pojęcia takie, jak zmienność, aterytorialność, ponadpaństwowość, szybkość przemian, niematerialność, niestabilność oraz innowacyjność.

Nie tylko teoretycy prawa coraz częściej próbują zmierzyć się z nową problematyką przestrzeni wirtualnej. W Polsce wydano dokument Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, w którym uznano, że cyberprzestrzenią jest: „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci

[8] R. Tadeusiewicz, *Wychowywanie dla cyberprzestrzeni jednym z warunków zapobiegania cyberuzależnieniom*, [w:] E. Mastalerz, K. Pytel, H. Noga (red.), *Cyberuzależnienia: przeciwdziałanie uzależnieniom od komputera i Internetu*, Kraków 2007, s. 23.
[9] P. Levy, *Drugi potop*, [w:] M. Hopfinger (red.) *Nowe media w komunikacji społecznej w XX wieku. Antologia*, Warszawa, 2002, s. 380.
[10] J. Janowski, *Cybernetyzacja prawa*, [w:] E. Galewska, S. Kotecka (red.), X-*lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego*, Warszawa 2012, s. 394.

telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami"[11]. W ustawie o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej z dnia 29 sierpnia 2002 r. za cyberprzestrzeń uznano z kolei przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, czyli współpracujące ze sobą urządzenia informatyczne i oprogramowanie wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[12].

Cyberprzestrzeni nie można utożsamiać z Internetem. Ma ona szerszy charakter, jest przestrzenią cyfrowej działalności człowieka, lecz w dużej mierze bazuje właśnie na sieci Internet. Joanna Kulesza za Internet uznaje „globalny system wymiany danych funkcjonujący w oparciu o wzajemnie połączone sieci lokalne, rozmieszczone w wielu fizycznych lokalizacjach, umożliwiający jednoczesną wielopłaczyznową interakcję użytkowników z całego świata"[13].

Karol Dobrzeniecki wyodrębnia dwa aspekty przestrzeni wirtualnej. Autor twierdzi, że na cyberprzestrzeń składają się: substrat technologiczny, czyli infrastruktura tworząca Internet oraz substrat społeczny, czyli użytkownicy Internetu – internauci[14]. Na substrat technologiczny składa się cała infrastruktura świata wirtualnego. Jego podstawowym ogniwem jest sieć komputerowa (ang. *network*), czyli zbiór komputerów i innych urządzeń połączonych ze sobą kanałami komunikacyjnymi, które umożliwiają wzajemne przesyłanie informacji, pomiędzy podłączonymi do sieci urządzeniami tak zwanymi „punktami sieci". Komputery posługują się specjalnym oprogramowaniem, dzięki któremu mogą ustalić, iż są częścią tej samej sieci. Tak skonstruowana sieć umożliwia łatwy i szybki dostęp do publikowanych danych oraz korzystania ze wspólnych zasobów informacji i informacji. Globalna pajęczyna (ang. *web*) komputerów i sieci komputerowych tworzy Internet[15].

Użytkownicy z dostępem do Internetu mogą pozyskiwać informacje i komunikować się między sobą na wiele sposobów. Niezwykle trudno jest podać precyzyjną kwalifikację

[11] Doktryna Cyberbezpieczeństwa Rzeczpospolitej polskiej 2015, wydana przez Biuro Bezpieczeństwa Narodowego dnia 22 stycznia 2015, s. 7.
[12] Dz.U. z 2002 r., Nr 156, poz. 1301.
[13] J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 57.
[14] K. Dobrzeniecki, *Prawo* ..., s. 21.
[15] Ibidem, s. 21-22.

rodzajów komunikacji ze względu na dużą dynamikę i ciągłą ich ewolucję. Karol Dobrzeniecki wyróżnia jednakże kilka podstawowych kategorii takich, jak: „komunikacja ściśle indywidualna (elektroniczny odpowiednik konwencjonalnej poczty), typ »odezwy« lub »słupa ogłoszeń« (jeden nadawca wielu odbiorców), komunikacja w czasie rzeczywistym, na podobieństwo rozmowy telefonicznej (na przykład *Internet Relay Chat*) oraz zdalne wyszukiwanie i pozyskiwanie informacji. Ostatnia z wymienionych metod komunikacji – *the World Wide Web,* jest najbardziej znaną i popularną usługą w Internecie, popularnie nazywaną siecią stron internetowych”[16]. Przeglądarki internetowe (ang. *web browsers*) umożliwiają korzystanie z zasobów Internetu – wymiany tekstów, plików, muzyki, animacji oraz filmów. Pliki te są zapisane w formie elektronicznej, na określonym nośniku w jednym miejscu, ale są obecne wirtualnie w każdym punkcie sieci, w którym zostaną one wywołane.

Cyberprzestrzeń nie ma jednolitego charakteru. Znawcy tematu wskazują słusznie, że: „w Internecie nie ma centralnego miejsca przechowywania danych, punktu kontroli, czy jednego kanału komunikacyjnego. Nie jest możliwe, z punktu widzenia aktualnego stanu techniki, żeby jeden podmiot kontrolował wszystkie informacje przesyłane przez Sieć. W efekcie Internet jest pierwszą w historii znaczącą globalną instytucją, która nie ma jednego ośrodka decyzyjnego. Zarządzenie nim przypomina system feudalnych władztw terytorialnych – każdy podmiot administruje własną (najczęściej stworzoną przez siebie) częścią tej struktury oraz pokrywa związane z tym wydatki. Zdecentralizowana struktura stanowienia i egzekwowania reguł postępowania jest jedną z najważniejszych cech charakterystycznych, z punktu widzenia prawnej analizy tego fenomenu.”[17] Brak jednolitej struktury, zdecentralizowany, aterytorialny charakter oraz ciągłe zmiany technologiczne powodują, że próby kodyfikacji przestrzeni wirtualnej na poziomie krajowym są co najmniej niewystarczające.

Drugim składnikiem cyberprzestrzeni, według Karola Dobrzenieckiego, jest substrat społeczny. Wskazuje on, że zmiany zachodzące w ostatnich dziesięcioleciach doprowadziły do powstania społeczeństwa informacyjnego (ang. *information society*) – społeczeństwa, gdzie najwyższym dobrem jest informacja[*]. Rewolucja informacyjna spowodowała powstanie zupełnie nowej struktury społecznej, w której ludzie skupiają się na produkcji, przetwarzaniu i dystrybuowaniu informacji, a nie dóbr materialnych. Jednym z warunków powstania

[16] K. Dobrzeniecki, *Prawo …*, s. 24.
[17] Ibidem, s. 25 (pisownia i zastosowanie interpunkcji za autorem).
*Więcej na ten temat w podrozdziale 1.3. *Etapy rozwoju społeczeństwa informacyjnego i zagrożenia z nim związane.*

społeczeństwa informacyjnego jest nowoczesna, rozbudowana sieć telekomunikacyjna, zapewniająca możliwość sprawnego gromadzenia i wymiany informacji. Technika cyfrowa przenika obecnie niemal do wszystkich dziedzin życia, zapewniając spełnienie jak najbardziej realnych potrzeb w świecie wirtualnym. Dotyczy to edukacji, kultury i rozrywki, możliwości załatwienia czynności urzędowych, telepracy czy też aktywizacji osób niepełnosprawnych.

Internet jest globalnym medium łączącym indywidualne osoby, instytucje i rządy na całym świecie. Dzięki łatwości i szybkości komunikowania jest miejscem, w którym ludzie o podobnych zainteresowaniach mogą tworzyć grupy i wymieniać poglądy. Uczestnicy tych grup nawiązują podobne więzi do tych, co członkowie społeczności w świecie materialnym. Nie będzie zbyt śmiałym twierdzenie, że „Internet stwarza nowe perspektywy dla organizacji społecznych, gospodarczych oraz dla subkultur. Mogą one powstawać i sprawnie działać nawet przy rozproszonej terytorialnie strukturze. Internet ułatwia formowanie się politycznych więzi niejako »w poprzek« tradycyjnych socjoekonomicznych barier, zwiększając możliwości partycypacji w życiu obywatelskim. Z drugiej strony, nowoczesne technologie informatyczne i telekomunikacyjne sprzyjają rozwojowi pozapaństwowych struktur politycznych, pozbawionych balastu biurokratycznej hierarchiczności. W perspektywie dalszego rozwoju cyberprzestrzeni mogą ulec osłabieniu więzy pomiędzy usytuowaniem geograficznym, a meritum spraw będących przedmiotem postępowań prawnych oraz instytucjami, które te sprawy załatwiają. Stopniowo wzrasta siła jednostki, słabnie natomiast przywiązanie do osadzonego na fundamencie terytorialnym państwa."[18] Część autorów (na przykład Józef Bednarek) uważa, że komunikacja w cyberprzestrzeni przybiera zupełnie nowy wymiar: „Rozwój technologii sieci komputerowych, w tym zwiększenie szybkości przesyłania informacji, oraz szerokie rozpowszechnianie usług sieciowych, głównie za sprawą Internetu, spowodowały, iż powszechne stało się projektowanie sieciowych serwisów informacyjnych i multimedialnych prezentacji z elementami trójwymiarowymi. Wirtualne światy, tworzące tak zwaną cyberprzestrzeń, stały się najbardziej rozwiniętą formą trójwymiarowości w Internecie. Odwiedzając wirtualne światy, stajemy się ich aktywną i integralną częścią. W wirtualnych światach chcemy być obecni poprzez swoje wirtualne reprezentacje. Naszymi reprezentantami stały się nazwy, rysunki, obrazy, ikony, aż w końcu mogliśmy się wcielić w trójwymiarowe obiekty, odgrywające aktywne role w wirtualnym świecie"[19]. Ciężko jest w chwili obecnej

[18] K. Dobrzeniecki, *Prawo …*, s. 28.
[19] J. Bednarek, A. Andrzejewska, *Cyberświat - możliwości i zagrożenia*, Warszawa 2009, s. 30 - 31.

przewidzieć, jak będzie wyglądała nasza rzeczywistość za pół wieku. Bez śladu wątpliwości można stwierdzić, iż cyberprzestrzeń będzie rozwijać się w ogromnym tempie, a coraz większa część naszego życia będzie przenoszona do świata wirtualnego. By jednak zrozumieć obecny stan przestrzeni wirtualnej i móc prognozować kierunku rozwoju w przyszłości musimy zwrócić uwagę na przeszłość przestrzeni wirtualnej.

1.2 Geneza i ewolucja cyberprzestrzeni

Należy wcześniej dokładnie zdefiniować przedmiot badań, genezę powstania i jego ewolucję na przestrzeni kilkudziesięciu ostatnich lat, aby dokładnie opisać i zbadać przestrzeń wirtualną. Cyberprzestrzeń jest nierozerwalnie związana z siecią Internet, czyli: „ogólnoświatową siecią komputerową, która jest logicznie połączona w jednorodną sieć adresową opartą na protokole komunikacyjnym TCP/IP (*Transmission Control Protocol/ Internet Protocol*). Internet jest globalną siecią komputerów komunikujących się ze sobą za pomocą wspólnego języka (...) składającą się z milionów serwerów oraz komputerów, z których korzystają użytkownicy na całym świecie. Pojedyncze komputery połączone są ze sobą w tak zwane sieci lokalne, które łączą się z siecią miejską, a te połączone są w tak zwane sieci krajowe. Połączone sieci krajowe tworzą sieć światową. Internet nazywa się często <<siecią sieci<<, ponieważ zbudowany jest na zasadzie łączenia ze sobą sieci o coraz większym zasięgu (…) Internet jest interaktywnym medium informacyjnym pozwalającym na dwukierunkową komunikację o globalnym zasięgu. Internet zmienia tradycyjne podejście do komunikacji, zacierając granice geograficzne pomiędzy ludźmi, ale także zmienia tradycyjne podejście do biznesu. Internet jako medium stał się najszybszym i największym źródłem informacji. Przejmuje coraz więcej funkcji tradycyjnych kanałów informacji, rozszerzając je o interaktywność, która nie jest dostępna w żadnym innym medium”[20].

[20] H. Babis, *Internet,* [w:] E. Cała– Wacinkiewicz, R. Podgórzański i in. (red.), *Encyklopedia zagadnień międzynarodowych*, Warszawa 2011, s. 540-541.

1.2.1. Historia powstania Internetu

Początki Internetu sięgają lat sześćdziesiątych XX wieku. W okresie zimnej wojny w Stanach Zjednoczonych została powołana w ramach Departamentu Obrony agencja *Advanced Research Projects Agency* (ARPA), której celem było opracowanie innowacyjnych projektów badawczych w dziedzinie obronności. Sama agencja nie posiadała własnych laboratoriów, zlecała więc badania instytucjom akademickim lub przemysłowym między innymi *Massachusetts Institute of Technology* (MIT). Począwszy od 1962 roku ARPA stała się głównym sponsorem badań nad techniką komputerową na terenie całych USA. Agencja fundusze swe poświęciła na stworzenie kilku komputerowych centrów badawczych oraz dofinansowanie uniwersytetów na badania naukowe[21]. Na początku lat sześćdziesiątych RAND Corporation[22] rozpoczęła badania nad opracowaniem nowego systemu komunikacji, który w razie ewentualnego zmasowanego ataku nuklearnego byłby zdolny do dalszego działania, a tym samym pozwoliłby na utrzymanie kontroli oraz umożliwił komunikację między różnymi jednostkami. W założeniu system ten miał być pozbawiony centralnego punktu kontroli i dowodzenia, a liczba węzłów informacyjnych miała być na tyle duża, by w przypadku zniszczenia części z nich sieć działałaby dalej dzięki pozostałym połączeniom, które kierowałyby ruchem w sposób zautomatyzowany[23]. Opracowana technologia *packet – switching*[24] pozwala na fragmentaryzację strumienia danych na kawałki (pakiety) i przesyłanie ich w takiej postaci do odbiorcy, który następnie składa je ponownie w całość. Technika ta umożliwia szyfrowanie wiadomości oraz zwiększa przepustowość przesyłu[25].

[21] J. Hofmokl, *Internet jako nowe dobro wspólne*, Warszawa 2009, s. 66.
[22] RAND Corporation – amerykańska organizacja badawcza o charakterze non-profit. Pierwotnie została ona stworzona na potrzeby sił militarnych USA. Organizacja została założona w maju 1948 r., początkowo pracując dla amerykańskiej armii, następnie dla innych organizacji rządowych i komercyjnych. Obecnie RAND posiada blisko dwa tysiące pracowników w sześciu siedzibach w Stanach Zjednoczonych oraz Europie. Korporacja RAND doceniana jest między innymi ze względu na duży wkład w naukę, między innymi w zakresie badań nad sztuczną inteligencją, obronnością, terroryzmem, edukacją czy zdrowiem publicznym.
[23] J. Gołaczyński, *Umowy elektroniczne w prawie prywatnym międzynarodowym*, Warszawa 2007, s. 11.
[24] Packet – switching (ang.) – komutacja pakietów, sposób transmisji danych polegający na dzieleniu danych na pakiety, a następnie wysyłaniu ich za pomocą łączy komunikacyjnych pomiędzy węzłami sieci.
[25] J. Hofmokl, op. cit., s. 66.

1.2.1.1. ARPANET

W 1969 roku w wyniku dotacji ARPA powstała pierwsza sieć połączonych komputerów z wybranych uniwersytetów kontaktujących się ze sobą na zasadzie *peer – to – peer* (równorzędnie). Sieć nazwano ARPANET[26], a jej głównym celem było umożliwianie połączenia między położonymi daleko od siebie komputerami oraz wymiana ich zasobów.

Przedsięwzięcie było kontrolowane przez agencję rządową, mimo to wypracowanie ogólnych reguł co do założeń projektu okazało się niezwykle trudne. Nad projektem pracowali informatycy posługujący się wyspecjalizowaną wiedzą, którą w obecnym czasie posiadała jedynie garstka osób. Projekt, prowadzony przez pracowników uniwersyteckich zdominowały swobodne relacje panujące w tym środowisku. Efektem tego było uznanie za główny cel ułatwiania i wspierania współpracy naukowców z różnych ośrodków akademickich. Prace nad projektem dzięki temu uzyskały znaczną decentralizację oraz charakteryzowały się kolegialnością oraz rezygnacją z sformalizowanych reguł postępowania. Wszelkie decyzje podejmowane były na zasadzie konsensusu i z uwzględnieniem relacji koleżeńskich. Tak ukształtowane stosunki odegrały znaczny wpływ na dalszy rozwój Internetu[27].

Powołano grupę badawczą – *Network Working Group* (NWG), by ujednolicić komunikację między komputerami. Jej członkami byli głównie młodzi doktoranci z wydziałów informatycznych. Grupa ta miała charakter otwarty i niezhierarchizowany, bez szczegółowego planu działania i formalnej struktury. NWG pełniła rolę centrum wymiany informacji między członkami grupy oraz forum technicznego opracowującego protokoły internetowe[28].

Pierwsza próba zdalnego połączenia pomiędzy komputerami znajdującymi się w Los Angeles i Stanford odbyła się 29 września 1969 roku. Komputery zdołały przesłać jedynie litery „l" i „o" (początek słowa login), jednakże jeden z komputerów zawiesił się przy próbie przesłania litery „g"[29]. Jak wskazuje Joanna Hofmokl, przed upływem 1971 roku infrastruktura ARPANET była już przygotowana. W jej skład wchodziło 15 węzłów i

[26] ARPANET – ang. *The Advanced Research Projects Agency Network.*
[27] J. Hofmokl, op. cit., s. 67.
[28] Ibidem, s. 67.
[29] J. Gołaczyński, *Umowy elektroniczne w prawie prywatnym …*, s. 12.

stopniowo przyłączane były nowe – niezwiązane bezpośrednio z ARPA. Warto zaznaczyć, iż mimo że ARPANET działał w ramach Departamentu Obrony i był całkowicie finansowany z ARPA udało się zachować dużą niezależność i swobodę. Nie wywierano na nią również nacisków, by sieć była kształtowana pod kątem militarnym[30]. W 1972 roku węzeł na Hawajach został podłączony przez łącze satelitarne, a rok później, za pomocą tej samej metody powstały dwa pierwsze węzły zagraniczne - w Wielkiej Brytanii i Norwegii. ARPANET przekształcił się w sieć międzynarodową[31].

Naukowcy i inni użytkownicy mieli ogromny wpływ na kształt sieci. W założeniach głównymi użytkownikami sieci mieli być specjaliści - informatycy i naukowcy, którzy za pomocą sieci komputerowej mogliby dzielić się osiągnięciami i wymieniać poglądy. To właśnie oni byli pierwszymi użytkownikami ARPANET. W pierwszym okresie dostęp do sieci był nie tylko ograniczony osobowo, ale również technologicznie. Komputery były kosztowne, zajmowały dużo miejsca, a ich obsługa była bardzo skomplikowana. Wdrożenie się w działanie komputerów był procesem nie tylko długotrwałym, ale również wymagającym dużej wiedzy i samozaparcia[32].

Przełomowym momentem działania ARPANET było opracowanie pierwszego programu do przesyłania poczty elektronicznej (*e-mail*). W kolejnych latach prowadzono badania nad wykorzystaniem łączności radiowej i satelitarnej w technologii sieciowej – co miało szczególne znaczenie militarne. W 1972 roku ARPA zmieniła swą nazwę na DARPA[33] obsługując trzy eksperymentalne sieci: ARPANET, PRNET (radiową) i SATNET (satelitarną).

Robert Kahn, ówczesny dyrektor DARPA, postanowił doprowadzić do połączenia trzech sieci, umożliwiając hostom[34] komunikację przez wiele sieci pakietowych bez konieczności znajomości technologii każdej z nich. To właśnie próby rozwiązania trudności funkcjonowania „międzysieci" dały początek idei Internetu. Joanna Hofmokl opisując początki powstania Internetu wskazuje: „W 1973 roku Robert Kahn wraz z Vintorem Cerfem opracowali projekt »otwartej architektury sieciowej« (ang. *open architecture networking*)

[30] J. Hofmokl, op. cit., s. 68.
[31] J. Gołaczyński, *Umowy elektroniczne w prawie prywatnym …*, s. 12-13.
[32] J. Hofmokl, op. cit., s. 68.
[33] DARPA – Agencja Zaawansowanych Obronnych Projektów Badawczych Departamentu Obrony Stanów Zjednoczonych (ang. - *Defence Advanced Research Project Agency*) - amerykańska agencja rządowa zajmująca się rozwojem technologii wojskowej.
[34] Host – jest to dowolne urządzenie (komputer, telefon, modem, tablet itp.) podłączony do Internetu lub innej sieci, posiadający niepowtarzalny adres IP uczestniczący w wymianie danych bądź usług sieciowych.

zakładający powstanie wielu niezależnych sieci, których struktura i technologia nie byłyby podporządkowane żadnym odgórnym zarządzeniom. Pracę nad nim podjęli nie tylko specjaliści komputerowi związani z ARPANET, lecz również przedstawiciele różnych międzynarodowych ośrodków zajmujących się projektami sieci pakietowych oraz dostawcy usług telekomunikacyjnych z różnych państw, którzy planowani budowę własnych sieci. Skupili się oni w ramach International Network Working Group (INWG). INWG nie przysługiwały żadne formalne uprawnienia, a jej członkowie liczyli, że uda im się osiągnąć nieformalne porozumienie i połączyć swoje systemy. W efekcie ich spotkań i konsultacji stworzono podstawowe założenia współpracy między różnymi sieciami, co wyznaczyło dalszy kierunek rozwoju Internetu. Pierwotne rozważania mające na celu połączenie różnych sieci ARPANET przyczyniły się do wypracowania polityki nieograniczania różnorodności sieci i wypracowania technologii, która umożliwiałaby im swobodne przesyłanie danych. Założenia te były odzwierciedleniem ideologii pionierów idei sieci, którzy widzieli w nich przede wszystkim narzędzie służące łączeniu odległych i odmiennych od siebie osób i instytucji”[35]. Okazało się, że technologią, która jest w stanie spełnić wszystkie powyższe wymagania jest jednolity protokół transmisji danych TCP/IP (ang. *Transmission Control Protocol / Internet Protocol*). Decyzja o zastosowaniu protokołu TCP/IP zapadła oddolnie. Twórcy sieci stwierdzili, że użyta technologia musi być prosta w zastosowaniu, a przechodzenie z sieci do sieci niemal niewidoczne.[36]. Protokół ten miał przede wszystkim umożliwić współdziałanie różnych typów sieci komputerowych – właśnie ta idea przyświecała samej nazwie Internet. Inter to międz*y*, a net to sieć.

W 1977 roku nastąpiło połączenie ARPANET, PRNET i SATNET. Departament Obrony USA dążył do wykorzystania sieci przede wszystkim w celu militarnym – przez pryzmat ich przydatności w dziedzinie obronności. W 1975 roku ARPANET został przejęty przez *Defence Communications Agency* (DCA). Była to próba wprowadzenia większego nadzoru nad siecią, gdyż im więcej osób niezwiązanych bezpośrednio z wojskiem korzystała z sieci, tym trudniej było zachować tajność projektów wojskowych. W efekcie, obawiając się wycieków informacji, DCA całkowicie ograniczyła dostęp do sieci osobom nieuprawnionym. Wprowadzony został system rejestracji użytkowników i przypisywania im indywidualnych haseł dostępu[37].

[35] J. Hofmokl, op. cit., s. 68.
[36] Ibidem, s. 69 - 70.
[37] Ibidem, s. 70-71.

Mimo ograniczenia dostępu do sieci, władze wojskowe w dalszym ciągu nie ufały społeczności akademickiej posiadającej dostęp do ARPANET. Na początku lat osiemdziesiątych pojawiły się pierwsze wirusy i hackerzy, który mogliby zaszkodzić nie tylko sieci cywilnej, ale również wojskowej[38]. W konsekwencji 4 kwietnia 1983 roku została wyodrębniona sieć przeznaczona wyłącznie do celów militarnych o nazwie MILNET[39]. Sieć ARPANET od tej pory służyła wyłącznie celom badawczym. Paradoksalnie wyodrębnienie sieci wojskowej przyczyniło się do rozwoju sieci cywilnej, która w danej chwili wykraczała już poza granice Stanów Zjednoczonych[40]. MILNET z czasem podzielił się na IPRNET (sieć wojskowa o obiżonym stopniu tajności), SIPRNET (sieć przeznaczona do tajnych operacji) i JWICS (sieć do ściśle tajnych działań)[41].

Zwiększona popularność ARPANET spowodowała, że kolejne ośrodki akademickie zaczęły domagać się dostępu do sieci, ponieważ we wczesnych latach osiemdziesiątych dostęp ten ograniczony został wyłącznie do jednostek i instytutów związanych, na mocy różnorakich umów, z agencją DARPA. Nowo powstała sieć - *Computer Science Network* (CSNET) sfinansowana została z funduszy Narodowej Fundacji Nauki (ang. *National Science Foundation*). CSNET została połączona z ARPANET i w znacznym stopniu przyczyniła się do spopularyzowania Internetu. Nie mniej istotny jest fakt, że członkostwo w CSNET było otwarte dla każdego podmiotu zainteresowanego rozwojem technik informacyjnych, o ile mógł on sobie pozwolić na opłatę kosztów związanych z obsługą sieci. CSNET nie mógł być wykorzystany w celach komercyjnych. Ponadto, sieć ta otworzyła połączenia międzynarodowe[42].

Joanna Hofmokl wskazuje, że „w połowie lat 80 powstała nowa sieć NSFNET[43] wzbogacona o bardzo szybkie łącza, które stworzyły tak zwany szkielet, do którego połączono mniejsze sieci poszczególnych uczelni – w tym ARPANET. W sumie NSFNET tworzyło na początku około 170 różnych sieci. Nowe możliwości NSFNET ujawniły słabości już 20-letniej sieci ARPANET, której łącza nie były przystosowane do dużego ruchu (w 1987 roku w Internecie było kilkaset tysięcy komputerów, z których korzystało około 1 miliona użytkowników). Do NSFNETU przyłączyły się również inne kraje, które budowały sieci

[38] M. Pudełko, *Prawdziwa histori@ Internetu*, Piekary Śląskie 2013, s. 72.
[39] MILNET – ang. *Millitary Network.*
[40] J. Hofmokl, op. cit., s. 71.
[41] M. Pudełko, op. cit., s. 73.
[42] J. Hofmokl, op. cit., s. 71.
[43] NSFNET – ang. *National Science Foundtion Network.*

szkieletowe[44] na wzór sieci amerykańskiej (Kanada, Francja i kraje skandynawskie). Dzięki temu sieć NSFNET stała się bardziej nowoczesna i 28 lutego 1990 roku zastąpiła całkowicie swoją poprzedniczkę, a ARPNET przestała istnieć. W ten sposób te sieci, które połączyły się NSFNET, stały się również częścią Internetu"[45].

Ważnym elementem, który przyczynił się do powstania Internetu było tworzenie sieci lokalnych LAN[46]. Sieci te tworzyły się głównie wokół ośrodków akademickich, niezależnie od projektów państwowych czy też tych wspieranych przez agencje rządowe. Rozwój sieci LAN nierozerwalnie łączy się z pojawieniem się pierwszych komputerów osobistych[47]. Z roku na rok następował gwałtowny rozwój sieci – w 1982 roku było ich 12, a w 1986 już ponad 400. Właśnie te sieci lokalne odegrały istotny wpływ na obecny kształt Internetu – charakteryzujący się niesformalizowaną strukturą. Dość szybko zaczęto przyłączać sieci nieformalne do Internetu. DARPA zezwoliła na przesyłanie poczty pomiędzy różnymi sieciami oraz dofinansowała badania nad oprogramowaniem umożliwiającym komunikację między sieciami[48].

W 1991 roku utworzono koncepcję języka HTML[49], który umożliwia łatwe tworzenie dokumentów, tabel, grafiki i innych obiektów zawierających dane. Jednakże ważniejsza funkcja tego języka jest związana z tak zwanym łącznikiem – dzięki któremu odbiorca informacji ma możliwość przeniesienia się bezpośrednio do innych stron, dokumentów lub plików[50]. W latach 1989-1990 Tom Berners - Lee i Robert Cailliau stworzyli system o nazwie ENQUIRE, który miał na celu pomoc w szybszym i bardziej efektywnym szukaniu plików. Opracowane oprogramowanie przyczyniło się do stworzenia przez Bernersa-Lee i Cailliau pierwszej strony internetowej oraz pierwszej internetowej przeglądarki[51].

---

[44] Sieć szkieletowa - (ang. *backbone network*) – sieć telekomunikacyjna, w tym sieć komputerowa, przez którą przesyłana jest największa liczba informacji. Łączy zwykle mniejsze sieci (sieci lokalne), grupy robocze, przełączniki, sieci rozległe. Urządzenia wchodzące w strukturę sieci szkieletowej z reguły odpowiedzialne są za funkcjonowanie całej sieci na określonym obszarze.
[45] J. Hofmokl, op. cit., s. 71-72.
[46] LAN (ang. *Local Area Networks)* – sieci komputerowe łączące komputery na określonym obszarze, takim, jak szkoła, biuro czy laboratorium. W porównaniu do sieci WAN (ang. Wide Area Network) LAN charakteryzuje się wyższym wskaźnikiem transferu danych oraz mniejszym obszarem geograficznym.
[47] Komputer osobisty (ang. *personal computer*) –komputer przeznaczony do użytku osobistego (domowego lub biurowego). Komputer służy do odtwarzania programów, gier, muzyki, filmów. Pierwszym komputerem osobistym dostępnym dla ogółu był Apple I wprowadzony przez firmę IBM.
[48] J. Hofmokl, op. cit., s. 73-74.
[49] HTML – ang. *Hypertext Markup Languuage.*
[50] K.B. Wydro, *Internet dziś – stan i wykorzystanie*, [w:] A. Szewczyk, E. Krok (red.), *Fenomen Internetu*, t. 1, Szczecin 2008, s. 50.
[51]A. Schwabach, *Internet and the Law: technology, society and compromises*, Santa Barbara, s. 187.

Rok 1991 przyniósł również podłączenie Polski do Internetu. Nastąpiło to 12 września 1991 roku. Budowa niezbędnej infrastruktury finansowana była z budżetu Komitetu Badań Naukowych, jednakże główną jednostką zajmującą się wdrażaniem sieci wirtualnej była Naukowa i Akademicka Sieć Komputerowa (NASK). Gdy rozwinęła się przeglądarka WWW do rozwoju Sieci włączyły się również firmy komercyjne[52].

1.2.1.2. Komercjalizacja Internetu

W latach dziewięćdziesiątych XX wieku nastąpiła gwałtowna komercjalizacja Internetu. W okresie, gdy Internet powstawał jako sieć wojskowa nikt nie przewidywał, iż będzie codziennie użytkowany przez miliardy użytkowników. W połowie lat 90 łącza nie były przystosowane do przesyłu tak wielkiej ilości danych i obsługi wzrastającej liczby użytkowników. Pojawiały się nawet poglądy, iż sieć nie wytrzyma takiej aktywności i w pewnym momencie przestanie działać. Prognozy te nie ziściły się, gdyż firmy prywatne inwestując w infrastrukturę zaczęły wzmacniać tak zwany „szkielet" Internetu – a mianowicie jego główne łącza. Mimo zaangażowania firm prywatnych nie były one w stanie zaspokoić całego popytu. Jak wynika z danych firmy inwestującej w łącza szkieletowe – WorldCom w 1997 roku popyt na przepustowość Internetu wzrósł dziesięciokrotnie. Było to wynikiem nie tylko większej liczby użytkowników, ale również zamieszczaniem w Sieci coraz większej ilości grafiki i plików dźwiękowych. Finansowanie rozwoju sieci wyłącznie z funduszy naukowych nie byłoby dłużej możliwe. Firmy prywatne dostrzegły jednak potencjał biznesowy wykorzystania Internetu[53].

Na początku lat dziewięćdziesiątych wolny rynek zainteresował się sieciami komputerowymi, ponieważ nastąpił znaczny wzrost liczby komputerów osobistych, a Internet osiągnął znaczne większe rozmiary niż w latach sziedemdziesiątych. Spowodowało to, iż sieć zaczęła dynamicznie rozwijać się w oddolnych strukturach przez małe prywatne firmy tworzące sieci na potrzeby lokalne. Ponadto, nastąpiła prywatyzacja dużych amerykańskich

[52] T. Bienias, *Internet*, Kraków 1998, s. 20-21.
[53] Ibidem, s. 21.

firm telekomunikacyjnych, które zobaczyły wielkie szanse związane z rozwojem sieci komputerowych[54].

Prywatyzacji podjęła się agencja NSF[55], której celem stało się całkowite wycofanie udziału agencji rządowych z administrowania Internetem. W statucie użytkowania sieci NSFNET do tej pory istniał zapis o zakazie korzystania z sieci do celów komercyjnych. Jednakże pod wpływem większej liczby użytkowników, zapis ten był coraz mniej przestrzegany – zarówno przez samych użytkowników, jak i dostawców usług sieciowych. Domagali się oni utworzenia konkurencyjnego rynku usług dla sieci szkieletowych – zwłaszcza, iż coraz prężniej rozwijały się w tym zakresie firmy prywatne[56]. Przedsiębiorstwa prywatne widząc potencjał wykorzystania Internetu, zaczęli również dodawać obsługę TPC/IP do sprzętu i produkowanego oprogramowania[57].

W efekcie agencja NSF widząc możliwość przeniesienia sieci NSFNET w sferę prywatną przyśpieszyła proces deregulacji Internetu. Deregulacja nastąpiła w sposób planowy – poprzedzony konsultacjami z użytkownikami i twórcami sieci. W listopadzie 1991 roku został opublikowany *Project Development Plan*, zgodnie z którym usługi internetowe zostały przejęte przez konkurujące ze sobą prywatne firmy dostarczające usługi sieciowe tak zwane *Internet Service Providers*. Plan wszedł w życie w 1994 roku. Zgodnie z projektem każdy z dostawców usług miał niezależnie zarządzać konkretnym szkieletem łączącym się następnie z centralnym szkieletem NSFNET. Centralny szkielet został włączony 30 kwietnia 1995 roku, a pracowało w nim 50 766 sieci z 93 krajów[58].

Stopniowe wycofywanie się agencji rządowych z zarządzania Internetem nie oznacza, iż zupełnie stracili oni zainteresowanie cyberprzestrzenią. Władze państw z zaciekawianiem obserwowały rozwój sieci cyfrowej. Zauważono, iż nowy obszar działalności człowieka będzie determinowało odpowiedzialność prawną w zakresie prawa karnego, cywilnego, handlowego czy praw własności intelektualnej.

[54] J. Hofmokl, op. cit., s. 75.
[55] NSF – ang. *The National Science Foundation* – Agencja rządowa Stanów Zjednoczonych wspierającą podstawowe badania i edukację we wszystkich pozamedycznych dziedzinach nauki i inżynierii. W niektórych dziedzinach takich, jak matematyka, informatyka, ekonomia i nauki społeczne NSF jest głównym źródłem federalnego wsparcia.
[56] J. Hofmokl, op. cit., s. 75.
[57] M. Pudełko, op. cit., s. 89.
[58] J. Hofmokl, op. cit., s. 76.

1.2.1.3. System domen internetowych

Każdy internauta, aby zdobyć konkretną informację musi wejść na stronę internetową o indywidualnie przypisanym adresie. Każdy komputer podłączony do sieci (ang. *host*) ma przypisaną nazwę i adres numeryczny, za pomocą którego sieć identyfikuje dany komputer. W okresie rozwoju sieci ARPANET Network Information Center opracowało podział nazw na tak zwane domeny. Nazwy hostów przybrały formę host@domain – oznaczało to, że dany adres jest zarejestrowany na konkretnej domenie. Uniwersytet Południowej Kalifornii w połowie lat osiemdziesiątych opracował System Nazw Domen (ang. *Domain Name System*). Agencja DARPA stworzyła 6 domen głównych reprezentujących różne dziedziny sieci: .gov (rządowa), .mil (wojskowa), .edu (edukacyjna), .com (biznes), .org (inne organizacje) oraz .net (zasoby sieciowe)[59]. Na poziomie poszczególnych domen system jest już zdecentralizowany i dzielone na poszczególne kategorie – na przykład www.uwb.edu.pl czy www.sejm.gov.pl. Głównym zadaniem systemu nazw domen jest tłumaczenie adresów stron internetowych znanym internautom, na adresy zrozumiałe dla urządzeń tworzących sieć komputerową[60].

W USA za rządów prezydenta Clintona został opracowany program przeniesienia funkcji kontrolowania nazw i adresów internetowych w niezależną organizację. Jak wskazuje Joanna Hofmokl, powodem takiej decyzji była „konieczność przekazania zarządzania w ręce prywatne i stworzenia ciała organizacyjnego, które nie podlegałoby wpływom ani rządów narodowych, ani międzynarodowych organizacji”[61]. Rozporządzeniem „White Paper” 18 września 1998 roku powstała Internet Corporation for Assigned Society and Numbers (ICANN[62]). Jest to organizacja *non – profit*, odpowiedzialna za przyznawanie nazw domen internetowych, ustalanie struktury oraz sprawująca ogólny nadzór nad działaniem serwerów DNS na całym świecie.

[59] J. Hofmokl, op. cit., s. 83.
[60] Z. Płoski, *Słownik encyklopedyczny - Informatyk*a, Hasło dostępne na stronie internetowej http://portalwiedzy.onet.pl/89394,,,,system_nazw_domen,haslo.html [16.02.2017].
[61] J. Hofmokl, op. cit., s. 87.
[62] ICANN- (ang. *The Internet Corporation for Assigned Names and Numbers)* - Internetowa Korporacja ds. Nadawania Nazw i Numerów.

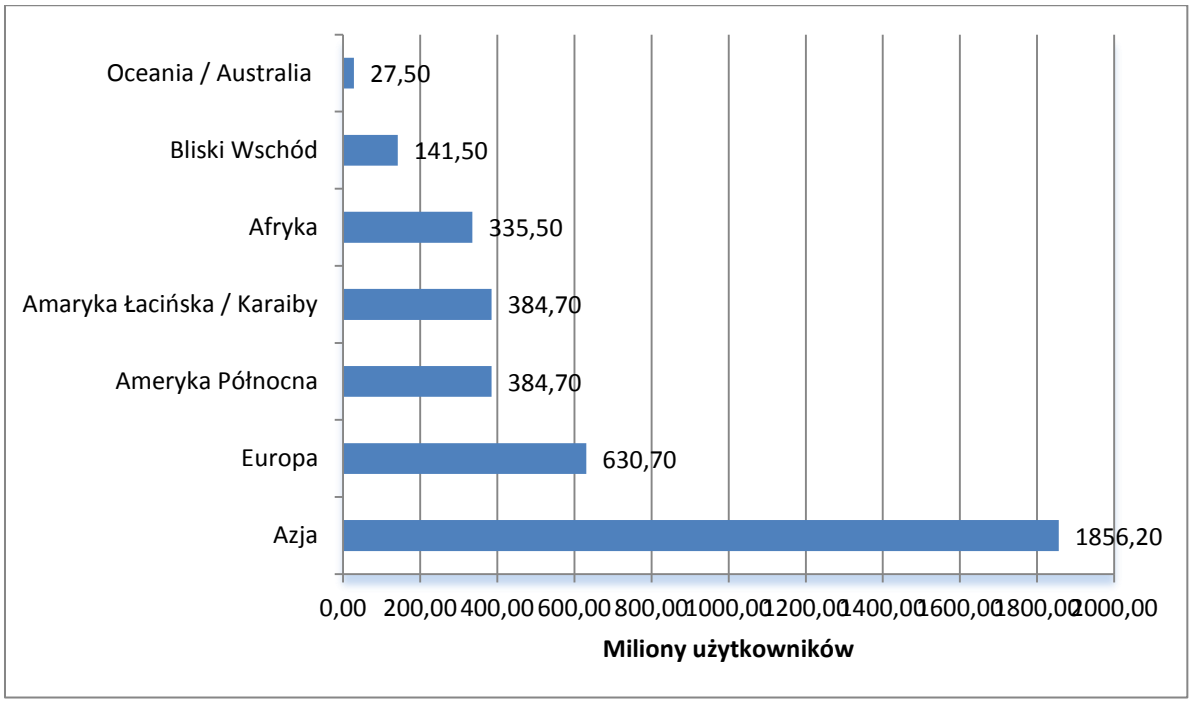
1.2.2. Internet na początku XXI wieku

Obecnie na Internet składają się sieci komputerowe LAN, sieci miejskie MAN[63] oraz sieci WAN łączące komputery organizacji na całym świecie. By zbadać wielkość Internetu, należy zadać sobie pytanie, w jaki sposób obliczyć tę wartość. Przyjmuje się, iż jest to: „liczba połączonych terminali albo serwisów, do których te terminale są połączone (hostów), liczbę połączonych sieci komputerowych, liczbę ludzi z Internetu korzystających lub też ilości przepływającej w nim informacji”[64]. W zależności od przyjętych metod badawczych, kryteriów i metod pomiarowych wartości te różnią się między poszczególnymi badaczami, a wymiary liczbowe nie są jednoznaczne. Nie bez znaczenia jest również dynamizm, szybkie zmiany i fluktuacja stanu Internetu. Ważniejsze jednak wydaje się obserwacja tendencji i zmian zaobserwowanych w badaniach.

Jedną z typologii które można przyjąć jest udział użytkowników Internetu w aktywności on – line z podziałem na kontynenty, z których pochodzą. Według statystyk zamieszczonych na stronie internetowej Internet World Stats w grudniu 2016 roku Internet miał ponad 3,69 miliardy użytkowników. Dla porównania, w grudniu 2000 roku było ich jedynie 360 milionów. Oznacza to, iż w liczba internautów na przestrzeni lat 2000 - 2016 zwiększyła się o 923%, a na chwilę obecną blisko połowa (49,2%) światowej populacji ma dostęp do sieci[65].

[63] MAN – ang. *Metropolitan Area Networks.*
[64] K.B. Wydro, op. cit., s. 51.
[65]Dane z oficjalnej strony internetowej World Stats: http://internetworldstats.com/stats.htm [20.04.2015].

Tabela 1. Liczba internautów na świecie (stan na 31 grudnia 2016 roku)



Źródło: Dane z oficjalnej strony internetowej Internet World Stats dostępny na stronie http://internetworldstats.com/stats.htm [01.02.2017].

Najliczniejszą grupą internautów na świecie, bo aż 50.01% z ponad 1,8 miliardową populacją są Azjaci. Na drugim miejscu plasują się Europejczycy, którzy stanowią 17,1% użytkowników sieci globalnej - aż 630,7 miliona mieszkańców Europy ma dostęp do Internetu. Kolejne miejsca zajmują: Ameryka Łacińska i Karaiby z odpowiednio 10,4% liczby użytkowników (około 335 milionów), Afryka - 9,1% (około 335 milionów), Ameryka Północna - 8,7% (około 320 milionów), Środkowy Wschód - 3,8% (około 141 milionów) oraz Australia i Oceania - 0,7% (około 27 milionów[66].

Zestawiając powyższe dane z liczbą ludności poszczególnych kontynentów okaże się, że 88,1% mieszkańców Ameryki Południowej ma dostęp do Internetu. Na podobnie wysokim poziomie znajduje się Europa (76,7%) oraz Australia i Oceania (68%). Ponad połowa, bo 59,4% ludności Ameryki Łacińskiej i Karaibów jest użytkownikami sieci wirtualnej. Na kolejnym miejscu plasuje się Środkowy Wschód (56,5%). Mimo, że ponad miliard użytkowników Internetu zamieszkuje Azję to jedynie 44,7% ma dostęp do sieci. Na ostatnim

[66]Dane z oficjalnej strony internetowej Internet World Stats http://internetworldstats.com/stats.htm [01.02.2017].

miejscu plasuje się Afryka, w której jedynie co czwarty mieszkaniec (26,9%) może korzystać z dobrodziejstw Internetu[67].

Dynamikę rozwoju sieci wirtualnej ukazuje porównanie liczby sieci, hostów i użytkowników na przełomie lat i stopień ich wzrostu (tabela 2).

Tabela 2. Ilościowy rozwój Internetu

Rok	Liczba sieci	Liczba hostów	Liczba użytkowników
1968	3	b.d.	b.d.
1970	b.d.	b.d.	b.d.
1975	12	b.d.	b.d.
1980	b.d.	b.d.	b.d.
1985	300	b.d.	b.d.
1990	5 tys.	1 mln	14 mln
1995	40 tys.	6,57 mln	57 mln
2000	120 tys.	60 mln	379 mln
2005	600 tys.	350 mln	1,04 mld
2007	b.d.	440 mln	1,26 mld
2010	1,5 mln[a]		1,8 mld[a]
2030			4 mld[a]

a prognozy
Źródło: K.B. Wydro, op. cit., s. 51.

W 1968 roku na świecie znajdowały się wyłącznie trzy sieci, mimo iż brak jest dokładnych danych co do liczby użytkowników bez wątpienia należy stwierdzić, że była to grupa nieliczna, powiązana z ARPA. Gwałtowny wzrost zarówno liczby sieci jak i użytkowników przypada na lata dziewięćdziesiąte XX wieku. Od tego czasu liczba użytkowników sieci, hostów i użytkowników zwiększyła się paręsetkrotnie. Co ciekawe, K.B. Wydro przewidywał w 2008 roku, iż liczba internautów w 2030 roku będzie wynosić około 4 miliardów. Wydaje się, iż stan ten zostanie osiągnięty szybciej niż mogły o tym świadczyć prognozy, ponieważ zgodnie z danymi witryny internetowej Internet Word Stats[68] w połowie 2014 roku liczba użytkowników sieci przekroczyła już 3 miliardy.

Inną typologią opisującą rozwój Internetu, którą można przyjąć jest ustalenie odsetka gospodarstw domowych z krajów Unii Europejskiej, które posiadają dostęp do Internetu w poszczególnych latach. Statystyczny podział w poszczególnych państwach został przedstawiony w tabeli 3.

[67] Ibidem.
[68] Ibidem.

Tabela 3: Odsetek gospodarstw domowych z dostępem do Internetu w Unii Europejskiej w latach 2005-2013

Rok / Wyszczególnienie	2005	2006	2007	2008	2009	2010	2011	2012	2013
Unia Europejska (28 krajów)	48	49	54	60	66	70	73	76	79
Holandia	50	51	56	62	90	91	94	94	95
Luksemburg	65	70	75	80	87	90	91	93	94
Szwecja	73	77	79	84	86	88	91	92	93
Dania	75	79	78	82	83	86	90	92	93
Niemcy	62	67	71	75	79	82	83	85	88
Finlandia	54	65	69	72	78	81	84	87	89
Wielka Brytania	60	63	67	71	77	80	83	87	88
Francja	b/d	41	49	62	69	74	76	80	82
Belgia	50	54	60	64	67	73	77	78	80
Austria	47	52	60	69	70	73	75	79	81
Irlandia	47	50	57	63	67	72	78	81	81
Malta	41	53	54	59	64	70	75	77	79
Estonia	39	46	53	58	63	68	71	75	80
Słowenia	48	54	58	59	64	68	73	74	76
Słowacja	23	27	46	58	62	67	71	75	78
Polska	30	36	41	48	59	63	67	70	72
Czechy	19	29	35	46	54	61	67	65	73
Litwa	16	35	44	51	60	61	60	60	65
Łotwa	31	42	51	53	58	60	64	69	72
Węgry	22	32	38	48	55	60	65	69	71
Hiszpania	36	39	45	51	54	59	64	68	70
Włochy	39	40	43	47	53	59	62	62	69
Chorwacja	b/d	b/d	41	45	50	56	61	66	65
Cypr	32	37	39	43	53	54	57	62	65
Portugalia	31	35	40	46	48	54	58	61	62
Grecja	22	23	25	31	38	46	50	54	56
Rumunia	b/d	14	22	30	38	42	47	54	58
Bułgaria	b/d	17	19	25	30	33	45	51	54

Źródło: opracowanie własne na podstawie: Raport strategiczny IAB Polska Internet 2010[69] oraz Raport strategiczny IAB Polska Internet 2013[70].

[69] Raport dostępny na oficjalnej stronie internetowej IAB: http://iab.org.pl/badania-i-publikacje/raport-strategiczny-iab-polska-internet-2010/ [21.07.2015].

W 2005 roku 48% gospodarstw domowych w Unii Europejskiej miało dostęp do Internetu. W ciągu 8 lat liczba ta wzrosła o blisko 30%, osiągając wynik 79%. Do państw, w których ponad 90% mieszkańców ma dostęp do sieci wirtualnej zaliczyć można Holandię (95%), Luksemburg (94%), oraz Szwecję i Danię (po 93%). W jedynie ośmiu państwach UE mniej niż 70% gospodarstw domowych ma dostęp do Internetu. Najgorzej sytuacja przedstawia się w Grecji i Bułgarii, gdzie jedynie co drugie gospodarstwo korzysta z dobrodziejstw cyberprzestrzeni. Powyższa statystyka wskazuje również jak szybko Internet rozwija się w państwach członkowskich Unii Europejskiej, w roku 2005 w Holandii jedynie 50% gospodarstw miało dostęp do sieci, w 2013 roku już 95%. Szczególnie dynamiczny wzrost dostępności Internetu nastąpił w Czechach i na Węgrzech, gdzie w 2005 roku jedynie co piąte gospodarstwo domowe miało dostęp do sieci. W chwili obecnej w obu państwach już co siódmy mieszkaniec korzysta z przestrzeni wirtualnej.

Internet, mimo że powstał zaledwie pięćdziesiąt lat temu, jest jednym z najbardziej rewolucyjnych wynalazków XX wieku. Projekt wojskowy, który swój zalążek miał w okresie zimnej wojny, w założeniu służyć miał obronności Stanów Zjednoczonych. Przekazanie prac nad siecią ośrodkom akademickim, w których panowały odformalizowane, kolegialne stosunki niewątpliwe wpłynęło na wolnościowy kształt Internetu. Popularyzacja sieci zapoczątkowana w latach dziewięćdziesiątych to przede wszystkim zasługa pojawienia się komputerów osobistych oraz komercjalizacji Internetu.

Sieć wirtualna dzięki swojej strukturze przyczyniła się do postępu procesu globalizacji, ułatwiła handel, komunikowanie się na odległość, przepływ informacji i danych. Sieć, która początkowo służyła jedynie garstce naukowców użytkowana jest obecnie przez ponad trzy miliardy ludzi. Trudno przewidzieć, w jakim kierunku będzie się rozwijać Internet, niewątpliwe jest tylko jedno - systematycznie zwiększać się będzie liczba jego użytkowników, rozwijając przed nimi coraz to nowe możliwości, niewymierne korzyści, ale również zagrożenia.

[70] Raport dostępny na oficjalnej stronie internetowej IAB: http://iab.org.pl/wp-content/uploads/2014/08/raport_iab_2013.pdf [21.07.2015].

1.3 Etapy rozwoju społeczeństwa informacyjnego

Przeobrażenia cywilizacyjne, których bezpośrednim skutkiem jest przyśpieszony rozwój techniczny skutkowały gruntownymi zmianami w systemie techniki, produkcji, edukacji, transportu czy kultury. Przyczyniło się to do powstania pojęcia społeczeństwa informacyjnego (ang. *Information Society)* – społeczeństwa opartego na wiedzy i informacji.

Johna Naisbitt, amerykański publicysta z zakresu futurologii, uważał, iż początek społeczeństwa informacyjnego datuje się w latach 1956-1957. Jako bezpośrednie źródło jego powstania wskazał takie wydarzenia, jak: rozwój gospodarki Stanów Zjednoczonych, wstąpienie Japonii do Organizacji Narodów Zjednoczonych (ONZ), wystrzelenie w 1956 roku radzieckiego sputnika w kosmos, co zapoczątkowało tym samym erę globalnej komunikacji satelitarnej. Ponadto, w 1956 roku po raz pierwszy liczba pracowników umysłowych w Stanach Zjednoczonych (tak zwanych *white – collar workers*) przewyższyła liczbę pracowników fizycznych (tak zwanych. *blue – collar workers*).[71]

Pierwsze wzmianki na temat społeczeństwa informacyjnego pojawiły się w połowie lat sześćdziesiątych w Japonii. Określenie *johoka shakai*[72] po raz pierwszy zostało użyte w 1963 roku przez Tadao Umesao w pracy dotyczącej ewolucyjnej teorii społeczeństwa opartego na informacji. Termin ten oznacza społeczeństwo komunikujące się przez komputer lub po prostu społeczeństwo informacyjne. Na początku lat siedemdziesiątych nazwą ta posługiwał się również Yoneji Masuda w rozważaniach o przemianach społecznych w powiązaniu z rozwojem sektora informacji i telekomunikacji. Pracę opublikowano w 1983 roku[73].

Yoneji Masuda opisał zmiany zachodzące w społeczeństwie opartym na informacji i technologii. Twierdził on, iż „cywilizacja, którą zbudujemy, zbliżając się do końca XX wieku, nie będzie cywilizacją materialną, symbolizowaną przez ogromne konstrukcje, ale będzie faktycznie cywilizacją niewidoczną. Precyzyjnie powinno się ją nazywać cywilizacją informacyjną. Homo sapiens, który pod koniec ostatniej epoki lodowcowej stanął przed

[71] M. Witkowska, K. Cholawo – Sosnowska (red.*), Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006, s. 13,
[72] Termin oznaczający w języku japońskim społeczeństwo informacyjne,
[73] Y. Masuda, *The information society as post-indrustial society*, Waszyngton 1983; J.S. Nowak, G. Bliźniuk, *Społeczeństwo informacyjne: doświadczenie i przyszłość,* Katowice 2006, s. 9.

początkiem pierwszej – materialnej cywilizacji, stoi dziś po dziesięciu tysiącach lat na progu drugiej – cywilizacji informacyjnej”[74].

W 1973 roku Daniel Bell sformułował główne cechy społeczeństwa informacyjnego, uznał, iż będzie się ono charakteryzować rosnącą dominacją specjalistów i naukowców w układzie zawodowym, sterowanym rozwojem techniki, a wiedza i informacja stanie się źródłem strategii i przemian społeczeństwa. Mianem postindustrialnego określał on społeczeństwo, w którym zatrudnienie w sektorze usług jest wyższe niż w sektorze rolniczym czy przemysłowym, tak więc następuje dominacja sektora usług zarządzanego przez specjalistów i naukowców. Głównym dobrem jest wiedza teoretyczna, społeczna kontrola rozwoju nauki, a podstawą podejmowania decyzji społecznych i politycznych są technologie intelektualne[75].

W światowej literaturze pojęcie społeczeństwa informacyjnego jest różnie definiowane (tabela 4). Piotr Sienkiewicz określa je, jako „taki system społeczny, ukształtowany w procesie modernizacji, w którym systemy informacyjne i zasoby informacyjne determinują społeczną strukturę zatrudnienia, wzrost zamożności społeczeństwa (dochodu narodowego) oraz stanowią o orientacji cywilizacyjnej”[76]. Maria Nowina Konopka przytacza definicję zaczerpniętą z raportu IBM Community Development Foundation: „Społeczeństwo informacyjne charakteryzuje się:

- wysokim stopniem korzystania z informacji w życiu codziennym przez większość obywateli i organizacji;
- użytkowaniem jednorodnej lub kompatybilnej technologii informacyjnej na użytek własny, społeczny, edukacji i działalności zawodowej;
- umiejętnością przekazywania, odbierania, a także szybkiej wymiany danych cyfrowych bez względu na odległość”[77].

Martin Bangemann w swym raporcie stwierdza: „społeczeństwo informacyjne charakteryzuje się przygotowaniem i zdolnością do używania systemów informatycznych i

[74] Y. Masuda, *Managing in the Information Society*, Basil Blackwell, Oxford 1990, [za:] M. Witkowska, K. Cholawo – Sosnowska (red*.), Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006, s. 14.
[75] J. S. Nowak, G. Bliźniuk, op. cit., s. 10.
[76] P. Sienkiewicz, *Teoria rozwoju społeczeństwa informacyjnego*, [w:] L. H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno - kulturowe*, Kraków 2002, s. 506-507.
[77] M. Nowinka Konopka, *Istota i rozwój społeczeństwa informacyjnego*, [w:] M. Witkowska, K. Cholawo – Sosnowska (red.), op. cit., s. 15.

wykorzystuje usługi telekomunikacyjne do przekazywania i zdalnego przetwarzania informacji"[78]. W polskiej doktrynie Jacek Mączyński definiuje społeczeństwo informacyjne jako takie, które określone informacje: wytwarza, przechowuje, przekazuje, pobiera i wykorzystuje[79]. Stanisław Juszczyk uwydatnia zawodowy czynnik, podkreślając, iż o społeczeństwie informacyjnym możemy mówić, gdy siła robocza składa się w większości z pracowników informacji, stosunki społeczne oparte są na gospodarowaniu informacją, a informacja jest najistotniejszym dobrem[80]. Jerzy S. Nowak podaje za socjologami Tomaszem Gobanem – Klas i Piotrem Sienkiewiczem, iż społeczeństwo informacyjne to „społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania się, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła utrzymania większości społeczeństwa"[81].

W materiałach OECD[82] zapisano, iż „społeczeństwo informacyjne może zostać znalezione na przecięciu kiedyś odrębnych przemysłów: telekomunikacyjnego, mediów elektronicznych i informatycznego, bazujących na paradygmacie cyfrowej informacji. Jedną z wiodących sił jest stale rosnąca moc obliczeniowa komputerów oferowanych na rynku, której towarzyszą spadające ceny. Innym elementem jest możliwość łączenia komputerów w sieci, pozwalająca im na dzielenie danych, aplikacji a czasami samej mocy obliczeniowej, na odległości tak małe jak biuro i tak duże jak planeta. Ten podstawowy model rozproszonej mocy obliczeniowej i szybkich sieci jest sednem społeczeństwa informacyjnego"[83].

Tabela 4. Definicji społeczeństwa informacyjnego

Kryterium identyfikacji	Opis	Przedstawiciele
Techniczne	decydujące znaczenie ma rozwój nowoczesnej technologii informacyjnej	J. Naisbitt J. Mączyński
Ekonomiczne	fundamentalne znaczenie dla rozwoju społeczeństwa informacyjnego ma wiedza oraz informacja	D. Bell
Zawodowe	społeczeństwo informacyjne nie tylko stwarza nowe możliwości, ale również wymusza elastyczną specjalizację	M. Piore C. Sabel S. Juszczyk

[78] Europe and the Global Information Society, Recomendations of the Bangerman Group to the European Council, http://www.epractice.eu/files/media/media_694.pdf [29.04.2012].
[79] Mączyński J., *Globalne społeczeństwo informacyjne. Wybrane kwestie adaptacyjne*, [w:] L.. W. Zacher (red.), *Rewolucja informacyjna i społeczeństwo. Niektóre trendy, zjawiska i kontrowersje*, „Transformacje"1997, s. 7.
[80] M. Nowinka Konopka, op. cit., s. 18.
[81] J. S. Nowak, G. Bliźniuk (red.), op. cit., s. 2.
[82] OECD – (ang. *Organisation for Economic Co – operation and Development*) - Organizacja Współpracy Gospodarczej i Rozwoju.
[83] J. S. Nowak, G. Bliźniuk (red.), op. cit., s. 2.

	produkcji i pracy	
Przestrzenne	społeczeństwem informacyjnym jest każde państwo narodowe zdolne do określenia zasobów alokacyjnych i władczych oraz do rozpoznania potrzeb własnych obywateli	M. Castells
Kulturowe	kultura współczesna stała się rzeczywistością wirtualną, *simulacrum*, czyli swoistą symulacją znaczeń trudnych do rozpoznania w natłoku informacji, świat jest natomiast taki, jakim wykreują go media	J. Baudrillard

Źródło: M. Nowinka-Konopka, op. cit., s. 19.

Szybkie tempo rozwoju technicznego powoduje również rozwój automatyki i powszechne zastosowanie komputerów. Dostęp do informacji stał się kluczem do dobrobytu i postępu, a informacja podstawą integracji przemysłu, usług i rynków w jedną całość. Analiza cech trzech typów społeczeństw: agrarnego, przemysłowego i informacyjnego doprowadziła Roberta Bałdysa i Tadeusza Leszczyńskiego do wniosku, iż kolejnym etapem rozwoju będzie społeczeństwo postinformacyjne (tabela 5).

Tabela 5. Porównanie trzech typów społeczeństw: przediformacyjnego, informacyjnego i postinformacyjnego

Cecha	**Społeczeństwo przedinformacyjne**	**Społeczeństwo informacyjne**	**Społeczeństwo postinformacyjne**
Bogactwo	Kapitał	wiedza	informacja
Produkt podstawowy	wyroby przemysłowe	informacja, dane	satysfakcja
Praca	daleko od domu	w domu, telepraca	w dowolnym miejscu
Transport	kolej, autostrada	infostrada	indywidualne kosmoloty
Energia	węgiel, para, benzyna	jądrowa	słoneczna, wiatrowa, oceaniczna
Skala działania	regionalna	globalna	międzyplanetarna
Rozrywka	Masowa	domowa	indywidualna
Tajemnica	polityczna	handlowa	organizacyjna
Oświata	Szkoła	komputer, telenauczanie	wirtualna klasa

Źródło: R. Bałdys, T. Leszczyński*, Cyberterroryzm zagrożeniem bezpieczeństwa energetycznego społeczeństwa informacyjnego,* [w:] T. Jemioła, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm - nowe wyzwania XXI wieku*, Warszawa 2009, s. 133.

Piotr Sienkiewicz zidentyfikował następujące cechy społeczeństwa informacyjnego:

1. „Dominacja sektora usług w gospodarce oraz rozwój (ilościowy i jakościowy) usług informacyjnych;

2. Wysokie tempo rozwoju sieci komunikacji społecznej i modernizacja informacyjnej infrastruktury; Ranga zasobów informacyjnych jako zasobów strategicznych i rozwój zasobów zarządzania informacjami (wiedzą, kapitałem intelektualnym);

3. Wiodąca rola edukacji i badań naukowych jako głównego źródła innowacji i postępu cywilizacyjnego;

4. »Nowa Gospodarka« (GOW, gospodarka cyfrowa, e-biznes) jako rezultat interakcji Techniki (IT), Gospodarki i Społeczeństwa;

5. Bezpieczeństwo informacyjne jako znaczący element bezpieczeństwa społeczeństwa (bezpieczeństwa narodowego); nowe koncepcje obronne (*»Information Warfare«, »Cyberwar«, »Netwar«*);

6. Wysoki wpływ Internetu i mediów elektronicznych na zmiany zachowań społecznych (*»Cyberculture«*);

7. Nowe koncepcje organizacji (organizacja wirtualna, sieciowa, ucząca się itp.) i nowe metody zarządzania (zarządzanie kryzysowe, zarządzanie ryzykiem, zarządzanie zmianami itp.)”[84].

W doktrynie zapisano dwie koncepcje społeczeństwa informacyjnego – europejską i amerykańską. Pierwsza z nich opiera się na ideach humanistycznych, które zakładają, iż rozwój techniki ma przyczynić się do realizacji celów społecznych, ekonomicznych i organizacyjnych. Według tego założenia technologia ma przyczynić się do wzrostu poziomu życia i pracy obywateli, oraz umacniania ich tożsamości kulturowej. Z kolei w koncepcji amerykańskiej dominuje paradygmat technologiczny. Główny nacisk kładzie się na globalizm w rozwoju technologii informacyjno komunikacyjnych (ICT[85]). Niezależnie jednak od różnic między tymi założeniami Mateusz Czapielewski wyróżnia cztery główne obszary działalności społeczeństwa informacyjnego:

[84] P. Sienkiewicz, *Prognozowanie rozwoju globalnego społeczeństwa informacyjnego: wizje i scenariusze*, [w:] A. Szewczyk, E. Kot (red.), *Fenomen Internetu*, t.1., Szczecin 2008, s. 25-26.

[85] ICT (ang. *Information and Communication Technologies*) – dział telekomunikacji i informatyki, umożliwiający manipulację i przesyłanie informacji (przesyłanie, sterowanie przepływem, transmisja danych). Jest obecnie uznawane za jedną z ważniejszych gałęzi technologii informacyjnych (IT).

1. „Technologiczny – dotyczy infrastruktury i stosowanych technologii, czyli obejmuje dostępność urządzeń służących gromadzeniu, przetwarzaniu, przechowywaniu i udostępnianiu informacji, mnogość kanałów przesyłania danych oraz możliwość łączenia ich w rozmaite koniugacje.

2. Ekonomiczny – ma związek z sektorem informacyjnym gospodarki, czyli tymi gałęziami produkcji i usług, które zajmują się wytwarzaniem informacji oraz technik informacyjnych, a także ich dystrybucją. Społeczeństwa informacyjne charakteryzują się dużym udziałem tych dziedzin gospodarki w PKB.

3. Społeczny – wynika z tego, że istnieje wysoki odsetek osób korzystających w pracy, szkole i domu z technologii informatycznych, co jest zbieżne z wysokim poziomem wykształcenia społeczeństwa.

4. Kulturowy – wynika z wysokiego poziomu kultury informacyjnej, przez którą rozumie się stopień akceptacji informacji jako dobra strategicznego i towaru, a także odpowiedni poziom kultury informatycznej”[86].

Maria Nowina Konopka przypisuje społeczeństwu informacyjnemu różne funkcje, w zależności od regionu występowania oraz etapu wdrożenia. Są to:

1. Funkcje edukacyjne – mają one na celu globalne upowszechnienie wiedzy naukowej oraz uświadomienie znaczenia podnoszenia kwalifikacji.

2. Funkcje komunikacyjne – jako nowa płaszczyzna budowania więzi społecznych. Ma to szczególne znaczenie w kontekście powstania w wyniku globalizacji społeczeństw wielokulturowych, wieloetnicznych i wielowyznaniowych. Społeczeństwo informacyjne ma na celu umożliwienie funkcjonowania i komunikowania się różnolitych grup w ramach globalnego społeczeństwa.

3. Funkcje socjalizacyjne i aktywizacyjne –przez mobilizację osób będących czasowo lub stale wyłączonych z funkcjonowania w społeczeństwie. Możliwość komunikacji, kształcenia się czy podjęcia telepracy bez konieczności wychodzenia z domu

[86] M. Czapielewski, *Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii),* [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioły, J. Kisielińskiego, K. Rakchela (red.), Warszawa 2009, s. 179.

znacząco zmienia sytuację osób do tej pory wykluczonych społecznie – osób niepełnosprawnych, przewlekle chorych czy też matek wychowujących dzieci.

4. Funkcje partycypacyjne – możliwość prowadzenia debat publicznych w Internecie, umożliwienie głosowania za pomocą sieci wirtualnej, powoduję aktywizację polityczną i aktywne uczestnictwo w życiu państwa.

5. Funkcje organizatorskie – mają się przyczynić do stworzenia warunków sprzyjających konkurencyjności na rynku teleinformatycznym oraz funkcjonowanie w nim wszystkich grup społecznych.

6. Funkcje ochronne i kontrolne – mają na celu stworzenie mechanizmów obronnych osób prywatnych oraz instytucji państwowych przed cyberprzestępczością oraz monitorowanie standardów funkcjonowania wszystkich podmiotów społeczeństwa informacyjnego.[87]

Można podzielić pogląd Piotra Sienkiewicza dotyczący wagi informacji w społeczeństwie informacyjnym. „Rozwój infosfery: społeczeństwa informacyjnego i gospodarki opartej na wiedzy, przyniósł świadomość kluczowej roli informacji zarówno w działaniach polityczno - militarnych, jak i ekonomicznych. Warunkiem sukcesu w walce i biznesie jest uzyskanie przewagi informacyjnej nad przeciwnikiem i konkurencją. Przewaga informacyjna (wiedzy) jest warunkiem przewagi strategicznej. Swoistym paradoksem społeczeństwa informacyjnego jest nierównomierny podział zasobów informacyjnych na rynku, czyli asymetria informacji. A zatem współczesne modele sytuacji decyzyjnej powinny uwzględniać asymetryczność informacyjną. Przewaga informacyjna to wszak stan asymetrii informacji (wiedzy - »świadomości sytuacyjnej«)”[88].

Od początku lat dziewięćdziesiątych rządy państw europejskich, dostrzegając konieczność rozwoju społeczeństwa informacyjnego w celu między innymi zwiększenia konkurencyjności rynku europejskiego zaczęły podejmować konkretne inicjatywy mające przyczynić się do rozwoju i promocji tej idei. Jednym z ważnych etapów rozwoju społeczeństwa informacyjnego była publikacja w grudniu 1993 Białej Księgi o „Rozwoju, Konkurencyjności i Zatrudnieniu”, a następnie w maju 1994 raportu Martina Bangemanna

[87] M. Witkowska, K. Cholawo – Sosnowska (red.), J. S. Nowak, G. Bliźniuk (red.), op. cit., s. 21-22.
[88] P. Sienkiewicz, *Od cybernetyki Wienera do cybernetycznej przestrzeni,* [w:] *10 wykładów*, Warszawa 2005, s. 36.

według którego, fundamentem tworzenia społeczeństwa informacyjnego były finanse sektora prywatnego i mechanizmy rynkowe. Raport ten wraz z Programem e- Europa (1999), Strategią Lizbońską (2000) oraz Programem i-2010 (2005) wyznaczył kierunek działania Unii Europejskiej w następnych latach. W kontekście tych działań można wyróżnić cztery kategorie działań związanych z budową społeczeństwa informacyjnego, są to rozwój sieci, szybkiego i taniego Internetu, rozwój e-usług, wzrost konkurencyjności przez powszechniejsze wykorzystanie ICT oraz aktywizacja społeczna[89].

Mimo różnic między poszczególnymi krajami w tworzeniu i rozwoju społeczeństwa informacyjnego można wyróżnić podstawowe uwarunkowania jego rozwoju. Zalicza się do nich:

1. „Pełną liberalizację rynków, na których realizowane są usługi dla społeczeństwa informacyjnego,
2. Rozległą infrastrukturę telekomunikacyjną,
3. Spójne i przejrzyste prawodawstwo dostosowane do potrzeb nowego typu społeczeństwa,
4. Wysoki poziom nakładów finansowych na badania i rozwój w tym zakresie,
5. Nieskrępowany dostęp do sieci wszystkich operatorów i usługodawców,
6. Szeroki, powszechny i tani dostęp do Internetu i zawartych w nim treści,
7. Szeroki publiczny dostęp do zasobów teleinformacyjnych,
8. Wysoki średni współczynnik kompetencji teleinformacyjnych,
9. Wysoki stopień korzystania z informacji,
10. Umiejętność przekazywania, odbierania, a także szybkiej wymiany danych cyfrowych bez względu na odległość,

[89] M. Czapielewski, op. cit., s. 180.

11. Wysoki odsetek osób zatrudnionych w szeroko rozumianych usługach (ze szczególnym uwzględnieniem sektora teleinformacyjnego)"[90].

Plan budowy społeczeństwa informacyjnego w Unii Europejskiej zapoczątkowano w 1993 roku w dokumencie Growth, *Competitiveness and Employment. The Challenges and Ways Forward into 21st Century*[91]. Ta Biała Księga skoncentrowała się głównie wokół kwestii ekonomicznych, a za priorytet przyjęła konkurencyjność gospodarki Wspólnoty Europejskiej oraz osiągnięcie standardów informatycznych wypracowanych przez Stany Zjednoczone[92]. Za początek rozwoju polityki tworzenia społeczeństwa informacyjnego uznaje się jednak publikację przez Komisję Europejską w 1994 roku dokumentu Europa i społeczeństwo globalnej informacji. Zalecenia dla Rady Europy[93]. Akt ten zyskał nazwę Raportu Bangermanna – od nazwiska komisarza do spraw przemysłu, technologii informacyjnych i telekomunikacji Martina Bangemanna. W ocenie ekspertów wyrażoną w raporcie społeczeństwo informacyjne powinno tworzyć się w oparciu o finanse sektora prywatnego i mechanizmy rynkowe. Sektor publiczny z kolei powinien pojąć odpowiednie kroki w celu opracowania odpowiednich regulacji prawnych, ochronie obywateli i konsumentów oraz podnoszeniu świadomości społeczeństwa. Postulaty zawarte w Raporcie Bangemanna wyznaczyły politykę Unii Europejskiej w dziedzinie społeczeństwa informacyjnego. Zgodnie z nimi:

- rozwój społeczeństwa informacyjnego powinien kierować wolny rynek – konieczne jest zatem stworzenie warunków uczciwej konkurencji w dziedzinie usług telekomunikacyjnych i informacyjnych;
- konieczne jest zapewnienie na terenie UE powszechnego dostępu do usług, aplikacji, usług i programów informacyjnych;
- środki finansowe przeznaczone na rozwój społeczeństwa informacyjnego powinny pochodzić przede wszystkim z sektora prywatnego;
- niezbędne są ochrona prywatności i bezpieczny przepływ informacji;

[90] M. Nowinka - Konopka, op. cit., s. 21.
[91] Dokument dostępny online: http://www.cvce.eu/content/publication/1997/10/13/b0633a76-4cd7-497f-9da1-4db3dbbb56e8/publishable_en.pdf [20.02.2016].
[92] M. Nowinka - Konopka, op. cit., s. 26-27.
[93] *Europe and the Global Information Society. Recommendations of the Bangemann Group to the European Council*, Brussels, 26 maja 1994 r.

- należy zapewnić ochronę i promowanie różnic kulturowych oraz językowych w Unii Europejskiej;

- trzeba podjąć współpracę z krajami mniej rozwiniętymi gospodarczo, w szczególności z krajami Europy Środkowej i Wschodniej;

- należy promować i uświadamiać, jakie nowe możliwości daje rozwój społeczeństwa informacyjnego oraz przeprowadzić odpowiednie szkolenia na wszystkich etapach edukacji[94].

W 1996 roku Komisja Europejska opublikowała Zieloną Księgę *Living and Working in Information Society. People First*[95]. Dokument ten skupiał się na konsekwencjach, jakie przyniesie dla obywateli transformacja w kierunku społeczeństwa informacyjnego oraz na wpływie ICT na ich życie. Kolejną inicjatywą Unii Europejskiej zmierzającą do budowy nowoczesnej i silnej gospodarki krajów członkowskich był projekt *eEurope – An Information Society for All* (eEuropa Społeczeństwo Informacyjne dla wszystkich)[96]. Projekt ten opierał się na kilku priorytetach: edukacji, sektorze zdrowia, aktywizacji zawodowej osób niepełnosprawnych i transporcie. W 1999 roku wydano Zieloną Księgę *Public Sector Information: a Key Resource for Europe*. Dokument ten opisuje korzyści zarówno dla obywateli jak i całej gospodarki, które wynikają z wykorzystania w obszarze służb publicznych technologii telekomunikacyjnych i informatycznych[97].

Jako priorytet Unia Europejska przyjęła umożliwienie powszechnego dostępu do Internetu. Plan mający na celu budowę europejskiego społeczeństwa informacyjnego został opracowany 23 i 24 marca 2000 roku w Lizbonie - na specjalnym posiedzeniu Rady Europejskiej – zyskał on nazwę Strategii Lizbońskiej. Plan działania został opracowany na dwóch płaszczyznach: gospodarczej i społecznej. Płaszczyzna gospodarcza budowy społeczeństwa informacyjnego opierać się miała na wykorzystaniu ICT w celu zwiększenia konkurencyjności gospodarki. Z kolei sfera społeczna opierała się na koncepcji Luca Soete'a, który uznał społeczeństwo informacyjne za „społeczeństwo, które właśnie się kształtuje, w którym technologie gromadzenia oraz transformacji informacji i danych są powszechnie

[94] J. S. Nowak, G. Bliźniuk (red.), op. cit., s. 16.
[95] Dokument dostępny na oficjalnej stronie internetowej Komisji Europejskiej w języku angielskim http://europa.eu/rapid/press-release_IP-96-688_en.htm?locale=en [10.12.2016].
[96] Dokument dostępny na oficjalnej stronie internetowej Eur-Lex w języku angielskim: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24221 [10.12.2016].
[97] M. Nowinka - Konopka, op. cit., s. 27-28.

dostępne po niskich kosztach. Powszechnemu dostępowi do informacji i danych towarzyszą organizacyjne, komercyjne, społeczne i prawne zmiany, które głęboko zmieniają życie, pracę i społeczeństwo jako takie"[98].

W trakcie szczytu europejskiego w Feira w 2000 roku został przyjęty kolejny plan *eEurope 2002 – An Information Society for All*. Dokument ten wskazywał konieczność rozwoju szybkiego, taniego, powszechnego Internetu, inwestowania w potencjał ludzki oraz popularyzacji wykorzystania sieci wirtualnej. Następny plan rozwoju społeczeństwa informacyjnego, rozumianego jako strategiczny element budowy gospodarki opartej na wiedzy, przedstawiono w Goteborgu w 2001 roku. W *eEurope + 2003: A Co – operative Effort to Implement the Information Society in Europe – Action Plan* założono przyśpieszenie reform i pobudzenie modernizacji gospodarek państw kandydujących do Unii przez wykorzystanie narzędzi i technologii społeczeństwa informacyjnego. Jednym z głównych celów była też poprawa konkurencyjności i spójności społecznej. Inicjatywę tą poparły również kraje kandydujące w tym czasie do Unii Europejskiej[99].

W Sewilli 21 i 22 czerwca 2002 roku odbył się szczyt Unii Europejskiej, w trakcie którego przyjęto plan rozwoju społeczeństwa informacyjnego do 2005 roku. W dokumencie eEurope 2005: An Information Society for All – Action Plan, państwa członkowskie UE zobowiązały się do realizacji następujących zadań:

- rozwoju usług elektronicznych tylu: e-*learning, e-government, e-health*;
- tworzenie dynamicznego środowiska do rozwoju gospodarki elektronicznej;
- zapewnienie powszechnego dostępu do Internetu szerokopasmowego;
- budowy systemu bezpieczeństwa infrastruktury informacyjnej[100].

W dokumencie Komisji Europejskiej z 2005 roku *i2010 – European Information Society for Growth and Employment,* uznano, iż wiedza i innowacje są motorem zrównoważonego wzrostu. Stwierdzono, iż konieczne jest zbudowanie integracyjnego społeczeństwa informacyjnego na fundamencie technologii informacyjnych i komunikacyjnych (ICT) wykorzystywanych w administracji publicznej, małych i średnich

[98] Ibidem, s. 28-29.
[99] Ibidem, s. 29.
[100] Ibidem, s. 28-29.

przedsiębiorstwach oraz w gospodarstwach domowych. W związku z powyższym Komisja Europejska określiła trzy priorytety polityki w zakresie budowy społeczeństwa informacyjnego: realizacja idei Europejskiej Przestrzeni Informacyjnej, promującej otwarty, konkurencyjny rynek, wspieranie innowacji i inwestycji w technologie ICT (w celu promowania rozwoju oraz wzrostu zatrudnienia) oraz stworzenie Europejskiego Społeczeństwa Informacyjnego[101]. W komunikacie do programu podkreślono szybki postęp technologicznych, a technologie ICT są coraz powszechniej stosowane. W dziedzinie sieci komunikacyjnych, mediów, usług i urządzeń zachodzi konwergencja cyfrowa – dzięki coraz lepszym sieciom i technikom kompresji tworzą się nowe, szybsze kanały dystrybucji. Uznano, że jeżeli Unia Europejska ma w pełni wykorzystać swój potencjał gospodarczy, to konieczne jest przyjęcie proaktywnego stanowiska politycznego stymulującego pozytywne trendy na rynku i wspierającego budowę społeczeństwa wiedzy, chroniące konsumentów oraz zmierzające do budowy bezpiecznego europejskiego społeczeństwa informacyjnego[102].

W Komunikacie stwierdzono, iż budując jednolitą przestrzeń informacyjną konieczne jest odniesienie się do czterech głównych wyzwań związanych z konwergencją cyfrową: szybkość (dostęp do szybkich usług szerokopasmowych, ułatwiających dostęp do zawartości multimedialnej, czyli na przykład wideo w wysokiej rozdzielczości), zawartość multimedialna (poprawa sytuacji ekonomicznej i prawnej sprzyjającej powstawaniu nowych usług i zawartości on – line), interoperacyjność (ulepszenie urządzeń i platform, oraz stworzenie usług umożliwiających komunikowanie się między różnymi platformami) oraz bezpieczeństwo – lepsze zabezpieczenie przed awariami technologicznymi, ale również przed oszustwami i szkodliwą zawartością[103].

Jedną z flagowych inicjatyw strategii „Europa 2020" na rzecz zatrudnienia i wzrostu gospodarczego jest Europejska Agenda Cyfrowa, mająca na celu optymalizację korzyści płynących z technologii cyfrowych. Program zaczęto realizować w maju 2010 roku. Komisja Europejska przedstawiła propozycje regulacyjne w sprawie stworzenia jednolitego europejskiego rynku usług telekomunikacyjnych oraz wzmocnienia cyfrowych połączeń w

[101] Ibidem, s. 30.
[102] Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno – Społecznego oraz Komitetu Regionów dotyczącego „*i2010 – Europejskie społeczeństwo informacyjne na rzecz rozwoju wzrostu i zatrudnienia*" COM (2005) 229 końcowy.
[103] Ibidem.

Europie. Unia Europejska podjęła działania mające na celu zapewnienie otwartego dostępu do Internetu, zniesienia opłat roamingowych i lepszą ochronę konsumentów[104].

Przedstawicie Unii Europejskiej dostrzeją nowe trendy, fakt coraz powszechniejszego używania smartphonów, najnowszych aplikacji, coraz większej dostępności do szybszego Internetu oraz postępu nowych technologii rozwijających się w zawrotnym tempie. Kraje unijne wspierają ten proces, ustanawiając akty prawne związane telekomunikacją między innymi z Internetem szerokopasmowym[105], dostępem do sieci łączności elektronicznej[106] czy też warunkami rynkowymi dla telefonów komórkowych i innych urządzeń komunikacyjnych[107], chroniąc prawa konsumentów i wspierając badania naukowe i innowacje. Strategia jednolitego rynku cyfrowego obejmuje 16 inicjatyw (od praw autorskich do problemu bezpieczeństwa w Internecie). Opiera się na ułatwieniu konsumentom i firmom z całej Europy dostępu do cyfrowych produktów i usług, stworzenie warunków do rozwoju sieci i innowacyjnych usług sieciowych oraz pobudzenie wzrostu gospodarczego związanego z gospodarką cyfrową. Szczególną rolę w kształtowaniu społeczeństwa informacyjnego odegrał Światowy Szczyt Społeczeństwa Informacyjnego oraz Forum Zarządzania Internetem.

Wyżej wymienione programy w głównej mierze zakładały rozwój gospodarczy, zwiększenie konkurencyjności, rozwój rynku ICT oraz budowę bezpiecznego społeczeństwa europejskiego. Szczególnie ten ostatni czynnik ma ogromne znaczenie, poniważ o ile Internet faktycznie znacznie przyczynił sie do rozwoju gospodarczego o tyle nie można pominąć zagrożeń, z którymi mamy do czynienia w przestrzeni wirtualnej.

---

[104] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie jednolitego rynku telekomunikacyjnego [COM(2013) 634 final z 11.9.2013 - nieopublikowany w Dzienniku Urzędowym].

[105] Dyrektywa Parlamentu Europejskiego i Rady 2014/61/UE z dnia 15 maja 2014 r. w sprawie środków mających na celu zmniejszenie kosztów realizacji szybkich sieci łączności elektronicznej, Dz.U. UE L 155 z 23.5.2014

[106] Dyrektywa Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (Tekst mający znaczenie dla EOG), Dz.U. L 337 z 18.12.2009.

[107] Dyrektywa Komisji 2008/63/WE z dnia 20 czerwca 2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych (Wersja skodyfikowana) (Tekst mający znaczenie dla EOG), Dz.U. L 162 z 21.6.2008

1.4 Zagrożenie w cyberprzestrzeni

Oprócz korzyści związanych z funkcjonowaniem społeczeństwa informacyjnego nie występują również zagrożenia i nowe problemy, które wiążą się z przestrzenią wirtualną. „Zjawiska i procesy zachodzące w cyberprzestrzeni znacznie wybiegają poza wymiar techniczny, przyjmując charakter społeczny. Jesteśmy obecnie świadkami kształtowania się tak zwanego społeczeństwa informacyjnego, czyli niezależnie od różnych prób jego definiowania, społeczeństwa o głębokich zmianach w świadomości społecznej, wywołanych skutkami rewolucji cyfrowej, oddziałujący wielowymiarowo, gospodarczo, politycznie, kulturowo, społecznie na otaczającą rzeczywistość za pomocą informacji. Społeczeństwo to bywa określane mianem społeczeństwa ryzyka, z uwagi na możliwe implikacje występujących w cyberprzestrzeni zagrożeń dla bezpieczeństwa pojedynczego człowieka, oraz zbiorowości ludzkich”[108] Zagrożenia w cyberprzestrzeni dotyczą jednostek, grup społecznych, organizacji, a nawet państw.

Według Ryszarda Czechowskiego oraz Piotra Sienkiewicza do negatywnych aspektów działalności społeczeństw informacyjnych zalicza się:

- konieczność budowy krajowej sieci informatycznej wiąże się z dużym nakładem finansowym;
- zagrożenie powstanie społeczeństwa kontrolowanego przez informatyzację administracji państwowej; możliwość włamań do systemu informacyjnego administracji państwowej i związane z tym naruszenie tajemnicy przedsiębiorstw lub tajemnicy państwowej;
- możliwość internetowego kształcenia terrorystów i członków organizacji przestępczych; coraz częściej spotykaną praktyką jest udostępnianie instrukcji, jak domowym sposobem stworzyć bombę czy przetransportować ją w dowolne miejsce unikając kontroli;

[108] R. Białoskórski, C*yberzagrożenia w środowisku bezpieczeństwa XXI w. - zarys problematyki*, Warszawa 2011, s. 13.

- wysokie koszty modernizacji systemu ochrony zdrowia, które mogą ponieść tylko najbogatsze kraje;

- całkowity paraliż ruchu drogowego i powietrznego w przypadku awarii skomputeryzowanego systemu komunikacji;

- ekspansję współpracy międzynarodowej i powstanie „globalnej wioski" sprzyjające zacieraniu się tożsamości kulturowej i narodowej;

- powstanie społeczeństwa kontrolowanego; szczególnym przykładem unaoczniającym ten problem jest regularne blokowanie przez chińskie władze dostępu do niektórych witryn internetowych poruszających drażliwe dla Chin tematy polityczne[109].

Cyberprzestrzeń doznaje specyficznych ograniczeń, które K. Węderska podzieliła na cztery obszary – prawa, przestrzeni, bezpieczeństwa i zagrożeń. Każdy z nich napotyka specyficzne problemy w swojej dziedzinie takie, jak niespójność i brak międzynarodowych standardów w obszarze prawa, brak przestrzennych, geograficznych granic w obszarze przestrzeni czy też brak jednolitych rozwiązań w kwestii bezpieczeństwa sieci wirtualnych (tabela 6).

Tabela 6. Obszary specyficznych ograniczeń cyberprzestrzeni

Obszar	**Charakterystyka**
PRAWO (law)	– prawo niejasne, niespójne; – niejasna odpowiedzialność za czyny i wykroczenia; – brak międzynarodowych (narodowych) kryteriów klasyfikacji i kwalifikacji; – nieprecyzyjne określenia aktów kryminalnych i aktów zagrożeń bezpieczeństwa narodowego.
PRZESTRZEŃ (space)	– brak przestrzennych granic; – brak politycznych granic; – brak geograficznych granic; – brak doraźnych granic.
ZAGROŻENIA (threats)	– prosta, ogólnie dostępna technologia; – anonimowośc sprawy; – wielośc form cyberataków; – „efekt domina" jako skutek;

[109] R. Czechowski, P. Sienkiewicz *Przestępcze oblicza komputerów,* Warszawa 1993, s. 133-134.

	– cechy „broni masowej dezorganizacji"; – niewielkie koszty ataków.
BEZPIECZEŃSTWO (safety)	– brak szybkich i skutecznych rozwiązań zabezpieczających; – mnogość obiektów zagrożeń (ataków); – wysokie koszty zabezpieczeń; – zróżnicowana podatność obiektów; – nieprzewidywalność źródeł zagrożeń; – bardzo wysokie koszty;

Źródło: P. Sienkiewicz, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, t. 9, s. 98.

Każdy z funkcjonujących systemów informatycznych i telekomunikacyjnych może być związany z określonymi zagrożeniami i podatnością na pewne działania o charakterze kryminalnym. Pierwszą grupą zagrożeń jest sabotaż i zagrożenia nieumyślne, które charakteryzuje występowanie szkody bez bezpośredniego materialnego lub informacyjnego zysku. Do kategorii tej zalicza się awarie zasilania energetycznego, pożary, klęski żywiołowe, dezintegrację, a także inne fizyczne czynniki destrukcyjne. Postacią dezintegracji lub destrukcji informatycznej mogą być wirusy komputerowe, bomby logiczne i konie trojańskie, a fizycznymi czynnikami destrukcyjnymi są między innymi ładunki wybuchowe niszczące aparaturę komputerową.

Drugą grupą zagrożeń tworzy infiltracja, czyli „działania osób nieupoważnionych, mające na celu przenikanie do różnych elementów systemu informatycznego lub sieci telekomunikacyjnej w celu zdobycia informacji za pomocą różnych sposobów i środków"[110]. Cechą charakterystyczną tej metody jest orientacja na osiągnięcie przez sprawcę zysku ze zdobytych informacji. Infiltracja dzieli się na dwie kategorie – infiltrację czynną i bierną. Infiltracja bierna jest to śledzenie informacji w określonym miejscu jej obiegu. Najczęściej stosowanymi technikami są:

- „przechwytywanie elektromagnetyczne, polegające bądź na uzyskaniu dostępu do połączeń między komputerem a terminalami, bądź do kierunkowej emisji promieniowania i na analizie sygnału odbitego od promieniującego urządzenia;
- dołączenie się do linii transmisji danych w sieciach telekomunikacyjnych lub przechwytywanie sygnałów przekazywanych drogą radiową;
- badanie i kopiowanie zasobów nie zabezpieczonych (piractwo komputerowe);

[110] Ibidem, s. 133-134.

- analiza makulatury lub pozostałości po nośnikach informacji, będąca rezultatem bądź niefrasobliwości w gospodarce makulaturą, bądź zlekceważenia obowiązku demagnetyzacji nośników informacji;

- stosowanie ukrytych nadajników”[111].

Infiltracja czynna jest to świadome zdobycie dostępu do systemu w zamiarze ingerencji w najbardziej wrażliwe oraz najważniejsze ogniwa systemu. Przyjmuje ona częstokrotnie następujące formy:

1. „Łamanie zabezpieczeń w celu dostępu do dowolnego miejsca w systemie informatycznym przy ominięciu zabezpieczeń stosowanych przez legalnego użytkownika systemu (na przykład dotarcie do rejestru zabezpieczeń) (…);

2. Ingerencja w struktury systemów operacyjnych;

3. Podszywanie się pod uprawnionego użytkownika systemów komputerowych;

4. Stosowanie programów i procedur dodatkowych (umieszczanych w fazie pisania oprogramowania lub podczas eksploatacji oprogramowania)”.[112]

Stosując metodę analizy prognostycznej GSO – technikę scenariuszy, bazującą na zestawie hipotetycznych zdarzeń Piotr Sienkiewicz opracował trzy warianty rozwoju społeczeństwa informacyjnego:

„Wariant A: ‘SYSTEM ROZPROSZONY’ o strukturze sieciowej, sprzyjającej ‘grze partykularnych interesów’, w którym podstawowymi zasobami jest informacja i wiedza. Zagrożeniami mogą być: atomizacja zachowań społecznych wraz z ‘atrofią więzi’ międzyludzkich.

Wariant B: ‘SYSTEM ZINTEGROWANY’ o strukturze hierarchicznej i grze ‘grup interesów’, w której wygraną jest dostęp do wiedzy jako podstawowego zasobu. Zagrożeniem może być swoisty ‘cyberatokrytaryzm’.

Wariant C: ‘SYSTEM CYBERNETYCZNY’ o strukturze nieliniowej sterowany ‘homeostatycznie’, sprzyjający dostępowi do wiedzy i ‘mądrości’ pojmowanej jako wolność

[111] Ibidem, s. 136.
[112] Ibidem, s. 137.

do stosowania wiedzy w interesie całego społeczeństwa. Strategia: trwały i zróżnicowany rozwój systemu”[113].

Walka informacyjna

Brak jest jednolitej definicji walki informacyjnej, lecz w występujących w doktrynie próbach zdefiniowania pojęcia pojawiają się wspólne cechy. Przede wszystkim może być uznana za konflikt, w którym informacja jest postrzegana zarówno jako obiekt ataku, broń oraz zasób. Równocześnie strony konfliktu mogą dokonywać fizycznych zniszczeń infrastruktury używanej przez przeciwnika do działań operacyjnych[114]. Piotr Sienkiewicz za walkę informacyjną uznaje „całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki informacyjnej jest:

- zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych;
- zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych”[115].

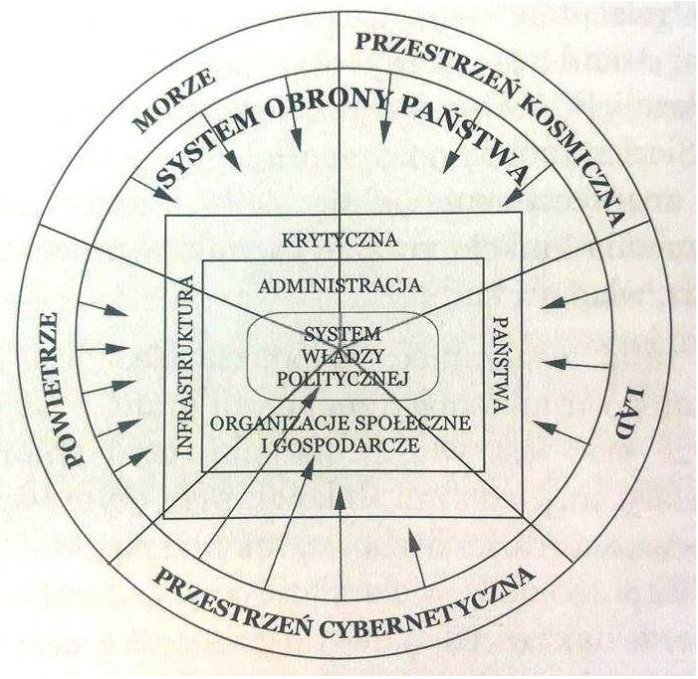
Walka informacyjna jest także uznana za „działanie informacyjne, prowadzone dla obrony własnej informacji i systemów informacyjnych lub dla atakowania i wywarcia wpływu na informację lub systemy informacyjne przeciwnika; jest prowadzona głównie w czasie kryzysu lub konfliktu, defensywny komponent tej walki, podobnie jak obrona powietrzna, realizowany jest w każdej fazie działań militarnych, od pokoju do wojny”[116]. Walka informacyjna, na skutek możliwości technologicznych danych przez cyberprzestrzeń

[113] P. Sienkiewicz, *Prognozowanie …*, s. 26.
[114] T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne - sieć - cyberprzestrzeń. Nowe zagrożenia*, [w:] K. Liedel, P. Piasecka, T.A. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna pokój i terroryzm w epoce informacji*, Warszawa 2014, s. 28-30, por. P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa - zjawisko walki informacyjnej*, [w:] M. Madej, M. Trelikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.
[115] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, [w:] L.H. Haber, *Społeczeństwo informacyjne - wizja czy rzeczywistość ?*, t. 1, Kraków 2004, s. 375.
[116] AFFDD 2-5 Information Operations, USAF, 1998 [za:] P. Sienkiewicz, H.Świeboda, *Sieci teleinformatyczne jako instrument państwa - zjawisko walki informacyjnej*, [w:] M. Madej, M. Trelikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 81.

wkroczyła w zupełnie nowy wymiar. W przestrzeni cyfrowej przechowywana jest ogromna ilość informacji i danych, a znaczna część infrastruktury, w tym infrastruktury krytycznej, uzależniona jest od niezakłóconego działania systemów informatycznych. Z tych względów przestrzeń cyfrowa może stać się łatwym celem ataków.

Tradycyjnie obszarami wojny i działań militarnych był ląd, powietrze i morze. W latach dziewięćdziesiątych XX wieku Warden wyróżnił piąty wymiar wojny - przestrzeń cybernetyczną (rysunek 1).

Rysunek 1. Przestrzeń zagrożeń bezpieczeństwa narodowego w społeczeństwie informacyjnym



Źródło: P. Sienkiewicz, H. Świeboda, *Niebezpieczna przestrzeń cybernetyczna*, Transformacje 2006, t. 47-50, s. 58 na podstawie J.A. Warden, *The Enemy as a System*, „Air Power Journal" 1995, t. 9, nr 1, s. 47.

Piotr Sienkiewicz i Halina Świeboda jako cechy charakterystyczne walki informacyjnej wskazują między innymi uzyskanie przewagi informacyjnej nad przeciwnikiem i pozorną anonimowość „niewidzialność" stron. Obszarem walki jest wówczas cyberprzestrzeń, a bronią są ataki o różnych formach i źródłach (głównie na infrastrukturę krytyczną państwa). Autorzy podkreślają, że „cyberwojna" wymaga rekonstrukcji paradygmatu bezpieczeństwa państwa, jego obronności oraz sposobu prowadzenia wojny. Zmiana ta przede wszystkim, powinna polegać na odejściu od liniowego postrzegania zagrożeń na rzecz myślenia „sieciowego", polegającego na postrzeganiu sieci sprzężeń

zwrotnych[117]. W ostatnich latach, zauważyć można pozytywny trend, do wprowadzania do krajowych porządków prawnych strategii cyberbezpieczeństwa. Władze krajowe, na skutek nasilających się ataków cybernetycznych (w tym ataków na kraje takie, jak Estonia i Gruzja), słusznie uznały, że podjąć należy odpowiednie prace legislacyjne, systemowe i techniczne, by przygotować się na ewentualną agresję w cyberprzestrzeni.

Walka informacyjna może przybierać wiele form Piotr Sienkiewicz i Halina Świeboda wskazują cztery metody ataku - elektromagnetyczny, ogniowy, działania psychologiczne oraz dezinformację. Każda z wymienionych kategorii będzie wywoływać inne skutki bezpośrednie i dalsze (tabela 7). Cel jednak jest zawsze jeden osłabienie przeciwnika, dezinformacja oraz zniszczenie jego zasobów.

Tabela 7: Przykładowy scenariusz zagrożeń na szczeblu państwa

Typ działań destrukcyjnych	**Skutek bezpośredni**	**Skutek dalszy**	**Przeciwdziałanie**
Atak elektromagnetyczny Wyzwolenie impulsów elektromagnetycznych w rejonach węzłów sieci. Uruchomienie urządzeń zakłócających pracę nadajników łączności bezprzewodowej	Zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznych - zakłócenie pracy lub paraliż tych sieci. Zniszczenie stacji nadawczych telefonii komórkowej zakłócenia w pracy sieci. Zakłócenie pracy stacji nadawczych telefonii bezprzewodowej	Utrata informacji administracyjnych. Zakłócenie pracy lub paraliż systemu administrowania miastem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń. Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny. Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci. Przerwanie linii magistralnych sieci.	Zniszczenie central telefonicznych i serwerowni - paraliż pracy sieci. Zakłócenie pracy lub paraliż systemu administrowania miastem.	Utrata informacji administracyjnych. Zakłócenie pracy systemu administrowania państwem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń. Fizyczne uodpornienie sieci na atak ogniowy. Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Działania psychologiczne	Umożliwienie dostępu do sieci	Zewnętrzny atak informatyczny na	Wykrywanie i ocena zagrożeń.

[117] P. Sienkiewicz, H. Świeboda, op. cit., s. 84-85.

Inżynieria społeczna - pozyskiwanie personelu urzędów do współuczestnictwa w atakach.	informatycznej systemów administrowania państwem, ujawnienie niejawnej informacji. Sabotaż wewnętrzny ze strony pozyskanego personelu. Defraudacje finansowe dokonywane przez pracowników administracji.	sieć. Zagrożenie bezpieczeństwa informacyjnego państwa. Kradzież niejawnych informacji (np. danych osobowych czy finansowych). Pogorszenie bezpieczeństwa finansowego. Zakłócenia w administrowaniu państwem. Wzrost poczucia zagrożenie i niezadowolenia społecznego.	Podnoszenie świadomości stanów osobowych Doskonalenie procedur kontroli dostępu do informacji.
Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz i kierownictw organizacji systemu administrowania państwem. Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu. Rozpowszechnianie fałszywych informacji o zamiarach władz państwa. Podawanie fałszywych informacji o pracy na rzecz interesów obcych państw i organizacji przez przedstawicieli władz.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania państwa. Próby zachwiania stabilnością finansową i płynnością finansową państwa. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Szybka reakcja władz na fałszywe informacje. Sprawne docieranie do ludności i personelu firm z obiektywną informacją. Zachowywanie prawdy w informowaniu. Wykrywanie i piętnowanie dezinformatorów.

Źródło: P. Sienkiewicz, H. Świeboda, op. cit.,s. 91, na podstawie T. Jemioło., P. Sienkiewicz (red.) *Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa, Teoria walki informacyjne*j, Warszawa 2004.

Państwo może doświadczyć różnego rodzaju zagrożeń mających na celu osłabienie ośrodków władzy. Nie będą to tylko fizyczne ataki na systemy i sieci powodujące zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznych, centrali telefonicznych czy też zakłócenie pracy lub paraliż tych sieci. Walka informacyjna następuje również w

strefie mentalnej poprzez przeprowadzanie chaosu, dezinformacji społeczeństwa oraz wykorzystanie inżynierii społecznej do nakłonienia personelu państwowego do współuczestnictwa w atakach.

Walka informacyjna może być prowadzona zarówno przez podmioty państwowe (na przykład siły zbrojne), ale również podmioty pozapaństwowe, które swoimi działaniami mogą wpłynąć na bezpieczeństwo państwa. Do pierwszej kategorii zaliczyć należy sprawców zagrożeń „systemowych", czyli organizacje państwowe, organizacje terrorystyczne czy też zorganizowane grupy przestępcze. Drugą kategorią są sprawcy zagrożeń „pospolitych", czyli wandale, hakerzy, krakerzy. Podmioty te działają trzyetapowo. Najpierw rozpoznają słabe strony systemu czy też obiektu, następnie uzyskują do niego dostęp, by - w finalnym etapie - spełnić swój cel, jakim może być kradzież, kopiowanie czy też modyfikacja danych[118]. W teorii, najpoważniejszy w swych konsekwencjach mógłby być cyberatak dokonany przez państwo na państwo. Taka forma agresji mogłaby być uznana za napaść w rozumieniu art. 5 Traktatu Północnoatlantyckiego[119], a w konsekwencji doprowadzić do konfliktu międzypaństwowego i działań zbrojnych.

W praktyce jednak sprawcami ataków są częściej podmioty pozapaństwowe niż państwowe. Jest to spowodowane kilkoma czynnikami. Pierwszym jest większa łatwość podjęcia decyzji o ataku (w przypadku służb państwowych decyzja ta jest bardziej sformalizowana, poddana planom, procedurom, podległości służbowej), zdecentralizowana struktura powoduje, iż podjęcie odpowiednich kroków może nastąpić jednostronną decyzją lidera czy wąskiej grupy osób. W przypadku ataku przeprowadzonego przez pojedynczą osobę decyzja o nim może zostać podjęta nawet w wyniku stanu emocjonalnego sprawcy. Drugim jest możliwość osiągnięcia własnych celów. W przypadku podmiotów pozapaństwowych atak elektroniczny niejednokrotnie jest jedynym sposobem realizacji założonych celów. W przypadku podmiotów państwowych wachlarz możliwych działań jest znacznie szerszy. Część teoretyków prawa twierdzi, że państwa dysponują wieloma instrumentami oddziaływania na obce rządy, posługują się atakami elektronicznymi ze znaczną ostrożnością, w obawie przed poważnymi konsekwencjami na arenie

[118] Ibidem, s. 90-92.
[119] Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r., Dz.U.z 2000 r., Nr. 87, poz. 970.

międzynarodowej.[120] Wydaje się jednak, że w obliczu ostatnich wydarzeń nie można zgodzić się z wyrażonym wyżej poglądem. Część państw (zwłaszcza cybermocarstaw takich jak Rosja, Chiny czy USA) dostrzegła ogromny potencjał cyberprzestrzeni. Coraz częściej przestrzeń ta zaczęła być wykorzystywana do realizacji polityki państwa, propagandy, inwigilacji, ale również działań militarnych. Rażącymi przykładami naruszeń ze strony państw były ataki cybernetyczne na Gruzję czy chociażby ingerowanie w sprawy wewnętrzne obcego państwa (jak to miało miejsce w 2016 r.oku w czasie kampanii prezydenckiej pomiędzy Hilary Clinton a Donaldem Trumpem, gdzie prawdopodobnie doszło manipulacji wynikiem wyborczym). Wydaje się, że w przyszłości państwa, kierując się potencjalnymi korzyściami (uzyskanie newralgicznych informacji, tajnych danych, dezinformacja i paraliż przeciwnika) coraz częściej (bardziej lub mniej jawnie) będą wykorzystywać cyberprzestrzeń do realizacji swojej polityki.

Podsumowanie

Czynności podejmowane w przestrzeni wirtualnej mają jak najbardziej realny charakter i mogą oddziaływać nie tylko na stosunki o charakterze elektronicznym. Społeczeństwo informacyjne, a w tym społeczność komputerowa, może mieć ogromny wpływ na działalność państwa. Podzielić należy pogląd Przemysława P. Polańskiego, który podkreślił coraz większą świadomość użytkowników cyberprzestrzeni w zakresie swych praw i obowiązków. Autor stwierdził, że „można jednak zaryzykować tezę, że początek 2012 roku ma szansę przejść do historii prawa jako ważny etap w drodze kształtowania się społeczeństwa informacyjnego, rozumianego jako społeczność użytkowników Internetu. Świadoma swoich praw i dążąca do ustanowienia nowych norm, najlepiej chroniących jej oczekiwania i interesy. Młodzi ludzie wyszli na ulicę największych miast w Polsce i na świcie po to, by protestować przeciwko ACTA i domagać sie prawa do prywatności podczas surfowania w sieci oraz określenia granic inwigilacji ze strony władzy publicznej. Spór ten ujawnił kształtującą sie świadomość prawną i polityczną młodego pokolenia internautów, żądną dookreślenia ram prawnych dla korzystania z dobrodziejstw Internetu. Reakcje rządów

[120] M. Trelikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Trelikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 96-97.

ujawniły słabą znajomość nie tylko oczekiwań młodego pokolenia czy obowiązującego prawa w odniesieniu do Internetu, lecz także brak programu politycznego uwzględniającego rosnące znaczenie społeczeństwa informacyjnego”[121].

Społeczność internetowa jest z całą pewnością formą społeczeństwa informacyjnego. Zagrożenia związane z cyberprzestrzenią nie dają się łatwo zidentyfikować i sklasyfikować w zamknięty katalog. Ciągłe zmiany i rozwój technologii powoduje, że kontrola cyberprzestrzeni staje sie niezwykle trudna. Dynamiczność zmian w tym zakresie skutkuje ogromem wyzwań regulacyjnych. Ogólnoświatowy zasięg Internetu potęguje to zjawisko. Budowa społeczeństwa informacyjnego wymaga stworzenia odpowiedniego zaplecza prawnego. Powinny być to jednak standardy o charakterze międzynarodowym, ponieważ architektura cyberprzestrzeni powoduje, że podjęcie odpowiednich prac na poziomach krajowych będzie niewystarczające do efektywnej i całościowej regulacji zarówno kwestii związanych ze społeczeństwem informacyjnym, jak i potencjalnymi zagrożeniami występującymi w przestrzeni wirtualnej.

[121] P.P. Polański, *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warszawa 2014, s. 4-5.

Rozdział 2

Jurysdykcja państwowa a cyberprzestrzeń

Rzeczywistość wirtualna utworzyła całkowicie nowy obszar działalności człowieka. Cyberprzestrzeń charakteryzuje się aterytorialną naturą, brakiem jednoznacznego powiązania z jednym konkretnym terytorium, a zwłaszcza z określonym terytorium państwowym. Nie jest możliwe wyznaczenie wirtualnych granic, odpowiadających obszarom geograficznym krajów, w których państwo posiada pełne władztwo nad osobami i rzeczami znajdującymi się na ich terytorium. Część autorów proponuje uznanie autonomiczności cyberprzestrzeni na wzór przestrzeni kosmicznej czy morza otwartego. Inni zdecydowanie oponują takiemu podejściu wskazując, że możliwe jest powiązanie działalności człowieka w Internecie z terytorium konkretnego państwa, zwłaszcza w stosunkach gospodarczych[122].

Cyberprzestrzeń w związku ze swoją cyfrową, aterytorialną formą nieuchronnie składnia do zadania pytania o możliwość stosowania prawa w jej obszarze. Dopuszczalność posługiwania się konkretnymi normami prawa jest związana bezpośrednio z kwestią wykonywania władczych uprawnień państwa. Wykonywanie jurysdykcji, jest związane nierozerwalnie terytorium. Kompetencje państwa, co do zasady, są realizowane w określonej przestrzeni i w niej są stosowane[123]. Wobec braku namacalności cyberprzestrzeni bądź jej fizycznych granic podstawowym pytaniem będzie kwestia ustalenia jurysdykcji właściwej w przestrzeni cyfrowej.

Internet stworzył nieograniczony rynek dla działalności handlowej i usługowej. Możliwość zawarcia umowy za pomocą cyberprzestrzeni z kontrahentem znajdującym się na drugim końcem świata stała się codziennością milionów internautów. Wolność gospodarcza, doświadczana dzięki przestrzeni wirtualnej, łączy się jednak z dużym ryzykiem - sprzedażą wadliwych produktów, problemem z wykonaniem umowy, odpowiedzialnością z tego tytułu,

[122] D. Kot, M. Świerczyński, *Prawo właściwe i jurysdykcja krajowa dla stosunków gospodarczych w Internecie*, [w:] J. Barta, R. Markiewicz, *Handel elektroniczny. Prawne problemy*, Kraków 2005, s. 360.
[123] J. Kulesza, *Międzynarodowe …*, s. 24-25.

podwyższonym ryzykiem naruszenia praw własności intelektualnej i w konsekwencji - możliwością bycia pozwanym przed sądem każdego z państw[124].

Kwestia jurysdykcji państwa w odniesieniu do przestrzeni wirtualnej ma kluczowe znaczenie zwłaszcza dla postępowania karnego. Wymiarowi sprawiedliwości, a w szczególności organom ścigania, sporych problemów może nastręczać sytuacja, gdy czyny zakazane przez porządek prawny danego państwa są dokonywane przez osobę lub za pośrednictwem serwera znajdującego się w innym kraju. Podobnie w przypadku przestępstw typowo komputerowych, jak hacking, sabotaż komputerowy czy cyberterroryzm problematyczne okazuje się określenie miejsca popełnienia przestępstwa, gdyż cyberprzestępca może znajdować się w innym kraju i za pomocą laptopa czy telefonu korzystać z bezprzewodowego łącza internetowego lub telefonicznego utrudniającego jego lokalizację.

W rozdziale niniejszym zostanie poruszone zagadnienie jurysdykcji cywilnej oraz karnej w odniesieniu do działalności człowieka w przestrzeni wirtualnej. Przedstawione zostaną akty prawne o charakterze międzynarodowym i regionalnymi, regulacje krajowe państw wybranych odnoszących się do jurysdykcji karnej oraz cywilnej w cyberprzestrzeni.

2.1. Jurysdykcja jako pojęcie prawa - istota

Według Malcolma N. Shaw termin jurysdykcja oznacza: „zdolność państwa do oddziaływania na ludzi, własność oraz okoliczności i stanowi odzwierciedlenie podstawowych zasad: suwerenności państwa, równości państw i nieingerencji w sprawy wewnętrzne. Jurysdykcja jest podstawową i w gruncie rzeczy główną cechą charakterystyczną suwerenności państwa, polega bowiem na korzystaniu z uprawnień do zmieniania, tworzenia lub rozwiązywania stosunków prawnych i wypowiadania zobowiązań”[125]. Vattel jurysdykcję rozumie jako nadanie przez naród swojemu przedstawicielowi uprawnienia do realizowania

[124] D. Karwala, *Dostępność przekazów internetowych jako podstaw jurysdykcji krajowej*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych. Materiały z konferencji*, Warszawa 2008, s. 303.
[125] M.N. Shaw, *Prawo* ... 2006, s. 371.

na określonym obszarze wymiaru sprawiedliwości: sądzenia popełnionych zbrodni i rozstrzygania wynikających tam sporów[126].

Marek Wasiński definiuje jurysdykcję państwową jako „wynikające z koncepcji suwerennej równości uprawnienie państwa do realizowania przezeń jego władczych uprawień: legislacyjnych, jurydycznych i egzekucyjnych względem osób, rzeczy i zjawisk, które władztwu temu podlegają, za pośrednictwem środków znajdujących umocowanie w jego prawie wewnętrznym"[127]. Maciej Siwiński wskazuje z kolei, że „zazwyczaj przez jurysdykcję rozumie się kompetencję państwa do stosowania jego prawa przez ograny sądownicze. Współcześnie pojęcia „jurysdykcja" używa się również w znaczeniu „prawa", „kompetencji" lub „upoważnienia" przysługujących państwu na płaszczyźnie międzynarodowej do stosowania prawa i utrzymania porządku prawnego na swoim terytorium. Na poziomie Unii konflikty jurysdykcyjne są traktowane głównie, jako 'problemy kompetencyjne, a więc dotyczące kwestii, jakie państwo ma prawo do rozstrzygania zawisłej przed nim sprawy w sposób wiążący również inne państwa"[128].

Termin jurysdykcja jest używany zamiennie z określeniem kompetencja. Podkreślić należy, że nie zawsze są to pojęcia tożsame, mające ten sam zakres semantyczny i konotacje. W sprawie *Procecutor v. Tadić*[129] prowadzonej przed Międzynarodowym Trybunałem Karnym dla byłej Jugosławii (MTKJ) podjęto próbę rozróżnienia obu wskazanych wyżej terminów. Stwierdzono, że: „pojęcie „kompetencji" jest węższe i bardziej techniczne oraz odnosi się zazwyczaj jedynie do określonych aspektów jurysdykcji (np. *ratione temporis, loci, personae, materiae*). Zakres materialny terminu 'jurysdykcja' nieść miałoby natomiast za sobą pełniejszy ładunek pojęciowy, czerpiąc z łacińskiego źródłosłowia *jurisdictio* oznaczającego uzasadnione władztwo 'oznajmienie prawa' (ang. *state the law,* fr. *dire le droit*) w określonym zasięgu i sferze, w sposób autorytatywny i ostateczny. Komplikacje te powodują, że ze

[126] E. de Vattel, *Prawo narodów, czyli zasady prawa naturalnego zastosowane do postępowania i spraw narodów i monarchów* (tłum. B. Winiarski), Warszawa 1958, s. 377.
[127] M. Wasiński, *Jurysdykcja legislacyjna państwa w prawie międzynarodowym publicznym*, „Państwo i Prawo" 2002, nr 3, s. 57.
[128] M. Siwicki, *Podstawy określenia jurysdykcji w sprawach cyberprzestępstw w UE*, „Europejski Przegląd Sądowy" 2013, nr 9, s. 21.
[129] Wyrok Międzynarodowego Trybunału Karnego dla byłej Jugosławii z 15 lipca 1999 r., *Procecutor przeciwko Tadić*, sygn. akt IT-94-1-A.

względu na bliskość semantyczną tych pojęć dokonuje się czasem ich syntezy, używając określenia kompetencje jurysdykcyjne”[130].

Jurysdykcja państwowa opiera się w głównej mierze na możliwości władczego kształtowania sytuacji prawnej i faktycznej osób oraz przedmiotów znajdujących się na terytorium danego państwa. Nie jest to jednak uprawnienie absolutne, gdyż prawo to ograniczone jest przez suwerenne prawa terytorialne innych państw. Uprawienie do wykonywania jurysdykcji nie jest ukształtowane zupełnie dowolnie. Podnosi się w doktrynie, że „jurysdykcja przysługuje danemu państwu, jeżeli pomiędzy określoną osobą, jej zachowaniem czy też skutkiem określonego zachowania występuje łącznik jurysdykcyjny, dający państwu uprawnienie stosowania ustanowionego prawa. Takim łącznikiem mogą być terytorium lub związek personalny (np. obywatelstwo, domicyl). W doktrynie nie ma jednak zgody co do tego, czy państwo jest ograniczone przy określeniu władzy jurysdykcyjnej do konieczności wykazania jakiegoś powiązania ze swoim terytorium. W szczególności poddaje się w wątpliwość, czy jurysdykcja państwa realizowana na jego terytorium jest wyłączna i absolutna. Szczególnie problematyczna jest kwestia kompetencji państwa do stosowania swojego prawa do spraw obejmujący element zagraniczny, m.in. ze względu na problem podziału kompetencji pomiędzy państwami”[131]. Jeszcze więcej problemów nastręcza określenie jurysdykcji w przestrzeni wirtualnej. Tradycyjnie stosowane łączniki jurysdykcyjne wydają się być nieodpowiednie i niewystarczające w nowym wirtualnym świecie.

Ewentualne konflikty jurysdykcyjne mogą być rozwiązywane w dwojaki sposób. Pierwszy z nich ma na celu zapobieganie powstawaniu sporów przez niedopuszczanie do powstawania stref pokrywających się kompetencji państwa. Drugim możliwym kierunkiem jest likwidowanie już powstałego konfliktu jurysdykcyjnego. Michał Płachta stoi na stanowisku, iż jedynym słusznym rozwiązaniem jest druga ze wskazanych metod, która wydaje się niezbędna w efektywnym zwalczaniu przestępczości[132]. Autor poruszając problem jurysdykcji karnej stanął stanowisku, że „działania zmierzające do znalezienia optymalnego rozwiązania tych problemów mogą być podejmowane w dwóch płaszczyznach:

[130] T. Ostropolski, *Zapobieganie sporom o jurysdykcję w Unii Europejskiej i ich rozstrzyganie*, [w:] A. Grzelak (red.), *Europejskie prawo karne*, Warszawa 2012, s. 93.
[131] M. Siwicki, *Podstawy …*, s. 21.
[132] M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: pojęcie, geneza i środki zaradcze*, „Prokuratura i Prawo” 2010, nr 11, s. 14.

A. w warstwie kompetencji[133] poprzez:

a_1) ścisłą delimitację (»dopasowanie«) stref kompetencyjnych poszczególnych państw,

a_2) ograniczenie kompetencji w sprawach o przestępstwa popełnione przez cudzoziemców za granicą,

B. w warstwie jurysdykcyjnej[134] poprzez:

b_1) wykonywanie jurysdykcji na podstawie ustalonej 'hierarchii' zasad kompetencyjnych,

b_2) rezygnację z wykonywania jurysdykcji:

- przekazanie ścigania za granicę,
- obowiązywanie reguły *ne bis in idem*,
- oportunizm ścigania,

b_3) podział jurysdykcji pomiędzy dwoma państwami w jednej sprawie (przekazanie wyroku do wykonania za granicę)

b_4) stosowanie obcego prawa karnego,

b_5) bezpośrednie porozumienie organów ścigania i organów sądowych zainteresowanych państw w celu optymalizacji jurysdykcji w konkretnej sprawie."[135]

Jurysdykcja nie jest prawem absolutnym i podlega pewnym ograniczeniom wynikającym z prawa międzynarodowego takim, jak immunitety dyplomatyczne.

2.1.1 Obszary jurysdykcji

Jurysdykcja może przyjąć kilka form. Są to: uprawnienie państwa do wiążącego sądowego rozstrzygania indywidualnych spraw (jurysdykcja sądownicza), kompetencja jurysdykcyjna ustawodawcza przejawiająca się możliwością dowolnego stanowienia prawa obowiązującego na danym terytorium oraz kompetencja do egzekucji prawa ustanowionego, czyli jurysdykcyjna kompetencja wykonawcza.

---

[133] Jako warstwę kompetencji (ustawodawczej) M. Płachta rozumie procesowe rozstrzygniecie, prawo którego państwa należy zastosować w przypadku konfliktu jurysdykcyjnego. Wskazuje on ponadto, iż kompetencja ze swej istoty ma charakter personalny, zob. M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: pojęcie …*, s. 7.

[134] Jako warstwę jurysdykcyjną M. Płachta rozumie procesowe wskazanie, który z organów kilku państw jest uprawniony do prowadzenia postępowania karnego w przypadku wystąpienia konfliktu jurysdykcyjnego. Podkreśla się przy tym, iż jurysdykcja ma charakter głównie terytorialny, zob.: M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: pojęcie …*, s. 7.

[135] Ibidem, s. 14.

Antonio Cassese podnosi, iż jurysdykcja jako pierwsze suwerenne uprawnienie państwa może się wyrażać w trzech różnych formach:

- jurysdykcji do rozstrzygania (ang. *jurisdiction to adjudicate*) - uprawniającej do wydawania wiążących rozstrzygnięć sądowych czy administracyjnych oraz przyznająca możliwość wykładni i interpretacji prawa stanowionego,
- jurysdykcji ustawodawczej (ang. *jurisdiction to prescribe*) - dającej możliwość nakładania obowiązków lub przyznawania uprawnień jednostkom znajdującym się w granicach zwierzchnictwa terytorialnego państwa,
- jurysdykcja w egzekwowaniu (ang. *jurisdiction to enforce*) - uprawnienie do wyegzekwowania prawa ustanowionego i ewentualnego zastosowania środków przymusu[136].

Jurysdykcja ustawodawcza odnosi się do zwierzchnictwa konstytucyjnie ustanowionych organów państwowych tworzących prawo wiążące na danym terytorium. Nie należy jednak zapominać, że tworzone w ten sposób akty prawa mogą w pewnych okolicznościach być również stosowane poza granicami państwa forum. Kompetencja państwa do wyłącznego regulowania określonych kwestii wyraża się m.in. w możliwości stworzenia reguł proceduralnych wiążących organy wymiaru sprawiedliwości. Normy te jednakże w żaden sposób nie wypływają na prawo czy też możliwość ich egzekucji w państwach trzecich. Prawo międzynarodowe dopuszcza możliwość nakładania zobowiązań na podmioty zagraniczne, o tyle o ile istnieje pomiędzy nimi a państwem jakiś łącznik faktyczny czyli na przykład domicyl czy posiadanie nieruchomości w obrębie terytorium państwa forum[137].

Jurysdykcja wykonawcza określa granicę działania prawa. Z zasady niezależności, równości i suwerenności terytorialnej wynika generalna zasada, iż żadne państwo nie może wykonywać swoich kompetencji władczych na obcej ziemi i nie może narzucać i egzekwować swojego prawa w innym państwie[138]. Jurysdykcja w egzekwowaniu prawa ma charakter niemal wyłącznie terytorialny, dopuszczający jednakże pewne wyjątki, w

[136] A. Cassese, *International Law*, Oxford 2005, s. 49-50.
[137] M. N. Shaw, *International Law*, Cambrige, 2008, s. 649-650.
[138] Ibidem, s. 650-651.

przypadku uzyskania zgody innego państwa na wykonanie czynności jurysdykcyjnych na swoim terytorium przez państwo obce[139].

2.1.2 Jurysdykcja cywilna

Jurysdykcja cywilna ma znacznie szerszy zakres niż jurysdykcja karna. Cechą charakterystyczną różnicującą te dwie formy kompetencji jest to, iż stosunki publicznoprawne, a więc te znajdujące się w bezpośredniej sferze zainteresowania państw, są oparte na podporządkowaniu się podmiotu państwu, a więc są połączone z uprawnieniem władzy do stosowania środków przymusu. Stosunki cywilne - prywatnoprawne są oparte na zasadach wolności i równości stron. Co więcej, stronom stosunku zobowiązaniowego przyznana została możliwość dowolnego kształtowania swoich relacji, więc również wyboru prawa właściwego do stosowania w przypadku wystąpienia ewentualnych sporów.

Głównym zadaniem jurysdykcji cywilnej jest rozgraniczenie strefy działania poszczególnych krajów w stosunkach cywilnych, gospodarczych, rodzinnych czy związanych z prawem pracy, gdzie stronami są osoby fizyczne i prawne. W przypadku jurysdykcji karnej naruszenie przepisów krajowej ustawy karnej powoduje konieczność reakcji władz państwowych. Uważa się, że czynem przestępczym sprawca nie tylko naruszył dobra ofiary, ale również państwa, zakłócając porządek społeczny. Kolejną różnicą jest fakt, iż strony stosunków cywilnych mogą wybrać prawo właściwe. Możliwość taka jest niedopuszczalna w przypadku czynów o charakterze karnym[140].

Jurysdykcja cywilna może być rozpatrywana w aspekcie podmiotowym i przedmiotowym. Aspekt podmiotowy przepisów jurysdykcyjnych rozstrzyga o tym, kto może być pozwany, a kto nie podlega władztwu określonego sądu krajowego. Aspekt przedmiotowy norm jurysdykcyjnych rozstrzyga, w jakich sprawach sądy krajowe są właściwe i mogą wydać prawomocne orzeczenie w sprawie[141]. Problemem, z którym można się spotkać w praktyce jest negatywny konflikt jurysdykcyjny nazywany też negatywnym sporem kompetencyjnym. Mianem tym określa się w międzynarodowym postępowaniu cywilnym sytuacje, gdy osoba zainteresowana nie może w konkretnej sprawie uzyskać

[139] T. Ostropolski, *Zapobieganie …*, s. 94-95.
[140] Ibidem, s. 96-97.
[141] A. Torbus, *Umowa jurysdykcyjna w systemie międzynarodowego postępowania cywilnego*, Toruń 2012, s. 44-45.

ochrony prawnej w żadnym z państw, w którym sprawa mogłaby się toczyć, ponieważ każdy sąd uznaje się za niewłaściwy do rozpoznania sprawy[142].

2.1.2.1. Zasady jurysdykcji cywilnej

Właściwość sądów cywilnych ustala się na podstawie właściwości rzeczowej, miejscowej bądź funkcjonalnej. Właściwość miejscowa oraz rzeczowa ustala zakres spraw, które mogą być rozpatrywane przez dany sąd. Właściwość rzeczowa rozstrzyga o kategorii rozpatrywanych spraw przez sądy pierwszej instancji, ale różnego rzędu w oparciu np. ustalony katalog spraw bądź wartość przedmiotu sporu. Właściwość ta jest stosowana w państwach, w których, tak jak w Polsce nie ma jednolitego systemu sądów pierwszej instancji (w Polsce rolę tę pełnią zarówno sądy rejonowe jak i sądy okręgowe). Z kolei właściwość miejscowa rozstrzyga o tym, w którym okręgu położony sąd, który winien rozstrzygnąć spór. Właściwość miejscową należy podzielić na właściwość ogólną, przemienną i wyłączną. Właściwość ogólna określa ogólne zasady rozstrzygające sąd właściwy do rozstrzygnięcia sprawy, gdy brak jest przepisów szczególnych. Właściwość przemienna z kolei umożliwia wybór sądu pomiędzy kilkoma sądami wskazanymi w ustawie. Właściwość wyłączna wskazuje konkretny sąd, który będzie wyłącznie właściwy do rozstrzygnięcia danej sprawy (np. w sprawach dotyczących nieruchomości). Właściwość funkcjonalna oznacza zakres czynności pełnionych przez dany sąd (rozpoznawanie środków zaskarżenia, udzielanie pomocy sądowej)[143].

Ogólną zasadą stosowaną również w innych porządkach prawnych jest przyjęcie, że powództwo wytacza przed sądem miejsca zamieszkania lub siedziby pozwanego. Rozwiązanie to jest wygodne dla osoby, która może być pozwany, ponieważ wszelkie ewentualne spory związane z jej czynnościami są rozstrzygane według prawa miejsca zamieszkania danej osoby - w więc prawa jej znanego. Nieco inną konstrukcję przyjmuje się zazwyczaj przy umowach zawieranych z konsumentem. Prawodawcy krajowi i europejscy uznają konsumenta za słabszą stronę stosunku zobowiązaniowego. Wobec czego, w

[142] T. Ereciński, *Kilka uwag o tzw. jurysdykcji koniecznej*, [w:] L. Ogiełła, W. Popiołek (red.), *Księga pamiątkowa Profesora Maksymiliana Pazdana*, Kraków 2005, s. 65.
[143] I. Kunicki, *Podmioty procesu*, [w:] W. Broniewicz, A. Marciniak i in., *Postępowanie cywilne w zarysie*, Warszawa 2014, s. 122-130.

stosunkach umownych z udziałem konsumentów powództwo wytacza się w miejscu zamieszkania powoda - konsumenta.

W wielu porządkach prawnych przyjęto wyłączną jurysdykcję cywilną. Ustawodawcy zazwyczaj uznają, iż danemu państwu przysługuje wyłączne władztwo w stosunkach określonego rodzaju. Zazwyczaj będą to sprawy związane z nieruchomościami położonymi w obszarze ich właściwości miejscowej czy spraw enumeratywnie wymienionych w ustawie. W polskim porządku prawnym, oprócz spraw związanych z nieruchomościami, wymienia się sprawy dotyczące dziedziczenia, członkostwa w spółdzielni, stowarzyszeniu bądź spółce, w sprawach małżeńskich oraz w sprawach pomiędzy rodzicami i dziećmi[144].

Powszechną praktyką państw jest przyjmowanie w ustawodawstwie krajowym norm kolizyjnych między innymi dotyczących zobowiązań umownych. Najczęściej stosowanym łącznikiem jurysdykcyjnym jest łącznik miejsca zawarcia umowy. Inne łączniki powiązane są z miejscem wykonania zobowiązania, miejscem świadczenia usługi, czy też miejscem dostarczenia towaru. W przypadku wątpliwości lub właściwości kilku sądów przyjmuje się, że sądem właściwym będzie ten, który ma najściślejszy związek z zobowiązaniem. Mimo istnienia szeregu zasad jurysdykcyjnych nie należy pominąć podstawowej zasady autonomii woli stron i swobody kontraktowania, która uprawniania strony do wyboru prawa właściwego według własnego uznania. Wybór prawa przez strony jest nazywany również umową jurysdykcyjną lub klauzulą jurysdykcyjną[145].

Zawarcie w umowie klauzuli jurysdykcyjnej jest najlepszym sposobem uniknięcia sporu jurysdykcyjnego w przyszłości. Nie oznacza to, że wybór prawa właściwego nie mógłby nastąpić w inny sposób na przykład dorozumiany wynikający z postanowień umowy lub okoliczności faktycznych wykonania zobowiązania. W doktrynie podkreśla się jednak, że w przypadku umów zawieranych w przestrzeni wirtualnej nie można domniemywać wyboru prawa właściwego tylko na podstawie wyboru przez nabywcę określonej wersji językowej strony internetowej czy też regulaminu sprzedaży *on-line*. Umowa jurysdykcyjna może być zawarta w stosunku do całej umowy, jej części, zarówno przed jak i po jej zawarciu, z uwzględnieniem jednakże przepisów bezwzględnie obowiązujących (na przykład ochrony

[144] E. Marszałkowska-Krześ, *Właściwość sądu*, [w:] E. Marszałkowska - Krześ (red.), *Postępowanie cywilne*, Warszawa 2013, s. 104.
[145] M. Świerczyński, *Jurysdykcja krajowa i prawo właściwe a Internet,* [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007, s. 135.

konsumentów w przypadku umów zawieranych na odległość)[146]. Wybranie prawa właściwego przez strony jest rozwiązaniem trafniejszym niż pozostawienie wyboru sądu jedynie powodowi, który mógłby szukać jurysdykcji i prawa najbardziej nań korzystnego. Poszukiwanie prawa najkorzystniejszego dla strony nazywane jest *forum shopping*. Zaakcentować w tym miejscu należy, iż umowy jurysdykcyjnej nie można stosować w sprawach, w których zastrzeżona jest właściwość wyłączna.

Spory kompetencyjne w cyberprzestrzeni mogą wyniknąć nie tylko na podstawie licznych umów cywilnoprawnych, ale również z powodu czynów pozaumownych, czyli deliktów pozaumownych. Za delikty elektroniczne można uznać „zarówno takie czyny niedozwolone, w przypadku których w procesie wyrządzania szkody korzystano z komunikacji elektronicznej, jak również te, w których zdarzenie powodujące szkodę polegało na uniemożliwianiu prawidłowego korzystania ze sprzętu, w tym ze środków komunikacji elektronicznej, a więc dobra zasługującego na ochronę prawną"[147]. Delikty wewnętrzne są związane ze między innymi ze specyfiką komunikacji elektronicznej. Do elektronicznych deliktów wewnętrznych zaliczyć trzeba rozpowszechnianie wirusów, włamania komputerowe czy świadome wpływanie na system komputerowy w celu przesyłania danych. Czyny te są jednak ściśle związane z odpowiedzialnością karną, wobec której nie opracowano jak dotąd ujednoliconego systemu prawnego. Wprowadzenie więc zunifikowanego systemu odpowiedzialności cywilnej uzależnione jest poniekąd od wcześniejszego ujednolicenia zasad jurysdykcji karnej[148].

Nie został opracowany jeden międzynarodowy akt prawny holistycznie regulujący zagadnienie jurysdykcji cywilnej. Konieczne jest zatem posiłkowanie się ogólnymi normami kolizyjnymi, przy uwzględnieniu osobliwego charakteru cyberprzestrzeni. „Internet wymaga (...) zmiany tradycyjnych poglądów odnośnie do pozycji stron stosunku zobowiązaniowego. Pojawia się bowiem pytanie, czy ze względu na możliwości, jakie daje Internet, np. dostępu do olbrzymiej ilości ofert, rozbudowanych narzędzi wyszukiwania i przetwarzania danych, pozycja strony tradycyjnie uznawanej za słabszą (np. konsumenta czy poszkodowanego) nie jest zdecydowanie mocniejsza niż w tradycyjnym obrocie, czemu sprzyjać może *forum shopping* tj. kierowanie pozwu przez nią nie do sądu zapewniającego najszybsze i

[146] Ibidem, s. 137.
[147] A. Całus, *Szansa unifikacji prawa właściwego dla zobowiązań z "deliktów elektronicznych" w ramach Unii Europejskiej*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych. Materiały z konferencji*, Warszawa 2008, s. 125.
[148] Ibidem, s. 144.

najsprawniejsze rozstrzygniecie, ale do sądu, który zapewni korzystniejsze rozstrzygnięcie"[149].

Aterytorialny charakter cyberprzestrzeni znacznie utrudnia wskazanie krajowego sądu właściwego w przypadku wystąpienia sporu w przestrzeni wirtualnej. W celu ustalenia jurysdykcji właściwej można wykorzystać jedną z następujących metod. Pierwszą z nich jest możliwość zastosowania przepisów ogólnych zawartych między innymi w Konwencji wiedeńskiej Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów[150] z dnia 11 kwietnia 1980 r. (Konwencja wiedeńska z 1980 r.) Wskazany akt prawny może być jednakże stosowany wyłącznie w odniesieniu do obrotu pomiędzy przedsiębiorcami. Można również posiłkować się normami kolizyjnymi prawa prywatnego międzynarodowego oraz normami jurysdykcyjnymi wskazującymi właściwość sądów danego kraju. [151] Innymi modelami będą przepisy międzynarodowych aktów prawnych, znajdujące się w konwencji lugańskiej[152], rozporządzeniu Rady i Parlamentu Europejskiego nr 1215/2012[153], rozporządzeniach Rzym I[154] i Rzym II[155] bądź w wiążących Polskę umowach bilateralnych o jurysdykcji krajowej i prawie właściwym.

2.1.2.2. Regulacje globalne

Globalny zasięg sieci internetowej powoduje, że prowadzone w cyberprzestrzeni działania nie mogą być podporządkowane czy też kontrolowane tylko przez jedno państwo. Coraz większa liczba umów zawieranych za pośrednictwem Internetu spowodowała, że koniecznym jest określenie prawa właściwego do rozstrzygnięcia możliwego sporu.

[149] M. Świerczyński, *Jurysdykcja …*, s. 117.
[150] Konwencja Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów, sporządzona w Wiedniu dnia 11 kwietnia 1980 r., Dz. U. z 1997 r. Nr 45, poz. 286.
[151] M. Świerczyński, *Jurysdykcja …*, s. 114-115.
[152] Konwencja o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń sądowych w sprawach cywilnych i handlowych podpisana w Lugano 30 października 2007 roku, Dz.Urz. UE L 147 z 10.06.2009 r.
[153] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, Dz.U. L 351 z 20.12.2012.
[154] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I), Dz.U. L 177 z 4.7.2008.
[155] Rozporządzenie (WE) nr 864/2007 Parlamentu Europejskiego i Rady z dnia 11 lipca 2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych (Rzym II), Dz.U. L 199 z 31.7.2007.

Konwencja Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów

Konwencja Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów, sporządzona w Wiedniu 11 kwietnia 1980 roku ma zastosowanie do umów sprzedaży towarów między stronami, które mają swoje siedziby w różnych krajach. Przy określaniu zakresu jej stosowania nie bierze się pod uwagę przynależności państwowej stron, ich statusu cywilnoprawnego ani handlowego. Ma ona zastosowanie wyłącznie w obrocie dwustronnie profesjonalnym. Artykułem 2 wyłączono jej stosowanie w stosunku do sprzedaży z udziałem konsumentów, sprzedaży m.in. na licytacji, akcji, papierów wartościowych czy sprzedaży energii.

Zgodnie z art. 10 konwencji wiedeńskiej z 1980 r., jeżeli strona ma więcej niż jedną siedzibę, za miejsce siedziby rozumie się to miejsce, które ma najściślejszy związek z umową i jej wykonaniem. Jeżeli jednak jedna ze stron nie posiada siedziby handlowej, przyjmuje się miejsce stałego zamieszkania kontrahenta. Konwencja nie będzie miała zastosowania, gdy fakt posiadania przez strony siedzib handlowych w różnych krajach nie wynikał z umowy czy też jakichkolwiek informacji czy stosunków handlowych ujawnionych przed zawarciem umów.

Konwencja wiedeńska z 1980 r. zawiera postanowienia o charakterze materialnoprawnym, można jednak w niej wyróżnić postanowienia o charakterze kolizyjnoprawnym. Artykuł 1 ust. 1 pkt. b) stanowi, że konwencja ma zastosowanie do umów sprzedaży towarów miedzy stronami mającymi siedziby handlowe w różnych państwach jeżeli normy międzynarodowego prawa prywatnego jako prawo właściwe wskazują prawo państwa strony konwencji. Również w art. 7 ust 2 wskazano, że kwestie które nie są w sposób wyraźny uregulowane w konwencji będą rozstrzygane według ogólnych zasad na których opiera się konwencja, a wobec ich braku przez normy międzynarodowego prawa prywatnego.

Konwencja z Lugano

Gdy konwencja o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń sądowych w sprawach cywilnych i handlowych z 1988 r. podpisana w Lugano (konwencja lubańska z

1998 r.) przestała odpowiadać nowoczesnym standardom, konieczne stało się zharmonizowanie standardów jurysdykcyjnych i wprowadzenie zmian, których konieczność była sygnalizowana w orzecznictwie Trybunału Sprawiedliwości (TS). Wynikiem prac Wspólnoty Europejskiej (obecnie UE)[156] było przygotowanie i ogłoszenie w grudniu 2007 roku nowej Konwencji o jurysdykcji i uznawaniu orzeczeń sądowych w sprawach cywilnych i handlowych (nowa konwencja lugańska lub konwencja lugańska). Konwencja lugańska w 28 marca 2007 roku została parafowana w Brukseli, a następnie zatwierdzono w imieniu Wspólnoty podpisanie Konwencji decyzją Rady z dnia 15 października 2007 r.[157] Konwencja obowiązuje pomiędzy UE, Królestwem Danii, Republiką Islandii, Królestwem Norwegii i Konfederacją Szwajcarską.

Nowa konwencja lugańska weszła w życie 1 stycznia 2010 roku z uwagi na złożenie dokumentów ratyfikacyjnych przez Wspólnotę Europejską 18 maja 2009 roku, Norwegię 1 lipca 2009 roku oraz Danię w 24 września 2009 roku. Ponadto, Konwencja weszła w życie również między Unią Europejską a Konfederacją Szwajcarską w dniu 1 stycznia 2011 r. oraz pomiędzy Unią Europejską a Islandią 1 maja 2011 roku[158]. Zgodnie z art. 69 ust 7 nowa konwencja lugańska zastąpiła pomiędzy państwami członkowskimi WE konwencję brukselską z 1986 roku oraz protokół luksemburski w sprawie wykładni Europejskiego Trybunału Sprawiedliwości z 1971 roku co do terytoriów pozaeuropejskich państw członkowskich, w stosunku do których nowa konwencja po jej wejściu w życie jest otwarta do przystąpienia[159].

Konwencja lugańska jako podstawową zasadę jurysdykcyjną wprowadza zasadę jurysdykcji ogólnej stanowiącą, że sądem właściwym do rozpoznania sprawy jest sąd miejsca zamieszkania lub siedziby pozwanego. Narodowość pozwanego nie odgrywa żadnej roli w ustaleniu jurysdykcji właściwej do rozstrzygnięcia sporu. Ustęp 2 art. 1 stanowi, że konwencja będzie miała zastosowanie również w stosunku do osób, które nie posiadają obywatelstwa państwa, w którym zamieszkują, jeżeli państwo to jest stroną konwencji.

[156] Wspólnota Europejska została powołana do życia 1 stycznia 1958 na mocy traktatów rzymskich jako Europejska Wspólnota Gospodarcza (EWG), Reformujący instytucje unijne Traktat lizboński z 2007 wprowadził istotne zmiany. Unia Europejska nabyła osobowość prawną i zastąpiła Wspólnotę Europejską, przejmując wszystkie jej kompetencje. Wraz z wejściem traktatu w życie 1 grudnia 2009 Wspólnota przestała istnieć.

[157] Decyzja Rady z 15.10.2007 r. dotycząca podpisania Konwencji lugańskiej o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń w sprawach cywilnych i handlowych (2007/712/WE), Dz.Urz. UE z 2007 r., nr. K 339.

[158] Oficjalna baza aktów prawnych Unii Europejskiej //eur-lex.europa.eu/legal-content/PL/TXT/?qid=1436791024801&uri=CELEX:22011X0526(01) [12.07.2015].

[159] P. Mostownik, M. Niedźwiedź, *Druga konwencja lugańska o jurysdykcji oraz uznawaniu i wykonywaniu obcych orzeczeń w sprawach cywilnych*, „Kwartalnik Prawa Prywatnego" 2006, z. 4, s. 1013.

Kolejne postanowienia poruszają problem jurysdykcji szczególnej, którą wprowadza się w określonych przypadkach, spośród których w tym miejscu wymienić należałoby tylko te, które mogą mieć zastosowanie do cyberprzestrzeni. Osoba, która ma miejsce zamieszkania na terytorium państwa związanego z konwencją lubańską (art. 5, ust. 1, pkt 1, 2, 4), może być pozwana w innym państwie związanym niniejszą konwencją:

- gdy przedmiotem postępowania jest umowa lub roszczenia wynikające z umowy - przed sąd miejsca, gdzie zobowiązanie zostało wykonane albo miało być wykonane. Jako miejsce wykonania zobowiązania rozumieć należy - w przypadku sprzedaży rzeczy ruchomych - miejsce, w którym rzeczy te zgodnie z umową zostały dostarczone albo miały być dostarczone, a w przypadku świadczenia usług - miejsce, w którym usługi zgodnie z umową były świadczone albo miały być świadczone,
- gdy przedmiotem postępowania jest czyn niedozwolony lub czyn podobny do czynu niedozwolonego albo roszczenia wynikające z takiego czynu - sąd miejsca, gdzie nastąpiło lub może nastąpić zdarzenie wywołujące szkodę,
- w sprawach roszczeń o odszkodowanie lub przywrócenie stanu poprzedniego, które wynikają z czynu zagrożonego karą - przed sąd karny, do którego wniesiono akt oskarżenia, o ile sąd ten może według swojego prawa rozpoznać roszczenia cywilnoprawne.

Nie ulega wątpliwości, iż rozwój cyberprzestępczości stworzył potrzebę regulacji tematyki kolizyjnoprawnej w zakresie deliktów internetowych. Internetowe zobowiązania deliktowe powstają *ex lege* w wyniku wyrządzenia szkody za pomocą przestrzeni wirtualnej. Wskazany przepis w pkt 2 wprowadza łącznik przedmiotowy - tj. miejsca zdarzenia wywołującego szkodę - rozumianego jako miejsce w którym szkoda nastąpiła (skutek), ale też jako miejsce czynu niedozwolonego wywołującego szkodę. Takie rozszczepienie stanu faktycznego deliktu, nazywane również wielomiejscowością deliktu, uważane jest w doktrynie za charakterystyczne dla cyberprzestrzeni. Za miejsce działania sprawcy w przestrzeni wirtualnej można zatem uznać miejsce, z którego sprawca działał, np. udostępniając dane czy wprowadzając określone treści do sieci komputerowej[160].

Zauważyć należy, iż art. 6 ust. 1 uszczegóławia zasady jurysdykcji szczególnej wskazując, iż w przypadku pozwania kilku osób sądem właściwym będzie sąd miejsca, w którym ma miejsce zamieszkania jeden z pozwanych, o ile między sprawami istnieje tak

[160] M. Świerczyński, *Jurysdykcja …*, s. 126-128.

ścisła więź, że pożądane jest ich łączne rozpoznanie i rozstrzygnięcie w celu uniknięcia wydania w oddzielnych postępowaniach sprzecznych ze sobą orzeczeń.

Wprowadzenie wyżej wymienionych postanowień dotyczących jurysdykcji szczególnej odzwierciedla zasadę prowadzenia efektywnego postępowania przed sądem właściwym ze względu na szczególny związek ze sprawą. Uregulowania takie umożliwiają łatwiejsze przeprowadzenie i gromadzenie dowodów, prowadzenie postępowania sądowego, więc również przyśpiesza proces i daje gwarancję ochrony stron.

Konwencja lugańska wprowadza zasadę jurysdykcji ochronnej w stosunku do umów zawieranych z udziałem konsumentów, czyli umowy sprzedaży na raty rzeczy ruchomych, umowy pożyczki oraz w każdym innym przypadku, gdy stroną stosunku jest konsument (art. 15-17). We wskazanych przypadkach traktat pozostawia wybór sądu konsumentowi. Może on wybrać sąd swojego miejsca zamieszkania, bądź też sąd właściwy dla siedziby jego kontrahenta. Wyboru takiego nie pozostawiono drugiej stronie umowy. Artykułem 16 ust. 2 kontrahent konsumenta został zobowiązany do wytoczenia powództwa przeciwko konsumentowi zawsze przed sądem właściwym ze względu na miejsce zamieszkania konsumenta. Taka regulacja ma na celu ochronę słabszej strony umowy, jaką jest osoba fizyczna - konsument. Pozostawienie wyboru sądu właściwego konsumentowi może mieć szczególne znaczenie w przypadku umów zawieranych na odległość za pomocą Internetu, czy też ogólnie pojętego handlu elektronicznego. Co istotne, podkreśla się, że „aby art. 15 ust 2 lit c) mógł być stosowany, nie jest wystarczające to, że przedsiębiorstwo kieruje swoją działalność do państwa członkowskiego, które jest miejscem zamieszkania konsumenta, lub do kilku państw członkowskich włącznie z tym państwem; oprócz tego umowa musi zostać zawarta w ramach działalności tego przedsiębiorstwa. Przepis ten odnosi się do niektórych metod marketingowych, w tym do umów zawieranych na odległość przez Internet. W tym kontekście Rada i Komisja podkreślają, że sam fakt dostępności strony internetowej nie jest wystarczający, by art. 15 miał zastosowanie; warunkiem jest to, by ta strona internetowa umożliwiała zawieranie umów na odległość i by taka umowa została rzeczywiście zawarta na odległość w dowolny sposób. W tym zakresie ani język, ani waluta używane na stronie internetowej nie mają znaczenia”[161]. Zastrzeżenie to jest tożsame do regulacji wprowadzonej w rozporządzeniu Rzym I.

[161] Wspólna deklaracja Rady i Komisji dotycząca art. 15 rozporządzenia (WE) nr 44/2001, której tekst dostępny jest w: F. Pocara, *Sprawozdanie objaśniające Konwencję o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń*

Artykuł 23 nowej konwencji lugańskiej przewiduje możliwość zawarcia umowy jurysdykcyjnej, na mocy której strony uzgadniają, że wszelkie spory już wynikłe albo te mogące wyniknąć w przyszłości będą rozstrzygane przez wskazany w umowie sąd właściwy. Umowa taka winna zostać sporządzona w formie pisemnej. Ustęp 2 omawianego artykułu uznaje za elektroniczne przekazy umożliwiające trwały zapis umowy za równoważny formie pisemnej. Fausta Pocara wskazuje, że: „umowa dotycząca jurysdykcji jest dorozumiana na korzyść sądu, który w przeciwnym przypadku na mocy konwencji nie miałby jurysdykcji, jeżeli powód występuje do tego sądu, a pozwany poddaje się jego jurysdykcji bez jej kwestionowania; to postanowienie tym różni się od umowy dotyczącej jurysdykcji, o której mowa w art. 23, że nie zakłada porozumienia między stronami i nie zobowiązuje sądu do zbadania, czy klauzula przyznająca mu jurysdykcję była w rzeczywistości przedmiotem obopólnej zgody”[162].

2.1.2.3. Regulacje regionalne na przykładzie Unii Europejskiej

Rzym I

Konwencja o prawie właściwym dla zobowiązań umownych (konwencja rzymska)[163] regulowała kwestie zobowiązań umownych, które wykazują związek z prawem różnych państw. Konwencja rzymska została zastąpiona między państwami członkowskimi Unii Europejskiej rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 593/2008 w sprawie prawa właściwego dla zobowiązań umownych (Rzym I). W trakcie prac nad projektem rozporządzenia dyskutowano o możliwości rozszerzenia jego zakresu o przepisy

sądowych w sprawach cywilnych i handlowych, podpisaną w Lugano w dniu 30 października 2007 r., s. 63, http://bip.ms.gov.pl/Data/Files/_public/bip/lugano/raportpocara_2.pdf, [13.07.2015].

[162] Ibidem.

[163] Konwencja o prawie właściwym dla zobowiązań umownych, otwarta do podpisu w Rzymie dnia 19 czerwca 1980 r., Dz.Urz UE C 169, z 08.07.2005 r.

dotyczące umów elektronicznych, jednakże ostatecznie zapisy takie nie znalazły się w rozporządzeniu[164].

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 jest fundamentem unijnego prawa kolizyjnego określającym kluczowe przesłanki pozwalające ustalić prawo właściwe dla danego stosunku umownego[165]. Rzym I jest stosowany w sprawach cywilnych i handlowych powiązanych z prawem różnych państw, w tym państw trzecich. Michał Bienias wskazuje, że dotyczy to też państw spoza obszaru Unii, a „stosowanie rozporządzenia nie jest więc uzależnione od powiązania zobowiązania umownego choćby z jednym państwem członkowskim Unii. Postanowienia rozporządzenia należy więc stosować w Polsce przy poszukiwaniu prawa właściwego dla umowy obligacyjnej zawartej w obrocie handlowym na przykład pomiędzy Chińską Republiką Ludową i USA lub Australią i Filipinami. W związku z powyższym normy kolizyjne rozporządzenia Rzym I będą konieczne do znalezienia prawa właściwego dla warunków umów konsumenckich i regulaminów w usługach świadczonych drogą elektroniczną zarówno w wypadku, gdy dostawcą usługi jest podmiot z UE, jak i wtedy, gdy jest to podmiot z państwa trzeciego (spoza UE)”[166]. Omawiane rozporządzenie przewiduje możliwość swobody wyboru prawa przez strony umowy, z tym, że wybór prawa musi zostać dokonany w sposób wyraźny i wynikać w sposób jednoznaczny z umowy bądź okoliczności sprawy[167]. Artykuł 3 ust. 2 stanowi, że strony mogą w każdym czasie umówić się, że umowa będzie podlegać innemu prawu niż to ustalone wcześniej w drodze klauzuli jurysdykcyjnej.

Istotną regulacją - z perspektywy obrotu elektronicznego - są przepisy określające skutki prawne braku wyboru prawa właściwego przez strony. Dość często strony zawierające transakcje w cyberprzestrzeni w ogóle nie regulują kwestii jurysdykcji. Rzym I (art. 4, ust. 1) przewiduje, iż w przypadku niedokonania wyboru prawa właściwego dla umowy, stosowane będzie prawo strony zobowiązanej do spełnienia świadczenia charakterystycznego[168]. Prawo właściwe będzie wybrane między innymi w sposób następujący:

[164] W. Popiołek, *Prawo właściwe dla umownych zobowiązań elektronicznych w konwencji rzymskiej i projekcie rozporządzenia Rzym I*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych. Materiały z konferencji*, Warszawa 2008, s. 22-23.
[165] P.P. Polański, *Europejskie …*, s. 356.
[166] M. Bienias, *Prawo właściwe i jurysdykcja w usługach świadczonych drogą elektroniczną*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych” 2012, nr 4, s. 18.
[167] P. P. Polański, *Europejskie…*, s. 356.
[168] Ibidem, s. 357.

1) umowa sprzedaży towarów - według prawa państwa, w którym sprzedawca ma miejsce zwykłego pobytu,
2) umowa świadczenia usług - według prawa państwa, w którym usługodawca ma miejsce zwykłego pobytu,
3) umowa dystrybucji - według prawa państwa, w którym dystrybutor ma miejsce zwykłego pobytu,
4) umowa sprzedaży towarów w drodze licytacji - wg. prawa państwa, w którym odbywa się licytacja, jeżeli można to ustalić,
5) umowa zawarta w ramach wielostronnego systemu, który kojarzy lub ułatwia kojarzenie wielu transakcji kupna i sprzedaży instrumentów finansowych w rozumieniu definicji z art. 4 ust. 1 pkt. 17 dyrektywy 2004/39/WE - zgodnie z regułami innymi niż uznaniowe i który podlega jednemu prawu - podlega właśnie temu prawu.

Rozporządzeniem Rzym I wprowadzono bardziej szczegółowe, w porównaniu z konwencją rzymską, uregulowania. Konwencja rzymska(art. 4) przewidywała, że w przypadku braku wyboru prawa właściwego przez strony roszczenie będzie podlegać prawu państwa, z którym wykazuje ona najściślejszy związek. Jednakże jeżeli część umowy dałaby się oddzielić od reszty, a wykazuje ściślejszy związek z innym państwem, to w drodze wyjątku dopuszczalne było zastosowanie prawa innego państwa. Za najściślejszy związek z państwem rozumie się związek z tym państwem, w którym strona, na której spoczywa obowiązek spełnienia świadczenia charakterystycznego, ma miejsce zwykłego pobytu w chwili zawarcia umowy, a w przypadku osoby prawnej, spółki lub stowarzyszenia - siedzibę zarządu. Świadczeniem charakterystycznym było świadczenie pozwalające odróżnić typ umowy. Rozporządzeniem Rzym I przyjęto rozwiązania bardziej przejrzyste, nieco kazuistyczne, lecz w jaśniejszy sposób wskazujące prawo właściwe. Nie mniej jednak sformułowanie „ściślejszy związek" niejednokrotnie powodowało problemy interpretacyjne.

Jeżeli strony umowy nie wybrały prawa właściwego dla umowy przewozu towarów, to zgodnie z art. 5 (Rzym I), prawem właściwym jest prawo państwa, w którym przewoźnik ma miejsce zwykłego pobytu, o ile w tym państwie przewidziane jest również miejsce przyjęcia towaru do przewozu, miejsce dostawy bądź miejsce zwykłego pobytu nadawcy. W przypadku braku spełnienia wskazanych wyżej przesłanek prawem właściwym będzie prawo państwa, w którym doszło do dostawy.

Artykuł 5 rozporządzenia Rzym I porusza zagadnienie umów konsumenckich, czyli umów zawartych z osobą fizyczną, niezwiązanych z jej działalnością gospodarczą lub zawodową (konsument), z inną osobą prowadzącą działalność (przedsiębiorca). Umowy takie będą podlegały prawu właściwemu dla miejsca zwykłego pobytu konsumenta, pod warunkiem, że przedsiębiorca prowadzi swoją działalność gospodarczą lub zawodową w państwie zwykłego pobytu konsumenta i kieruje w jakikolwiek sposób swoją działalność do tego państwa, lub do kilku państw z tym państwem włącznie (art. 6 ust. 1).

Należy rozwinąć wymienione powyżej sformułowanie dotyczące „kierowania w jakikolwiek sposób" działalności przedsiębiorcy, w kontekście stron internetowych oferujących zawarcie umowy w drodze elektronicznej. Przyznanie ochrony konsumentowi uzależnione będzie od ustalenia, czy działalność gospodarcza przedsiębiorcy kierowana była do kraju konsumenta[169]. W doktrynie wskazuje się (również w odniesieniu do rozporządzenia Rzym I), iż „sam fakt, że strona internetowa jest dostępna, nie wystarcza do zastosowania przepisu art. 15 rozporządzenia Bruksela I[170], konieczne jest również to, by strona ta umożliwiała zawieranie umów na odległość i umowa została rzeczywiście zawarta „za pomocą dowolnych środków". Nie musi to być przy tym strona interaktywna, także strona proponująca zawarcie umowy przez przesłanie zamówienia faksem czy w inny podobny sposób umożliwiająca zawarcie umowy na odległość. W rozumieniu omawianego przepisu nie jest stroną umożliwiającą zawieranie umów na odległość strona internetowa, która jest przeznaczona dla konsumentów z całego świata, dostarczająca informacji na temat produktu (usługi), która jednak zachęca do zawarcia umowy z dystrybutorem czy lokalnym przedstawicielem nie proponując zarazem jej zawarcia bezpośrednio poprzez skierowanie oferty (oświadczenie o przyjęciu oferty) „do" strony internetowej. Umowa zawarta w ten sposób nie jest zresztą, w przyjętym tu znaczeniu, umową elektroniczną"[171]. Podobne stanowisko zostało zaprezentowane w wyroku Trybunału Sprawiedliwości w sprawie *Pammer v Hotel Alpenhof*[172], w którym sprecyzowano kryteria, które winno się wziąć pod uwagę przy ocenie czy strona www jest kierowana do określonego państwa członkowskiego.

[169] P. P. Polański, *Europejskie …*, s. 358.
[170] Rozporządzenie Rady (WE) nr 44/2001 z dnia 22 grudnia 2000 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.U. L 12 z 16.1.2001) nazywane rozporządzeniem Bruksela I,
[171] W. Popiołek, op. cit., s. 25-26.
[172] Wyrok Trybunału Sprawiedliwości UE z dnia 7 grudnia 2010 r. w sprawach połączonych C-585/08, *Peter Pammer przeciwko Reederei Karl Schluter GmbH & Co KG*, oraz C-144/09, *Hotel Alpenhof GesmbH przeciwko Oliverowi Hellerowi*, ECR [2010] I-0000.

By konsument uzyskał ochronę na mocy rozporządzenia musi zaistnieć związek pomiędzy interaktywną stroną internetową przedsiębiorcy a państwem pobytu konsumenta. Dodatkowym warunkiem jest zawarcie umowy w ramach tej działalności, czyli przez interaktywną stronę www przedsiębiorcy. Michał Bienias podkreśla, że „witryna musi zawierać określony zespół cech, które wskazują związek z państwem i które mogą być uznane za kierowanie działalności do tego państwa"[173]. Agata Jaroszek uważa, że: „interaktywna komunikacja przez witrynę internetową może polegać na zapewnianiu następujących form komunikacji pozwalających na wykazanie związku z państwem zamieszkania konsumenta:

a) możliwość wysyłania i odbierania poczty elektronicznej,
b) możliwość wysyłania i odbierania informacji (np. forum dyskusyjne), które mogą dotyczyć opinii innych klientów na temat jakości oferowanych towarów lub usług za pośrednictwem strony, czy też rzetelności sprzedawcy, terminów realizacji zamówienia itp.,
c) zapewnieniu połączenia telefonicznego, w tym bezpłatnego numeru, w celu uzyskania szczegółowych informacji na temat oferowanych produktów lub usług, rozwiązywanie problemów itp.,
d) możliwość wypełnienia oraz wysłania formularza zamówienia na towary bądź usługi, zamieszczenie reklamy w prasie lub telewizji na terenie danego państwa".[174]

Ustęp 2 artykułu 6 stanowi, że mimo wymienionych wyżej regulacji strony mogą zawsze dokonać wyboru prawa właściwego na zasadach ogólnych. Wybór prawa właściwego przez strony umowy nie może jednakże prowadzić do pozbawienia konsumenta ochrony przysługującej mu z mocy prawa przez przepisy państwa, które byłoby właściwe w braku wyboru. Oznacza to, że strony jako prawo właściwe mogą wybrać na przykład prawo hiszpańskie, lecz jeżeli okaże się ono mniej korzystne dla konsumenta, który ma miejsce pobytu na przykład w Holandii to przepisy holenderskie nie zastąpią całkowicie, lecz jedynie „wyprą" te przepisy, które są mniej korzystne dla konsumenta. Sąd rozstrzygając powstały spór będzie zatem brał pod uwagę nie tylko przepisy hiszpańskie, ale również holenderskie w zakresie w jakim przyznają one większą ochronę konsumentowi[175].

Rzym I wprowadza o wiele dalej idące postanowienia niż konwencja rzymska. Podzielić należy pogląd M. Świerczyńskiego, stwierdzający że „regulacja (...) wynikająca

[173] M. Bienias, *Prawo …*, s.18.
[174] A. Jaroszek, *Prawo właściwe dla umów konsumenckich zawieranych przez Internet*, Warszawa 2009, s. 144.
[175] M. Świerczyński, *Jurysdykcja …*, s. 140.

konwencji rzymskiej jest uważana za archaiczną, nieprzystającą do współczesnego obrotu, w szczególności ze względu na fakt, że chroni przede wszystkim konsumenta pasywnego, a nie typowego dla Internetu konsumenta aktywnego"[176]. Konieczna okazała się zmiana przepisów i dostosowanie ich do kryteriów zaawansowanego technologicznie świata i aktywnego internauty. Rozporządzeniem Rzym I wprowadzono nowe modele postępowania, które bardziej przystają do nowoczesnego obrotu elektronicznego, są bardziej szczegółowe, więc łatwiej je zastosować do handlu elektronicznego.

Rzym II

Kwestia ustalenia jurysdykcji dla zobowiązań wynikających z deliktów elektronicznych w Unii Europejskiej została unormowana rozporządzeniem (WE) Parlamentu Europejskiego i Rady nr 846/2007 dotyczącym prawa właściwego dla zobowiązań pozaumownych (Rzym II). Reguluje ono kwestię zobowiązań pozaumownych w sprawach cywilnych i handlowych, powiązanych z prawami różnych państw. Podobnie jak rozporządzenie Rzym I, ma powszechny charakter stosowania, co oznacza, iż przepisy te można stosować bez względu na to, czy jest ono przepisem państwa członkowskiego[177]. Rozporządzenie może być stosowane do spraw związanych z własnością intelektualną czy też czynów nieuczciwej konkurencji. Z omawianego aktu prawnego wyłączone zostało jednak stosowanie pozaumownych zobowiązań wynikających z naruszenia prawa do prywatności, jak i innych dóbr osobistych, w tym zniesławienia (art. 1, ust. 2, lit. g). Rozporządzenie ma szczególne znaczenie w kontekście deliktów i innych szkód, które mogą wystąpić z tytułu zobowiązań pozaumownych w cyberprzestrzeni (zakup leków bądź zabawek niespełniających atestów i innych produktów niebezpiecznych).

Definicja szkody została sformułowana w rozporządzeniu Rzym II jako wszelkie następstwa wynikające z czynu niedozwolonego, bezpodstawnego wzbogacenia, prowadzenia cudzych spraw bez zlecenia oraz *culpa in contrahendo*. Co istotne, za szkodę uznano nie tylko sam fakt jej wyrządzenia, lecz rozszerzono odpowiedzialność również na samo prawdopodobieństwo wystąpienia szkody (art. 2, ust. 1i 3).

[176] Ibidem, s. 142.
[177] P.P. Polański, *Europejskie …*, s. 359.

Wprowadzoną w rozporządzeniu Rzym II ogólną zasadą ustalania odpowiedzialności deliktowej jest stosowanie prawa państwa, w którym powstaje szkoda, niezależnie od tego, w jakim państwie lub państwach miało miejsce zdarzenie wywołujące delikt oraz gdzie występują skutki pośrednie tego zdarzenia. Wyjątkiem od tej zasady jest fakt zamieszkiwania poszkodowanego i sprawcy w tym samym państwie - wówczas stosowane jest prawo właściwe dla danego państwa. Jednakże, jeżeli podobnie jak w rozporządzeniu Rzym I, z okoliczności faktycznych sprawy wynika, iż czyn ma ściślejszy związek (np. istnienie wcześniejszy stosunek między stronami tj. umowa związana z danym czynem) z innym państwem niż wyżej wymienione to stosuje się prawo tego właśnie państwa (art. 4).

W przypadku odpowiedzialności deliktowej z tytułu szkody wyrządzonej przez produkt (art. 4. ust. 1) prawem właściwym będzie:

1. jeżeli produkt został wprowadzony do obrotu w państwie zwykłego pobytu poszkodowanego - prawo tego państwa, jeżeli poszkodowany w chwili powstania szkody miał tam miejsce zwykłego pobytu,
2. prawo państwa w którym produkt został nabyty, jeżeli został on w tym państwie wprowadzony do obrotu,
3. prawo państwa w którym powstała szkoda, jeżeli produkt został w tym państwie wprowadzony do obrotu.

Wyjątkiem od wyżej wymienionych zasad jurysdykcji szczególnej będzie okoliczność, że osoba, której przypisuje się odpowiedzialność nie mogła w uzasadniony sposób przewidzieć wprowadzenia produktu do państw opisanych w w/w punktach. Wówczas prawem właściwym będzie prawo państwa miejsca zwykłego pobytu osoby odpowiedzialnej (art. 3, ust. 2).

W rozporządzeniu Rzym II art. 8 poświęcono kwestii naruszenia praw własności intelektualnej. Stanowi się w nim, że w przypadku naruszenia praw własności intelektualnej prawem właściwym będzie prawo państwa, na podstawie którego dochodzi się ochrony. Jednakże w przypadku, gdy dochodzi do naruszenia jednolitego wspólnotowego prawa własności intelektualnej to strony obowiązane są stosować prawo państwa, w którym naruszenie miało miejsce we wszelkich kwestiach, które nieodpowiadaną odpowiednim instrumentom wspólnotowym (art. 8).

Mimo ogólnych zasad jurysdykcyjnych Rzym II wprowadza możliwość wyboru prawa w drodze porozumienia zawartego po wystąpieniu zdarzenia powodującego szkodę bądź w przypadku prowadzenia przez wszystkie strony stosunku działalności gospodarczej - na mocy postanowienia negocjowanego przed wystąpieniem zdarzenia powodującego szkodę. W takim przypadku nie dopuszcza się możliwości wyboru prawa w sposób dorozumiany. Porozumienie musi być wyraźne i nie może naruszać praw osób trzecich. Wskazać należy, że jeżeli mimo wyboru prawa, wszystkie elementy stanu faktycznego (w chwili wystąpienia zdarzenia wywołującego szkodę) nastąpią w innym państwie niż wybranym, to rozstrzygnięcie sprawy nie może nastąpić z wyłączeniem prawa tego państwa (art. 14).

Rozporządzenie nr 1215/2012 w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych

Unia Europejska kwestię jurysdykcji cywilnej rozstrzygnęła w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, który to akt uchylił poprzednio obowiązujące rozporządzenie Rady (WE) nr 44/2011[178]. Przedmiotem rozporządzenia jest jurysdykcja sądów oraz uznawalność i wykonalność orzeczeń sądowych. Aktu nie stosuje się jednakże do spraw dotyczących odpowiedzialności państwa za działania lub zaniechana władzy publicznej.

Podstawą jurysdykcji ogólnej w sprawach cywilnych i handlowych jest miejsce zamieszkania osoby fizycznej lub miejsce położenia siedziby osoby prawnej. Powód, który ma zamiar pozwać daną osobę zgodnie z rzymską maksymą *actor sequitur forum rei* musi wybrać sąd właściwy dla pozwanego[179]. Unia Europejska w rozporządzeniu nr 1215/2012 w art. 4 przychyliła się do wskazanej podstawy jurysdykcji ogólnej przyjmując, że osoby mające miejsce zamieszkania na terytorium państwa członkowskiego mogą być pozywane, niezależnie od ich obywatelstwa przed sądami tego państwa członkowskiego. Przepisy

[178] Rozporządzenie Rady (WE) nr 44/2001 z dnia 22 grudnia 2000 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, Dz. Urz. L 012, przestało obowiązywać 09.01.2015 r. zgodnie z danymi zawartymi na stronie http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32001R0044 [13.07.2015].

[179] M. Zalisko, *Instrumenty prawne w obszarze współpracy sądowej w sprawach cywilnych i handlowych w Unii Europejskiej*, Warszawa 2013, s. 81.

jurysdykcyjne właściwe dla państwa członkowskiego stosuje się odpowiednio w stosunku do osób, które nie są obywatelami tego kraju, lecz mają w nim miejsce zamieszkania. Łącznikiem jurysdykcyjnym we wskazanym wyżej przypadku jest domicyl pozwanego w państwie członkowskim. Nie jest wówczas istotne miejsce pobytu czy obywatelstwa pozwanego[180].

Oprócz ogólnej jurysdykcji rozporządzenie 1215/2012 zawiera szereg postanowień dotyczących zasad jurysdykcji szczególnej - przemiennej, jednakże w niniejszym opracowaniu skupiono się jedynie na tych, które mogą mieć zastosowanie w przypadku wystąpienia sporu jurysdykcyjnego w cyberprzestrzeni. Osoby, które mają miejsce zamieszkania na terytorium państwa członkowskiego, według art. 7, ust. 1-3 mogą być pozywane w innym państwie członkowskim w sprawach dotyczących:

1. umowy - przez sądy miejsca wykonania umowy (w przypadku sprzedaży rzeczy ruchomych miejsce wykonania umowy rozumiane jest jako miejsce gdzie rzeczy te miały być dostarczone, a w przypadku świadczenia usług - miejsce gdzie usługi były lub miały być świadczone),
2. czynu niedozwolonego - przez sądy miejsca, w którym nastąpiło lub może nastąpić zdarzenie wywołujące szkodę,
3. roszczeń cywilnoprawnych, o odszkodowanie lub przywrócenie stanu poprzedniego, które wynikają z czynu zagrożonego karą - przez sąd, do którego wniesiono akt oskarżenia, o ile sąd ten może według swego prawa rozpoznać roszczenia cywilnoprawne.

Rozporządzenie nr 1215/2012 zawiera postanowienia niemalże tożsame do wcześniej obowiązującego rozporządzenia nr 44/2001 oraz konwencji lugańskiej. Ustalenie miejsca wykonania zobowiązania w przypadku umów elektronicznych może nastręczyć wiele trudności np. w gdy umowa przewiduje wykonanie usługi w sposób cyfrowy, czyli przez skopiowanie danych z komputera na komputer. Usługi polegające na świadczeniu treści cyfrowych nie mogą być uznane ani za dostarczenie towaru ani usług w świetle przepisów omawianego rozporządzenia. Należy postawić sobie zatem pytanie, gdzie zostanie wykonana umowa polegająca na świadczeniu treści cyfrowych - czy w państwie sprzedawcy tych treści (umieszcza on bowiem stamtąd produkty na swojej stronie www) czy też w państwie

[180] J. Gołaczyński (red.), *Jurysdykcja, uznawanie orzeczeń sądowych oraz ich wykonywanie w sprawach cywilnych i handlowych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012. Komentarz*, Warszawa 2015, s. 25.

nabywcy (który otrzyma tam np. kod dostępu do treści zawartych *on-line*). Marek Świerczyński stoi na stanowisku, że w większości przypadków można uznać, że miejscem wykonania zobowiązania w takim przypadku będzie miejsce działania sprzedawcy, czyli miejsce, gdzie dane zostały wprowadzone do systemu komputerowego. Autor podkreśla również, że nie będzie miało znaczenia miejsce położenia serwerów firmy[181].

W sprawie *Electrosteel Europe SA v. Edil Centro SpA*[182] stwierdzono, że „w przypadku sprzedaży na odległość miejsce, w którym towar został lub powinien zostać dostarczony zgodnie z umową, określa się na podstawie postanowień umowy. W celu ustalenia, czy miejsce dostawy zostało określone „zgodnie z umową", sąd krajowy winien brać pod uwagę wszystkie istotne reguły i klauzule umowy, które mogą określić w sposób jednoznaczny to miejsce, w tym reguły i klauzule powszechnie uznane i potwierdzone zwyczajami handlu międzynarodowego, jak *Incoterms* opracowane przez Międzynarodową Izbę Handlową, w wersji opublikowanej w 2000 roku. W braku możliwości określenia miejsca dostawy na tej podstawie, bez odwoływania się do przepisów materialnych znajdujących zastosowanie do umowy, miejscem dostawy jest miejsce faktycznego wydania towaru, w wyniku którego to wydania nabywca uzyskał lub powinien był uzyskać możliwość rzeczywistego dysponowania towarem w ostatecznym miejscu przeznaczenia transakcji sprzedaży"[183]. Orzeczenie to zostało wydane na kanwie obowiązującego wówczas rozporządzenia 44/2011, lecz pozostaje ono aktualne również w stosunku do umów elektronicznych rozpatrywanych na mocy rozporządzenia 1215/2012.

Czyn niedozwolony należy interpretować, jako każdą sytuację, w której powód domaga się naprawienia szkody, a roszczenie nie opiera się na postanowieniach zawartych w umowie[184]. Jacek Gołaczyński uznaje, że „w odniesieniu do zdarzenia powodującego szkodę posłużono się zwrotami »czynu niedozwolonego lub czynu podobnego do czynu niedozwolonego« tak, aby przez nie rozumieć jak najszerszy zakres zdarzeń powodujących powstanie zobowiązania pozaumownego. Nie jest to zatem przepis regulujący jedynie jurysdykcję w zakresie deliktów, ale wszelkich podobnych zdarzeń powodujących szkodę o

[181] M. Świerczyński, *Komentarz do art. 7,* [w:] J. Gołaczyński (red.), *Jurysdykcja, uznawanie orzeczeń sądowych oraz ich wykonywanie w sprawach cywilnych i handlowych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012. Komentarz,* Warszawa 2015, s. 51-52.
[182] Wyrok Trybunału Sprawiedliwości UE z dnia 09 czerwca.2011 r. w sprawie *Electrosteel Europe SA v. Edil Centro, SpA*, sygn. akt C-87/10.
[183] Ibidem, sentencja wyroku, pkt. 26.
[184] M. Świerczyński, *Komentarz ...*, s. 45.

pochodzeniu pozaumownym."[185] Przyznanie jurysdykcji państwu, w którym nastąpiło zdarzenie wywołujące szkodę z czynu niedozwolonego, uzasadnione jest koniecznością zapewnienia sprawnego funkcjonowania wymiaru sprawiedliwości oraz prawidłowego ukształtowania procesu. Sąd miejsca wystąpienia szkody, ze względu na bliskość do przedmiotu sporu i możliwości przeprowadzenia dowodów jest najwłaściwszym do rozpoznania sprawy w tym zakresie[186].

Trybunał Sprawiedliwości wypowiedział się 03.04.2014 roku w kwestii miejsca popełnienia czynów niedozwolonych, które naruszyły majątkowe prawa autorskie w sprawie *Hi Hotel HCF SARL v. Uwe Spoering*[187]. Przyjął, że „w wypadku gdy kilku domniemanych sprawców spowodowało podnoszoną szkodę w zakresie majątkowych praw autorskich chronionych w państwie członkowskim, w którym siedzibę ma sąd, przed którym zawisł spór, przepis ten nie umożliwia ustalenia – ze względu na miejsce wystąpienia zdarzenia powodującego powstanie szkody – jurysdykcji sądu, na którego obszarze właściwości pozwany przed tym sądem sprawca nie działał, lecz umożliwia ustalenie jurysdykcji tego sądu ze względu na miejsce materializacji szkody, pod warunkiem że podnoszona szkoda może się zmaterializować na obszarze właściwości sądu, przed którym zawisł spór. W tej ostatniej sytuacji sąd ten jest właściwy jedynie do rozpoznania powództwa dotyczącego szkody wyrządzonej na terytorium państwa członkowskiego, w którym sąd ten ma swoją siedzibę".[188]

Rozporządzenie nr 1215/2012 w art. 17-18 reguluje kwestię jurysdykcji w sprawach dotyczących umów konsumenckich, uznając, że konsument może wytoczyć powództwo przeciwko swojemu kontrahentowi przed sądem państwa członkowskiego, na którego terytorium kontrahent ten ma miejsce zamieszkania, albo bez względu na miejsce zamieszkania kontrahenta - właściwym dla miejsca zamieszkania konsumenta. Z kolei kontrahent ma możliwość wytoczenia powództwa przeciwko konsumentowi tylko przed sądem właściwym dla miejsca zamieszkania konsumenta. Bez wątpienia przepis ten będzie miał szczególne znaczenie w odniesieniu do umów zawieranych przez Internet przez osoby fizyczne. Zamawiając produkty ze sklepów internetowych przedsiębiorców innych państw członkowskich Unii Europejskiej istnieje wysokie prawdopodobieństwo powstania sporów w przedmiocie zawarcia i wykonania umowy oraz sądu właściwego. Przepis ten słusznie

[185] Ibidem, s. 56.
[186] K. Weitz, *Kilka uwag na temat jurysdykcji krajowej w sprawach z czynów niedozwolonych w prawie europejskim*, „Roczniki Nauk Prawnych" 2006, t. 16, s. 122.
[187] Wyrok Trybunału Sprawiedliwości UE z dnia 03 kwietnia 2014 r., w sprawie *Hi Hotel HCF SARL przeciwko Uwe Spoering*, sygn. akt C-387/12.
[188] Ibidem, sentencja wyroku, pkt. 40.

ustanawia normy korzystne dla konsumenta, uznając go za stronę słabszą gospodarczo w porównaniu z przedsiębiorcą.

Rozporządzenie nr 1215/2012 wprowadza ponadto możliwość zawarcia umowy jurysdykcyjnej. Artykuł 25 stanowi, że jeżeli strony zawarły w umowie klauzulę jurysdykcyjną, to sądowi lub sądom tego państwa przyznana została jurysdykcja, chyba że umowa na mocy prawa danego państwa członkowskiego jest nieważna pod względem materialnym. Tak określona jurysdykcja jest jurysdykcją wyłączną, o ile strony nie uzgodniły inaczej. Przepis ten został zmodyfikowany w odniesieniu do poprzednio obowiązującego rozporządzenia nr 44/2001. Rozporządzenie nr 1215/2012 nie wprowadza dodatkowego wymogu by chociażby jedna ze stron miała miejsce zamieszkania na terytorium państwa członkowskiego[189].

Umowę jurysdykcyjną można przyjąć zarówno przy zawieraniu umowy, jak i po jej zawarciu, zarówno w sytuacji wystąpienia sporu, jak i przed zaistnieniem takiej sytuacji. Jurysdykcja wybrana na mocy postanowienia stron będzie miała wówczas charakter jurysdykcji wyłącznej, chyba że strony stosunku zobowiązaniowego postanowią inaczej[190].

2.1.2.4. Jurysdykcja cywilna w cyberprzestrzeni w aspekcie prawnoporównawczym

Omawiając kwestię jurysdykcji cywilnej w odniesieniu do cyberprzestrzeni należy wyjść poza ścisłe międzynarodowe i regionalne ramy prawne. Warto również przyjrzeć się rozwiązaniom przyjętych w porządkach prawnych poszczególnych państw. Kraje będące członkami Unii Europejskiej w dużej mierze posiadają zunifikowane regulacje, co wynika z podległości prawu wspólnotowemu[191]. Niejednokrotnie jednak orzecznictwo wydane na niwie krajowej było szeroko dyskutowane przez praktyków i teoretyków prawa w innych państwach. Część orzeczeń wpłynęła też na kształtowanie się prawodawstwa unijnego,

[189] P. Rodziewicz, *Komentarz do art. 25*, [w:] J. Gołaczyński, *Jurysdykcja, uznawanie orzeczeń sądowych oraz ich wykonywanie w sprawach cywilnych i handlowych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012. Komentarz*, Warszawa 2015, s. 133-134.
[190] Ibidem, s. 134-135.
[191] J. Gołaczyński, *Umowy elektroniczne w prawie wybranych państw*, [w:] J. Gołaczyński (red.), *Umowy elektroniczne w obrocie gospodarczym*, Warszawa 2005, s. 264.

dlatego też w niniejszym podrozdziale omówione zostaną również najważniejsze orzeczenia krajowe poruszające kwestię jurysdykcji w cyberprzestrzeni.

W piśmiennictwie wskazuje się, że stosunkowo często przepisy wewnętrzne państw zawierają tak pojemne i elastyczne uregulowania, że w praktyce nie wykształciła się nowa kategoria prawa - prawa internetowego. Istniejące dotychczas przepisy stosuje się odpowiednio do czynności podejmowanych w przestrzeni wirtualnej. Szczegółowe regulacje pojawiają się przede wszystkim by usuwać niejasności wynikające z postępu technologicznego[192]. Wskazanie prawa właściwego w aspekcie zobowiązań elektronicznych ma znaczenie nie tylko teoretyczne, ale też praktyczne. Państwa uznając swoją jurysdykcję za właściwą w niektórych przypadkach starają się wpłynąć na podmioty podlegające de facto innej jurysdykcji[193].

Regulacje europejskie

Francja

Wybór sądu właściwego na podstawie francuskiego Kodeksu Postępowania Cywilnego[194] może być oparty na kilku łącznikach jurysdykcyjnych między innymi na właściwości rzeczowej bądź miejscowej. Właściwość rzeczowa wynika z przepisów organizacji sądów powszechnych oraz przepisów szczegółowych. W sytuacji, gdy właściwość sądu zależy od wartości przedmiotu sporu, to sąd właściwy rzeczowo do rozstrzygnięcia roszczenia głównego będzie również właściwy do rozstrzygnięcia roszczeń pobocznych tj. interwencji i pozwów wzajemnych. Strony, zgodnie z zasadą swobody kontraktowania, mogą jednakże ustalić na mocy klauzuli jurysdykcyjnej, iż właściwym do rozpoznania sprawy będzie inny sąd niż wynikałoby to z przepisów ogólnych[195].

[192] Ibidem, s. 265.
[193] D. Karwala, *Dostępność* op. cit., s. 304.
[194] *Nouveau Code de Procédure Civile* z dnia 1 stycznia 1976 r. dostępny na stronie internetowej: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070716 [10.10.2017].
[195] A. Machowska, *Postępowanie cywilne*, [w:] A. Machowska, K. Wojtyczek (red.), *Prawo francuskie*, t. 1, Kraków 2004, s. 218.

Właściwość miejscową w prawie francuskim można podzielić na właściwość ogólną, przemienną lub wyłączną. Według zasad ogólnych sądem właściwym jest ten sąd, w okręgu którego pozwany ma miejsce pobytu (fr. *lieu où demeure le défendeur*) w dniu wniesienia pozwu. Za miejsce pobytu osób fizycznych należy uznać miejsce zamieszkania oraz centrum aktywności życiowej (fr. *domicile*) bądź miejsce, w którym pozwany przebywa (fr. *résidence*). W przypadku zaś osób prawnych decydować będzie ich siedziba główna, lecz gdy spór dotyczy działalności oddziału pozew być wniesiony przed sądem właściwym dla tego oddziału[196].

W sprawach, w których stroną pozwaną jest więcej niż jedna osoba, powód będzie mógł wytoczyć spór według własnego uznania, przed jednym z sądów właściwych dla poszczególnych pozwanych. Artykuł 42 i 43 francuskiego kodeksu postępowania cywilnego reguluje kwestie braku miejsca zamieszkania pozwanego, bądź jego zamieszkiwania za granicą. W takim przypadku dopuszczalne jest wniesienie pozwu według miejsca zamieszkania powoda. Sąd ten pozostanie właściwy do końca sporu, nawet w przypadku późniejszej zmiany miejsca zamieszkania stron[197]. Regulacje te mają szczególne znacznie zwłaszcza dla sporów mogących wyniknąć w przestrzeni wirtualnej. Osoba mająca miejsce zamieszkania na terytorium Francji, która chce dochodzić swoich praw w związku z czynem dokonanym w cyberprzestrzeni, może zatem wytoczyć powództwo przed sądem francuskim, nawet wówczas, gdy druga ze stron stosunku nie ma faktycznego powiązania z Francją.

Właściwość przemienna będzie z kolei przysługiwała w przypadku roszczeń wynikających z prawa zobowiązań. Powód ma możliwość wyboru sądu innego niż sąd miejsca zamieszkania pozwanego w przypadkach, czyli następujących:

- zobowiązań umownych - przed sądem miejsca, gdzie wg umowy rzecz miała być dostarczona bądź gdzie miała być wykonana usługa,
- zobowiązań wynikających z czynów niedozwolonych - przed sądem, w okręgu którego popełniono szkodę,
- zobowiązań mieszanych (dotyczących roszczeń zarówno osobistych jak i prawa rzeczowego np. dotyczącego unieważnienia umowy sprzedaży nieruchomości) - przed sądem miejsca położenia nieruchomości,
- zobowiązań wynikających z prawa rodzinnego - wg miejsca pobytu wierzyciela.

[196] Ibidem, s. 218.
[197] Ibidem, s. 219.

Wskazane powyżej zasady prawa francuskiego z powodu przyjmowania szerokiego zakresu jurysdykcyjnego doprowadziły do szeregu sprzecznych orzeczeń sądów francuskich. Praktyka orzecznicza w odniesieniu działań podejmowanych w cyberprzestrzeni przyjęła bardzo niespójną linię. Michał Bohaczewski, odnosząc się do kwestii użycia znaków towarowych w cyberprzestrzeni wskazuje: „ostatnia dekada przyniosła we Francji wiele wyroków, w których sądy orzekały o jurysdykcji krajowej w związku z nieuprawnionym użyciem znaków towarowych w Internecie. Trudno jest jednak mówić o jednolitości orzecznictwa. Niekiedy przy określeniu jurysdykcji krajowej sądy zadowalają się wykazaniem technicznej dostępności treści zamieszczonej w sieci, którą uznają za wystarczającą dla stwierdzenia naruszenia. W części orzeczeń rozważania sądów prowadzą do odmiennej oceny dokonania naruszenia w zależności od stadium procesu. Wreszcie, zwłaszcza w ostatnim czasie, sądy często uznają się za międzynarodowo właściwe, gdy ponad samą dostępność na terytorium państwa *fori,* uprawdopodobniony zostanie ekonomiczny związek sprawy z krajowym porządkiem prawnym”[198]. By w pełni zrozumieć problem wynikający z konieczności stosowania przepisów francuskich obowiązujących w odniesieniu do jurysdykcji w cyberprzestrzeni należy przytoczyć kilka interesujących orzeczeń poruszających omawianą kwestię.

Najbardziej znaną sprawą francuską, która wywołała ogólnoświatową dyskusję na temat granic kompetencji jurysdykcyjnych sądów krajowych była sprawa *Yahoo!*[199] Pozew przeciwko internetowemu gigantowi Yahoo! Inc, wytoczyła organizacja LICRA (ang. The *League Against Racism and Antisemitism* - Liga Przeciwko Rasizmowi i Antysemityznowmi) oraz Francuski Związek Studentów Żydowskich. Firma Yahoo! na swojej aukcji internetowej zamieściła przedmioty o tematyce nazistowskiej. Aukcja była również dostępna dla internautów francuskich - zarówno za pomocą amerykańskiej, jak i francuskiej wersji strony. Francuski sędzia uznał, iż Yahoo! naruszyło prawo francuskie, które zakazuje wszystkiego, co „pobudza nienawiść rasową” i nałożył na amerykańską firmę grzywnę pieniężną za „obrazę zbiorowej pamięci Francuzów” oraz nakazał zablokowanie dostępu do witryny, na której odbywała się aukcja[200].

[198] M. Bohaczewski, *Jurysdykcja krajowa w sprawie o naruszenie praw własności intelektualnej w internecie na tle orzecznictwa francuskiego,* [w:] A. Sztoldman (red), *Prawo wobec innowacji technologicznych*, Warszawa 2013, s. 46.
[199] Orzeczenie Sądu Okręgowego w Paryżu z 20 października 2000 r., w sprawie *Anit-Semitism LICRA przeciwko Yachoo! Inc.,* sygn. akt N° RG 00/05308.
[200] J. Kulesza, *Międzynarodowe …*, s. 241-242.

Sędzia Gomez uznał, że „podczas gdy Yahoo! pozostaje świadome faktu skierowania swoich działań do podmiotów francuskich, ponieważ dokonując połączenia ze stronami aukcji z terminali znajdujących się we Francji przekazuje ono ogłoszenia reklamowe w języku francuskim; (...) niniejszym ustanowione zostało wystarczające połączenie dla uznania połączenia z Francją, które pozwala naszym sądom uznać się za całkowicie kompetentne do rozstrzygania powierzonej im kwestii (...)"[201]. Sąd francuski oparł swoje rozstrzygnięcie na konieczności obrony porządku publicznego, przestrzegania prawa oraz wartości wspólnym wszystkim narodom, czyli potępienie zbrodni hitlerowskich. Yahoo! broniła swego stanowiska opierając się na Pierwszej Poprawce do amerykańskiej Konstytucji gwarantującej wolność słowa. Mimo złożenia apelacji sąd wyższego rzędu utrzymał wyrok sądu pierwszej instancji w mocy. Sąd francuski nakazał firmie amerykańskiej zablokowanie dostępu do witryny, na której widniała aukcja[202].

Yahoo! nie złożyła kasacji od wyroku sądu drugiej instancji, lecz sama złożyła pozew w Stanach Zjednoczonych, licząc na wydanie decyzji potwierdzającej niemożność wykonania orzeczenia francuskiego na amerykańskim terytorium. Amerykański sąd pierwszej instancji uznał powództwo Yahoo! Wyrok został też utrzymany w mocy przez Sąd Apelacyjny Dziewiątego Okręgu[203], który uznał jurysdykcję sądów amerykańskich do rozstrzygnięcia sporu, jednakże lecz mimo nadziei Yahoo! nie orzeczono zakazu wykonania francuskiego wyroku na terytorium USA. J. Kulesza w rozważaniach na temat sprawy Yahoo! uznała, że „z perspektywy rozważań jurysdykcyjnych sprawa ta stanowi sygnał rozszerzenia stosowanych dotychczas standardów, w oparciu o które sądy Stanów Zjednoczonych decydowały się wykonywać uprawnienia jurysdykcyjne wobec spraw z przeważającym elementem obcym. Sprawa ta wydaje się więc sygnałem dla sądów innych państw, że wolno im wykonywać władzę w spawach z minimalnym udziałem podmiotów amerykańskich (...). O ile konsekwencje prawne i jurysdykcyjne są ważne dla omawianej sprawy, o tyle jej aspekt internetowy podkreśla złożoność zależności świata on-line i tradycyjnych granic".[204] Wyrok sądu francuskiego był szeroko krytykowany w doktrynie. Nie można zgodzić się z poglądem wyrażonym w wyroku, jakoby sam fakt dostępności treści w danym języku był wystarczającym czynnikiem do uznania swojej jurysdykcji. Przyjęcie takiej koncepcji

[201] Ibidem, s. 242.
[202] Ibidem, s. 242.
[203] Wyrok Sądu Apelacyjnego Dziewiątego Obwodu USA z dnia 12 stycznia 2006 r., w sprawie *Wyrok Yahoo! v. La Ligue Contre le Racisme et l'Antisémitisme*, sygn. akt 2006 WL 60670 (9th Cir. 2006) C-00-21275 JF.
[204] J. Kulesza, *Międzynarodowe …*, s. 243.

prowadziłoby do absurdalnego uznania, że wszystkie anglojęzyczne strony podlegają prawu - no właśnie, którego państwa? USA, Wielkiej Brytanii, Australii czy może Nowej Zelandii?

W orzeczeniu z 25 października 2011 r. *eDate Advertising i Marines*[205] podniesiony został zarzut braku jurysdykcji krajowej z powodu nirozwiązania treści, które miały obrazić dobra osobowe strony, z porządkiem prawnym danego kraju. Trybunał wskazał, iż zasadniczą cechą odróżniającą publikowanie treści w cyberprzestrzeni i w tradycyjnej prasie jest to, że z założenia udostępnianie treści w przestrzeni wirtualnej jest nieograniczone w czasie i miejscu, więc łącznik oparty na rozpowszechnianiu traci na znaczeniu, ponieważ zasięg Internetu jest światowy[206]. Trybunał Sprawiedliwości w orzeczeniu wypracował nowy łącznik pozwalający dochodzić powodowi naprawienia szkody przed jednym sądem. Łącznikiem tym ma być centrum interesów życiowych poszkodowanego, które z zasady będzie odpowiadać jego miejscu zamieszkania. Zastosowanie tego łącznika jest zgodne z teorią dostępności, zgodnie z którą właściwość krajową można stwierdzić wyłącznie na podstawie tego, że dana treść jest dostępna w Internecie. Tak rozumiana jurysdykcja znacznie ułatwia dochodzenie roszczeń przez osoby, których prawa zostały naruszone[207].

Omawiane orzeczenie wzbudziło ożywioną dyskusję i kontrowersje w doktrynie. Wskazywano, że wyrok ogranicza się jedynie do naruszeń popełnionych z użyciem cyberprzestrzeni, w sytuacji, gdy czyny naruszające dobra osobiste mogą być popełniane również z użyciem innych narzędzi w tym tradycyjnych, czyli prasy. Trybunał Sprawiedliwości za podstawę jurysdykcji krajowej za naruszenie dóbr osobistych w cyberprzestrzeni uznał szeroko rozumiane centrum interesów życiowych poszkodowanego. Podkreśla się jednak, iż jest to nie tylko sprzeczne z ogólną zasadą ustalania właściwości według miejsca zamieszkania pozwanego, ale również z dotychczasowym orzecznictwem wspólnotowym[208].

Innym ciekawym przykładem orzecznictwa TS była sprawę *L'Oreal v. eBay* z 12 lipca 2011 r.[209], w której stwierdzono, że sam fakt, iż strona jest dostępna na terytorium, na którym dany znak towarowy jest zastrzeżony, nie oznacza, że jest to kryterium wystarczające do

[205] Wyrok Trybunału Sprawiedliwości UE z dnia 25 października 2011 r. w sprawach *eDate Advertising GmbH przeciwko X* (C0509/09) oraz *Robert Martinez przeciwko MGN Limited* (C-161/10), sygn. akt ECR [2011] I-000.
[206] Ibidem, setencja wyroku, pkt. 45-46.
[207] M. Bohaczewski, op. cit., s. 38.
[208] Ibidem, s. 39-40.
[209] Wyrok Trybunału Sprawiedliwości UE z 12 lipca 2011 r., w sprawie *L'Oreal S.A. i inni przeciwko eBay International AG i inni,* sygn. ak. C-324/09, sygn. akt ECR [2010] I-0000.

stwierdzenia, że oferty sprzedaży zamieszczone na stronie www są skierowane do konsumentów zamieszkujących określone terytorium[210]. Podobnie TS orzekł w sprawie *Pammer i Hotel Alpenhof*, poruszającej problem sporów wynikających z umów konsumenckich. Trybunał uznał, że sam zwrot „kieruje [działalność] do" nie może być interpretowany w ten sposób, że dotyczyłby faktu dostępności witryny w danym kraju[211].

Przytoczyć w tym miejsce należy orzeczenie francuskiego Sądu Kasacyjnego z 9 grudnia 2003 r.[212] w sprawie znaku towarowego francuskiego szampana Cristal. Sprawa została wytoczona przeciwko hiszpańskiemu producentowi win musujących, który posługiwał się na swojej hiszpańskojęzycznej stronie internetowej identycznym znakiem. Sąd Kasacyjny uznał, że sąd francuski jest „międzynarodowo właściwy dla roszczeń o zaniechanie i odszkodowanie za szkodę wyrządzoną we Francji na skutek eksploatacji strony internetowej w Hiszpanii, chociażby strona ta była tylko »biernie« dostępna na terytorium Francji. Sąd nie wyjaśnił, co rozumie przez bierny charakter strony. Za wystarczającą przesłankę uzasadniającą jurysdykcję francuskiego sądu uznano stwierdzenie, że strona wyświetla się na terytorium Francji"[213]. Orzeczenie to rozstrzygnęło zatem problem dostępności treści w cyberprzestrzeni w sposób analogiczny do mediów tradycyjnych. Za łącznik jurysdykcyjny uznano kryterium dostępności strony internetowej na danym terytorium. Znawcy tematu podkreślają jednak, że wyjątek od zasady właściwości sądu miejsca zamieszkania pozwanego nie może być zbyt rozszerzany. Rozważnie należy przyjmować kryterium dostępności strony www w sprawach cyberdeliktów, a w żadnym razie nie można przyjmować tej zasady automatycznie ze względu na specyfikę czynów dokonywanych w cyberprzestrzeni[214]. W doktrynie francuskiej kryterium dostępności akceptuje Fredric Pollaud - Dulian[215], z kolei Sylvain Bollée oraz Bernard Haftel, uznają je za mniejsze zło wobec braku lepszego rozwiązania[216]. Zupełnie inne stanowisko prezentuje Gwendoline Lardeux, która uważa, że nie można - z braku innego rozwiązania - uznać cyberprzestrzeni za miejsce podlegające

[210] M. Bohaczewski, op. cit., s. 42.
[211] Wyrok Trybunału Sprawiedliwości UE z dnia 7 grudnia 2010 r. w sprawach połączonych C-585/08, *Peter Pammer przeciwko Reederei Karl Schluter GmbH & Co KG*, oraz C-144/09, *Hotel Alpenhof GesmbH przeciwko Oliverowi Hellerowi*, sygn. akt ECR [2010] I-0000, sentencja wyroku pkt. 69.
[212] Wyrok Sądu Kasacyjnego we Francji, z 9 grudnia 2003 r., Cour de cassation nr 01-03225.
[213] M. Bohaczewski, op. cit., s. 46-47.
[214] D. Kot, M. Świerczyński, op. cit., s. 460-462.
[215] F. Pollaud - Dulian, *Cometence internationale. Contrefacon. Internet. Droits voisins de l'artiste interprete*, "Revue trimestrielle de droit commercial" 2011, nr 2, s. 356.
[216] S. Bollee, B. Haftel, *Les nouveaux (des) equilibres de la competence internationale en matiere de cyberdelits apres l'arret eDateAdvertising et Martinez*, "Recueil Dalloz", 2012, nr 20, s. 1285.

jurysdykcji wszystkich państw świata i wszystkich porządków prawnych, ponieważ wprowadzi to chaos oraz niepewność obrotu prawnego[217].

Część orzecznictwa francuskiego jako przesłankę naruszenia prawa z rejestracji znaku towarowego uznała z kolei kryterium nakierowania przekazu. Sąd Apelacyjny w Paryżu w orzeczeniu z dnia 27 września 2006 r.[218], odrzucił kryterium dostępności strony internetowej jako podstawy uznania swej jurysdykcji. Jest to orzeczenie zupełnie sprzeczne z wyrokiem zapadłym w sprawie dotyczącej hiszpańskiego przedsiębiorcy posługującego się na swojej stronie www identycznym znakiem towarowym jak przedsiębiorca francuski. Sąd uznał, że „z uwagi na zredagowanie strony w języku hiszpańskim i umożliwienie za jej pośrednictwem dokonywania transakcji w pesetach (stan faktyczny odnosił się do 2001 r.) w żaden sposób nie zostało dowiedzione, że posłużenie się identycznym oznaczeniem do podlegającego ochronie we Francji na stronie internetowej, choć dostępnej we Francji, stanowi wkroczenie w zakres prawa wyłącznego przysługującego na jej terytorium"[219]. Spotkać się można z poglądem, iż w internetowych stosunkach handlowych język winien być kryterium jurysdykcyjnym, który wprowadza domniemanie skierowania treści zawartych na stronie internetowej do odbiorcy krajowego. Innym kryterium może być waluta, oferowane możliwości dostawy czy nazwy domeny. Odrzucić należy ten pogląd. Język, waluta czy nazwa domeny winna być stosowana jedynie pomocniczo. Nie można uznać, iż winien to być główny i jedyny łącznik jurysdykcyjny określający prawo właściwe do rozstrzygnięcia sporu.

Niemcy

W doktrynie niemieckiej jurysdykcja terytorialna istnieje wyłącznie w granicach danego państwa, ale ma charakter nieograniczony i władczy. Oznacza to, że zgodnie z poglądami niemieckich znawców prawa każde państwo na swoim terytorium może rozstrzygnąć każdą sprawę cywilną, bez względu na to czy strony uczestniczące w sporze lub przedmiot procesu mają jakikolwiek związek z danym krajem[220].

[217] G. Lerdeux, *La competence internationale des tribunaux francais en matiere de cyberdelits*, "Recueil Dalloz" 2010, nr 19, s. 1183.
[218] Wyrok Cour d'appel w Paryżu, z dnia 27 września 2006 r., nr 04-20185.
[219] M. Bohaczewski, op. cit., s. 46-47.
[220] K. Weitz, *Jurysdykcja krajowa w postępowaniu cywilnym*, Warszawa 2005, s. 43.

Zgodnie z prawem niemieckim podstawą jurysdykcji terytorialnej jest miejsce zamieszkania osoby na danym terytorium. W przypadku osób fizycznych miejsce to ustala się na podstawie tego, gdzie osoba będzie miała miejsce pobytu w dłuższej perspektywie. Nawet dla osób, czyli pomocy domowych, pracowników, studentów, uczniów czy praktykantów sądem właściwym będzie miejsce, gdzie przebywają z zamiarem dłuższego pobytu. Podobnie jak w Polsce, w przypadku przedsiębiorstw powództwo może być wytoczone w miejscu działalności jego siedziby bądź oddziału.

Zgodnie z art. 23 niemieckiego kodeksu postępowania cywilnego w przypadku powództwa wynikającego z prawa własności wniesionego przeciwko osobie, która nie ma miejsca zamieszkania w Niemczech, właściwy winien być sąd, w okręgu którego położone są aktywa pozwanego. Ustawodawca niemiecki zdecydował się na wprowadzenie jurysdykcji wyłącznej w kwestiach takich jak sąd spadku oraz prawa wynikające z nieruchomości.

Problem jurysdykcji dotyczącej prawa umów została rozstrzygnięty w art. 29 niemieckiego kodeksu postępowania cywilnego. Uznano, iż sądem właściwym będzie miejsce, w którym umowa miała być wykonana. W przypadku umów zawieranych poza lokalem przedsiębiorstwa, spór winien być wytoczony przed sądem właściwym dla miejsca zamieszkania konsumenta, jeżeli sprawa dotyczy zaś czynów niedozwolonych - sąd miejsca popełnienia czynu. Artykuł 38 dopuszcza możliwość wybrania przez strony sądu właściwego. Uznaje się, że strony mogą zawrzeć umowę dotyczącą jurysdykcji, jednakże musi być ona zawarta na piśmie, a jeżeli została zawarta ustnie to musi zostać potwierdzona na piśmie. Jeżeli tylko jedna ze stron ma miejsce zamieszkania w Niemczech, to strony mogą uznać za sąd właściwy do rozstrzygnięcia sporu wyłącznie ten sąd, we właściwości której osoba ta miejsce zamieszkania, bądź następuje inny łącznik z danym miejscem. Porozumienie dotyczące wyboru sądu właściwego będzie jednak nieważne i niedopuszczalne, w przypadku jurysdykcji wyłącznej oraz w przypadku sporów dotyczących roszczeń niepieniężnych, które są przypisane do lokalnych sądów[221].

Sądy niższego szczebla - *Amtsgerichte* - mają jurysdykcję w sprawach w, których wartość przedmiotu sporu nie przekracza 5.000 euro, Sądy Rejonowe pierwszej instancji *Landgerichte* - rozstrzygają sprawy, których wartość przekracza 5.000 euro. Praktyka sądowa w Niemczech pokazuje, że większość spraw związanych z cyberprzestrzenią dotyczy

[221] Niemiecki Kodeks Postępowania Cywilnego, Zivilprozessordnung (ZPO) Opublikowany 5 grudnia 2005 (Bundesgesetzblatt (BGBl., Federal Law Gazette) I page 3202; 2006 I page 431; 2007 I page 1781), art. 29 - 40.

roszczeń w zakresie ochrony konsumentów. Miejscem właściwym do rozstrzygnięcia sporu będzie sąd miejsca zamieszkania konsumenta. Jeżeli więc niemiecki konsument ma zamiar dochodzenia praw wynikających z umowy zawartej przez Internet z zagranicznym kontrahentem, to może on dochodzić swoich praw w sądach niemieckich.

Wielka Brytania

Pojęcie jurysdykcji (ang. *jurisdiction*) w cywilnym systemie *common law* jest rozpatrywane w kontekście tego, czy sądom krajowym przysługuje prawo do rozstrzygnięcia konkretnej sprawy. Za jurysdykcję sądową w prawie angielskim uważa się prawne umocowanie i władzę sądu do wydania orzeczenia wiążącego strony w sprawie należycie wniesionej przed ten sąd. Jurysdykcja taka ma dwojaką postać. W pierwszej kolejności dotyczy rozstrzygnięcia, który z angielskich sądów będzie właściwy do rozstrzygnięcia sprawy, drugi aspekt odnosi się zaś do występującego w sprawie elementu zagranicznego, a mianowicie do kwestii, które państwo może sprawę rozpoznać. Podstawą zasadą jurysdykcyjną jest oczywiście zasada terytorialności, według której jurysdykcja odnosi się jedynie do osób zamieszkałych w kraju, rzeczy położonych na jego terytorium bądź powstałych tam zobowiązań[222].

W prawie anglosaskim istnieją wyjątki powodujące rozszerzenie bądź zawężenie jurysdykcji terytorialnej. Do rozszerzenia jego prawa może dojść na przykład w przypadku poddania się przez strony pod jurysdykcję sądów angielskich. Do zawężenia z kolei dochodzi w przypadku wyłączeń wynikających na przykład z immunitetów. Prawo angielskie wyróżnia trzy rodzaje ograniczeń, wyłączającą jurysdykcję sądów angielskich. Należą do nich:

- ograniczenia dotyczące przedmiotu sporu np. nieruchomości poza granicami Zjednoczonego Królestwa, zagranicznych praw własności intelektualnej,
- ograniczenia dotyczące rodzaju dochodzonej ochrony np. dotyczącego statusu małżeńskiego stron,
- ograniczenia dotyczące stron postępowania np. przedstawicieli obcych państw[223].

[222] K. Weitz, *Jurysdykcja …*, s. 61.
[223] Ibidem, s. 61 - 62.

Regulacje pozaeuropejskie

Stany Zjednoczone

Trudno jest mówić o zunifikowanych zasadach jurysdykcji cywilnej na terenie Stanów Zjednoczonych. W kraju tym mamy do czynienia z prawem federalnym, stanowym i miejscowym wzbogaconym nie tylko o prawo stanowione, ale również system precedensowy. Możemy wyróżnić pewne wspólne cechy amerykańskiej procedury cywilnej.

W prawie amerykańskim jurysdykcja sądowa obejmuje prawo do wydania rozstrzygnięcia w stosunku do konkretnej osoby lub rzeczy (ang. *personal jurisdiction* - w ramach której wyszczególnić można *jurisdiction in personam, in rem* oraz *quasi in rem*) oraz kompetencję do rozstrzygnięcia poszczególnych kategorii spraw (ang. *subject matter jurisdiction*)[224]. Bierna jurysdykcja personalna opiera się na Due Process Clause, według której pozwany, by podlegać prawu konkretnego sądu musi posiadać chociażby minimalny łącznik z państwem forum (stanem forum), tak by miał on świadomość, że może podlegać pod jurysdykcję tego państwa[225]. Wykonywanie jurysdykcji personalnej musi zatem być sprawiedliwe i rozsądne. Można ponadto wyróżnić jurysdykcję rzeczową (ang. *subject matter jurisdiction*), która wskazuje na przedmiot sporu (ang. *basis of the suit*), jurysdykcję miejscową (ang. *local jurisdiction*), która ma na celu wskazanie sądu właściwego do rozstrzygnięcia sprawy. W odniesieniu do jurysdykcji miejscowej w większości amerykańskich stanów obowiązuje zasada tak zwanego długiego ramienia sądów (ang. *long - arm statutes),* która ma na celu rozszerzeniu granic jurysdykcyjnych poza granice stanów. Zgodnie z obowiązującymi przepisami prawa, jeżeli właściwość sądu jest niewygodna dla jednej ze stron sporu, może ona kwestionować jurysdykcję opierając się na zasadzie *forum non conveniens*[226].

W początkowych etapach rozwoju cyberprzestrzeni sądy amerykańskie przyjmowały dość szerokie podstawy jurysdykcyjne. Trend ten można zaobserwować w sprawie z 1996 roku z powództwa spółki *Inset Systems Inc*. z siedzibą w Connecticut przeciwko *Instruction*

[224] Ibidem, s. 62-63.
[225] E.S. Moore, *Cyber jurisdiction*, "Virginia Lawyer Magazine" kwiecień 2002, s. 28-29.
[226] R. Tokarczyk, *Prawo amerykańskie*, Warszawa 2011, s. 129.

Set Inc. z siedzibą w Massachusetts (sprawa Insert Systems[227]). Stan faktyczny sprawy wyglądał następująco. Firma Instruction Set Inc. była właścicielem domeny www.inset.com, którą wykorzystywała do promowania swoich produktów w Internecie. Powodowa spółka Inset Systems Inc. uznała, że działalność pozwanego narusza jej prawa do znaku towarowego „Inset". Sąd w Connecticut uznał swoją właściwość do rozpoznania sprawy, na tej podstawie że pozwana spółka prowadząc reklamę ciągłą (ang. *continuous advertisement*) za pomocą strony internetowej w sposób ciągły kierowała swą działalność na obszar Connecticut. W ocenie sądu pozwany winien zatem liczyć się z możliwością pozwania przed sądem stanu Connecticut[228].

Wyrok ten wzbudził falę krytyki w doktrynie amerykańskiej. Znawcy prawa zarzucili sądowi, że przy rozpatrywaniu sprawy nie wziął on pod uwagę specyfiki Internetu i stron internetowych. Podniesiono, że tak szerokie podejście jurysdykcyjne może ograniczyć, a nawet sparaliżować komercyjny rozwój przestrzeni wirtualnej, gdyż przedsiębiorcy będą obawiać się prowadzenia działalności gospodarczej w cyberprzestrzeni ze względu na niepewność prawną i możliwość pozwania w dowolnym miejscu na świecie[229].

Podobna próba rozszerzenia granic jurysdykcji miała miejsce w stanie Minnesota, w której prokurator generalny Huber Humprey III w oficjalnym oświadczeniu stwierdził, że „osoby spoza Minnesoty, które przekazują informacje przez Internet wiedząc, że informacje te będą rozpowszechniane w Minnesocie, będą podlegały jurysdykcji sądów Minnesoty za naruszenie przepisów prawa karnego i cywilnego"[230]. Nota ta i wynikające z niej wytyczne były obowiązującą wykładnią prawa wprowadzającą jurysdykcję stanu Minnesota wyłącznie na tej podstawie, że informacje umieszczone w Internecie były dostępne na jej terytorium. Konsekwencją takiej interpretacji był między innymi wyrok *Minnesota v. Granite Gate Resorts*[231], gdzie uznano właściwość sądu w Minnesocie na podstawie tego, że w czasie dwóch tygodni w lutym i marcu 1996 roku co najmniej 248 komputerów w Minnesocie miało dostęp do danych strony internetowej pozwanego. Podobny argument został przyjęty przez

[227] Wyrok Sądu Rejonowego dla Okręgu Connecticut, z dnia 17 kwietnia 1996 r., w sprawie *Inset Systems, Inc. przeciwko Instruction Set, Inc.*, sygn. akt 937 F. Supp. 161 (D. Conn. 1996).
[228] D. Karwala, op. cit., s. 308.
[229] Ibidem, s. 308.
[230] Nota oficjalna Prokuratora Generalnego Minnesoty (18.07.1995), zob.: J. Czekalska, *Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych*, „Państwo i Prawo" 2004, nr 11, s. 76.
[231] Wyrok Sądu Rejonowego w Minesocie, z dnia 11 grudnia 1996 r., w sprawie *Minnesota przeciwko Granite Gate Resorts*, sygn. akt 658 N.W.2d, 718.

sędziego w sprawie *Maritz v. Cybergold*[232]. Obecnie zarówno w doktrynie amerykańskiej, europejskiej, jak i polskiej wyrażona wyżej koncepcja nie znajduje aprobaty. Akt miejscowy *de facto* poddał całą cyberprzestrzeń i wszelkie dostępne w niej dane pod jurysdykcję stanu Minnesota. Praktyka taka jest nie do zaakceptowania nie tylko ze względów politycznych, ale przede wszystkim praktycznych[233].

Sprawa *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*., 952 F. Supp. 1119 (W.D. Pa. 1997)[234] dotyczyła powództwa firmy produkującej znane zapalniczki Zippo Manufacturing Co. przeciwko kalifornijskiej spółce prowadzącej stronę internetową o nazwie Zippo, na której użytkownicy mieli możliwość korzystania z usług oferowanych przez spółkę. Według powodowej spółki pozwany narusza jej znak towarowy „Zippo". Orzeczenie określiło trzy ogólne kategorie obecności użytkownika w Internecie, tworząc podwaliny pod trzy główne kierunki orzecznicze w Stanach Zjednoczonych dotyczące stron internetowych. Pierwsza kategoria dotyczy pasywnych stron internetowych, na których zamieszczone są informacje o danej treści, lecz nie dają możliwości interakcji z użytkownikiem, czyli nie wprowadzają możliwości zakupu towaru czy skorzystania z usługi. Druga kategoria stron internetowych ma charakter pasywno – aktywny, gdzie istnieje możliwość dokonania pewnych czynności przez użytkownika. Wówczas sąd musi dokonać analizy poziomu interaktywności z klientem bądź użytkownikiem w celu określenia swojej ewentualnej jurysdykcji. Trzecia kategoria dotyczy z kolei witryn internetowych, w których przedsiębiorca aktywnie prowadzi działalność gospodarczą, oferując towary i usługi na miejscu oraz *on-line*. Zwolennicy tej kategorii uznają, iż sądy mają wówczas pełną jurysdykcję.[235]

Ocena interaktywności, czyli „aktywności" czy też „pasywności" stron internetowych w doktrynie amerykańskiej określa się jako „test Zippo". Uznaje się, że „kluczowa jest ocena charakteru strony internetowej, za pomocą której prowadzona jest działalność handlowa, w tym zawierane są umowy z użytkownikami sieci. Witryny aktywne (*active web-sites*) znajdują się jednej stronie »ruchomej skali« (*sliding scale/ continuum*). Strony takie pozwalają na wprowadzanie danych przez użytkowników, w szczególności składanie zamówień za pośrednictwem formularzy dostępnych na stronie. Na drugim końcu skali

[232] Wyrok Sądu Okręgowego Wschodniego Missouri, z dnia 19 sierpnia 1996 r., w sprawie *Maritz przeciwko Cybergold*, 947 F, sygn. akt Supp. 1328 (E.D. Mo.1996)
[233] J. Czekalska, *Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych*, „Państwo i Prawo" 2004, nr 11, s. 76-77.
[234] Wyrok Sądu Rejonowego Zachodniej Pensylwanii, z dnia 16 stycznia 1997 r., w sprawie *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*., o sygn. akt. 952 F. Supp. 1119 (W.D. Pa. 1997).
[235] E.S. Moore, op. cit., s. 29.

znajdują się tzw. strony pasywne (*passive web-sites*), które takich właściwości nie przejawiają, ograniczając się do aspektu informacyjnego (podanie informacji handlowych, ofert lub reklam) na temat produktów czy usług danego przedsiębiorcy. Pośrodku lokuje się niezwykle pojemne spektrum witryn, których jednoznaczna kwalifikacja nie jest prosta, z uwagi na fakt, iż strony te pozwalają co prawda użytkownikom komunikować się z serwerem, na którym użytkowana była dana strona, jednak poziom tej komunikacji nie jest na tyle wystarczający, aby jednoznacznie przesądzić o »aktywności« strony. Operacje przeprowadzane za pośrednictwem stron aktywnych (»kontakt« z użytkownikami) przesądzały o występowaniu minimalnego związku (*minimal contact*) z terytorium forum, co w konsekwencji pozwalało sądowi uznać jurysdykcję w sprawie. Z kolei strona pasywna wykluczała jurysdykcję ze względu na brak realizacji konstytucyjnej zasady prawa amerykańskiego, czyli zasady minimalnego związku".[236] Mimo znacznej popularności „testu Zippo" dostrzeżono, iż nie można go zastosować w stosunku do każdego konfliktu jurysdykcyjnego w cyberprzestrzeni. Nie ma możliwości zastosowania testu aktywności bądź pasywności strony do wszystkich witryn internetowych - zwłaszcza obecnie, gdy strony internetowe stają się coraz bardziej zaawansowane technologicznie i zdarza się, że są częściowo pasywne, a częściowo aktywne.

Brak jednolitej praktyki spowodował, iż część sądów uznawała dane witryny za pasywne, inne zaś za częściowo pasywne. Doprowadziło to wydania zupełnie sprzecznych wyroków w dość podobnych sprawach. Sądy uznawały, iż nie ma podstaw do stwierdzenia jurysdykcji między innymi. w sprawach *Revell przeciwko Lindov*[237], *Cybersell Inc. przeciwko Cybersell Inc*.[238] Zupełnie odmiennie orzeczono między innymi we wspomnianej wcześniej sprawie *Inset Systems, Inc. v. Instruction Set, Inc*. W sprawach aktywnych stron internetowych sądy amerykańskie zazwyczaj nie miały problemów z zastosowaniem jurysdykcji personalnej w odniesieniu do dostawców tych stron tak jak np. w sprawie internetowej księgarni *Rainy Day Books, Inc. przeciwko Rainy Day Books & Café, L.L.C,*[239]

[236] D. Karwala, op. cit., s. 312.
[237] Wyrok Sądu Apleacyjnego Piątego Okręgu, z dnia 31 grudnia 2002 r., w sprawie *Revell przeciwko Lindov*, o sygn. akt 317 F 3d 467 (2002).
[238] Wyrok Sądu Rejonowego w Arizonie, z dnia 2 grudnia 1997 r,, w sprawie *Cybersell Inc. v. Cybersell Inc*. o sygn. akt 130 F.3d 414 (9th Cir. Dec. 1997).
[239] Wyrok Sądu Rejonowego w Kansas, z dnia 05 lutego 2002 r. w sprawie *Rainy Day Books, Inc. przeciwko Rainy Day Books & Café, L.L.C,* o sygn. akt 186 F.Supp.2d 1158 (2002).

czy rozpowszechniania oprogramowania komputerowego za pomocą internetowej sieci powoda *Compuserve, Inc. przeciwko Patterson*[240].

Wobec problematyki rozszerzania jurysdykcji przekazów internetowych, która nie sprzyja obrotowi elektronicznemu i pewności prawnej skutków zachowań w cyberprzestrzeni w sądach wielu państw, a zwłaszcza sądach amerykańskich doszło do zmiany poglądów. W chwili obecnej zarówno krajowi, jak i zagraniczni znawcy tematu nie mają wątpliwości, że potencjalna dostępność strony internetowej nie powinna być wyłącznym łącznikiem do określenia jurysdykcji w cyberprzestrzeni[241].

Przedstawiciele doktryny stwierdzili, iż opracowanie podstaw jurysdykcji w cyberprzestrzeni winno być oparte na neutralności technologicznej tak by nie była podatna na szybkie zmiany technologiczne. Uznano, iż odpowiednie będzie zastosowanie „doktryny skutków" ustanowionej w orzeczeniu Sądu Najwyższego USA w sprawie *Calder przeciwko Jones*[242], dzięki któremu można było zastosować jurysdykcję państwa forum oceniając faktyczne skutki, jaki dany czyn wywoływał. Kluczową kwestią były intencje podmiotu, który działa w cyberprzestrzeni ze świadomością, że skutki tych działań mogą być odczuwalne w innych państwach czy też stanach[243].

Indie

Sądy indyjskie w sprawach cywilnych kwestię sądu właściwego rozstrzygają głównie opierając się na zasadzie jurysdykcji personalnej, w tym do działalności człowieka w cyberprzestrzeni. Stosując zasadę właściwości *legis fori* sądy indyjskie uznają się za właściwe do rozstrzygnięcia sporu[244]. Zasada jurysdykcji personalnej znalazła oparcie w przepisach indyjskiego kodeksu postępowania cywilnego z 1908 r. (ang. *Code of Civil Procedure*)[245]. Nie określa on żadnego odrębnego zestawu zasad jurysdykcji w przypadku sporów

[240] Wyrok Sądu Apelacyjnego Szóstego Okręgu, z dnia 22 lipca 1996 r, w sprawie *Compuserve, Inc. przeciwko Patterson*, o sygn. akt 89 F.3d 1257.
[241] D. Karwala, op. cit., s. 310.
[242] Wyrok Sądu Najwyższego USA, z dnia 20 marca 1984 r., w sprawie *Calder przeciwko Jones*, sygn. akt 465 U.S. 783(1984).
[243] D. Karwala, op. cit., s. 315.
[244] B. R. Lashkari, *Issue of jurisdiction under cyber law in India*, Racolblegal. Artykuł dostępny na: http://racolblegal.com/issue-of-jurisdiction-under-cyber-law-in-india/ [07.09.2016].
[245] The Code Of Civil Procedure of India, 1908 (Act No. 5 of 1908).

międzynarodowych prywatnych. Uwzględnia natomiast szczególne przepisy dotyczące spełnienia wymogów obsługujących procedurę poza granice terytorialne[246].

Dodatkowo w prawie indyjskim można posiłkować się zasadą jurysdykcji rzeczowej w sprawach ściśle określonych w kodeksie postępowania cywilnego. Zasada ta znajdzie zastosowanie w odniesieniu do pozwów dotyczących nieruchomości, ruchomości i szkód na osobach. Zasada właściwości miejscowej zostanie zastosowana, jeżeli pozwany w momencie wytoczenia powództwa zamieszkuje, przebywa lub prowadzi działalność na obszarze działalności sądu[247]. Każdemu sądowi indyjskiemu przyznano prawo do badania swej własnej jurysdykcji, z tym że strony mogą zakwestionować taką decyzję. W takich przypadkach ciężar dowodu do udowodnienia jurysdykcji innego sądu spoczywa na stronie, która wywodzi taki wniosek[248].

Tak jak w innych systemach prawnych, strony zawierając umowę mogą zastosować klauzulę jurysdykcyjną, ale indyjskie sądy nie pozwolą na rozstrzygnięcie sprawy przez sąd, który w żaden sposób nie ma związku ze sprawą. Uznaje się bowiem, że autonomia stron co do wyboru sądu jest dozwolona, ale nie kosztem poddania się pod jurysdykcję zupełnie dowolnego sądu - działając sprzecznie z dobrem wymiaru sprawiedliwości. Na podstawie sekcji 20 indyjskiego k.p.c. sądy decydują o właściwości na podstawie miejsca zamieszkania stron w granicach terytorialnych obwodu sądowego, miejsca prowadzenia tam działalności, nawet jeżeli obecnie strony tam nie przebywają. Sądy również uznają swoją jurysdykcję w przypadku, gdy skutek wystąpił na terytorium działania sądu. Oznacza to, iż posiłkując się zasadą wystąpienia skutku mogą oni orzekać również w sprawach dotyczących cudzoziemców, nie mających w Indiach miejsca pobytu, jeżeli łącznie zostaną spełnione trzy warunki:

1) działalność pozwanego miała wystarczający związek z państwem forum (Indiami),
2) niezależnie od działania pozwanego skutek następuje w państwie forum,
3) wykonanie jurysdykcji w Indiach byłoby rozsądne[249].

---

[246] S. Dwivedi, *Jurisdictional Issues in Cyber Crime*. [online] Academia.edu. Artykuł dostępny na http://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime [07.09.2016].
[247] B. R. Lashkari, op. cit.
248 S. Ojha, *Jurisdiction Of Civil Court Under Civil Procedure Code*, artykuł dostępny online: http://www.legalservicesindia.com/article/article/jurisdiction-of-civil-court-under-civil-procedure-code-508-1.html [07.09.2017].
[249] B. R. Lashkari, op. cit.

Jeżeli zatem okaże się, że inny sąd ma lepszą podstawę jurysdykcji to sprawa zostanie przekazana mu według właściwości.

Kwestia jurysdykcji cywilnej w cyberprzestrzeni została uregulowana w ustawie o technologiach informacyjnych z 2000 r. (*Information Technology Act 2000*). Ustawa została oparta na ustawie modelowej UNCITRAL z 1996 r. Akt prawny znajdzie zastosowanie, jeżeli obie strony mają miejsce zamieszkania bądź siedzibę w Indiach. Ustawa została stworzona specjalnie w celu rozstrzygania sporów w cyberprzestrzeni z udziałem osób przebywających na terytorium Indii. Ustawa wprowadza:

1. Urzędników orzekających (ang. *Adjudicating Officers*) - którzy są mianowani przez administratora. Ich zadaniem jest podjęcie decyzji o lokalizacji geograficznej - właściwości terytorialnej wg której strony mogłyby rozstrzygnąć spór.
2. Sąd Apelacyjny do spraw cyberregulacji (ang. *Cyber Regulations Appellate Tribunal*) - sąd ten jest ustanowiony przez rząd. Rozpatruje sprawy odwoławcze od decyzji urzędników orzekających.
3. Sąd Najwyższy (ang. *High Court*) - do którego mogą odwołać się (w ciągu 60 dni) strony niezadowolone z decyzji Sądu Apelacyjnego ds. cyberregulacji[250].

Jeżeli jednak żadna bądź wyłącznie jedna ze stron posiada miejsce zamieszkania bądź siedzibę na terytorium Indii, ustawa nie znajdzie zastosowania; ma zatem charakter wyłącznie wewnętrzny, rozstrzygający spory w cyberprzestrzeni między osobami przebywającymi na terytorium Indii.

2.1.3 Jurysdykcja karna

Michał Płachta definiuje jurysdykcję karną jako „uprawnienie organów danego państwa do rozpoznawania i rozstrzygania spraw o przestępstwa na podstawie jego ustawodawstwa karnego oraz wykonywania orzeczonych kar i środków karnych. Pojęcie »ustawodawstwa karnego« obejmuje nie tylko wszystkie przepisy związane z obowiązującym w tym państwie ustawach karnych, lecz także postanowienia traktatów międzynarodowych,

[250] Ibidem.

które weszły w skład krajowego systemu prawnego. Całokształt tych przepisów stanowi materialnoprawną podstawę jurysdykcji"[251]. Wykonywanie jurysdykcji karnej przez państwa może nastąpić przez zastosowanie tak zwanych zasad jurysdykcyjnych. Zasady te, podobnie jak w prawie cywilnym, zostały skonstruowane opierając się na łączniku jurysdykcyjnym, przez który rozumie się istnienie pewnych okoliczności faktycznych, które łączą sprawę z określonym państwem. Istnienie takiego łącznika powoduje, iż państwo może zastosować własną jurysdykcję w danej sprawie[252].

Wśród formalnych przesłanek do nałożenia odpowiedzialności karnej w przypadku przestępstw z elementem obcym jurysdykcja odgrywa szczególną rolę. W przypadku konfliktu jurysdykcyjnego, niezbędne wydaje się dogłębne zbadanie systemów prawnych, które mogą mieć zastosowanie. Tradycyjny anglo - amerykański system prawa karnego z zasady nie przykładał szczególnej uwagi do kwestii jurysdykcji, przyjmując zasadę jurysdykcji terytorialnej. Nawet obecnie jurysdykcja karna w systemie prawa *common law* jest traktowana jako synonim terytorialności[253].

W prawie międzynarodowym wykształciło się kilka podstawowych sposobów ustalania jurysdykcji karnej[254]. Jest to: zasada jurysdykcji terytorialnej, personalnej ochronnej i uniwersalnej. Malcom N. Show podkreśla jednak, że państwo stosując jurysdykcję nie ma obowiązku stosowania wszystkich wymienionych wyżej zasad. O sposobie ustalenia jurysdykcji karnej decyduje przede wszystkim prawo krajowe[255].

Zaakcentować należy, że w prawie karnym nie obowiązuje zasada jurysdykcji wyłącznej (e*xperssio unius est exclusio alterius*). Oznacza to, że kilka państw może mieć łącznik ze sprawą i żądać zastosowania swojej jurysdykcji krajowej. Taki konflikt jurysdykcyjny może mieć dwojaki charakter:

1) jednozasadowy - gdy kilka państw uzasadnia swoją jurysdykcję możliwością zastosowania zasady terytorialnej (na przykład gdy za miejsce popełnienia przestępstwa może być uznane miejsce działania lub zaniechania sprawcy lub też miejsce wystąpienia skutku),

[251] M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: pojęcie …*, s. 6.
[252] T. Ostropolski, *Zapobieganie …*, s. 98.
[253] M. Dirk Dubber, *Comparative Criminal Law*, [w:] M. Reimann, R. Zimmermann (red.), *The Oxford Handbook of Comparative Law*, Oxford 2006, s. 1311.
[254] Zob. E. Karska, *Karna jurysdykcja krajowa a międzynarodowa*, [w:] J. Kolasa (red.), *Współczesne sądownictwo międzynarodowe, Tom 2 Wybrane zagadnienia prawne*, Wrocław 2010.
[255] M.N. Shaw, *Prawo międzynarodowe*, Warszawa 2011, s. 415.

2) wielozasadowy - będzie miał miejsce gdy kilka państw wykonuje swoją jurysdykcję na podstawie innej zasady (na przykład zwierzchnictwa personalnego, ochronnej, terytorialnej)[256].

Powstanie konfliktu jurysdykcyjnego rodzi niebezpieczeństwo naruszenia zasady *ne bis in idem.* O ile przyjęcie tej zasady w ustawodawstwach krajowych jest już kanonem, o tyle na gruncie prawa międzynarodowego nie wypracowano jeszcze powszechnej reguły zakazującej organom sprawiedliwości danego państwa do ścigania i skazania oskarżonego za czyn, za który był już skazany (a nawet odbył już karę) w innym państwie[257]. Istnienie konfliktów jurysdykcyjnych nie zawsze jednak należy postrzegać jako zjawisko negatywne. Tomasz Ostropolski postawił tezę, że: „istnienie jurysdykcji konkurencyjnej umożliwia skuteczniejszą walkę z przestępczością poprzez zapobiegnięcie lukom kompetencyjnym i uszczelnienie ścigania karnego"[258]. Eliminacja luk prawnych następuje również w przypadku przestępstw konwencyjnych (czyli takich, których ściganie i karalność zobowiązują umowy międzynarodowe). Traktaty o takim charakterze nakładają na państwa strony obowiązek uznania danego czynu za przestępstwo w prawie krajowym, wzywają strony na terytorium których doszło do zatrzymania sprawcy do jego osądzenia lub ekstradycji[259].

2.1.3.1. Zasady jurysdykcji karnej

Konflikty jurysdykcyjne można rozstrzygnąć stosując jedną z zasad jurysdykcyjnych - zasadę terytorialności, zasadę personalną, zasadę ochronną czy też zasadę uniwersalną. W niniejszym podrozdziale zostaną omówione wszystkie zasady jurysdykcyjne stosowane w prawie karnym.

Zasada jurysdykcji terytorialnej

Podstawowym łącznikiem jurysdykcyjnym stosowanym niemal na całym świecie jest łącznik terytorialny. Prawo międzynarodowe przewiduje, że wszelkie osoby, rzeczy i

[256] T. Ostropolski, *Zapobieganie …*, s. 102.
[257] M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: propozycja rozwiązania w Unii Europejskiej*, „Studia Europejskie" 2010, nr 2, s. 136.
[258] T. Ostropolski, *Zapobieganie …*, s. 102.
[259] Ibidem, s. 102.

zdarzenia mające miejsce na terytorium danego państwa znajdują się pod jego jurysdykcją. Rozwiązanie takie jest niezwykle praktyczne, bo to zazwyczaj na terytorium państwa forum znajduje się sprawca i osoba poszkodowana lub też występuje sama szkoda. Nie bez znaczenia pozostaje również łatwość i efektywność prowadzenia postępowania karnego, zebrania dowodów i osądzenia sprawcy. Jak wskazuje Malcolm N. Shaw „założenie, iż państwo powinno być zdolne do ścigania przestępstw popełnionych na jego terytorium, stanowi logiczny przejaw światowego porządku opartego na suwerennych państwach i jest całkowicie racjonalne, ponieważ władze państwowe ponoszą odpowiedzialność za stanowienie i egzekwowanie prawa oraz utrzymanie porządku prawnego na swoim terytorium"[260].

Wykonywanie władztwa nad terytorium państwa nie ogranicza się wyłącznie do samego lądu, lecz rozciąga się również na wody wewnętrzne, morze terytorialne, wody archipelagowe w przypadku państw archipelagowych oraz przestrzeń powietrzną nad tymi obszarami[261]. Podkreślić również należy, iż państwo ma również uprawnienia do wykonywania władztwa w obszarach o ograniczonej jurysdykcji, czyli w wyłącznej strefie ekonomicznej oraz na szelfie kontynentalnym. Obszary te nie wchodzą w skład terytorium państwowego, jednakże państwu zostały przyznane pewne uprawnienia w przypadku określonych działań podejmowanych przez inne podmioty[262].

Jurysdykcja terytorialna rozciąga się również na obszary uznawane za quasi - terytorium państwa, czyli na pokłady statków morskich i powietrznych. O przynależności statku decyduje jego rejestracja według prawa wewnętrznego każdego z państw. Statki morskie i powietrzne znajdujące się na terytorium niepodlegającym niczyjej jurysdykcji, na przykład na morzu otwartym, znajdują się pod wyłączną jurysdykcją państwa bandery (w przypadku statków morskich) lub państwa rejestracji (w przypadku samolotów).

Istnieje jednakże szereg umów międzynarodowych ograniczających tą generalną zasadę. Przykładowo, konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi sporządzona w Hadze dnia 16 grudnia 1970 r.[263] stanowi w art. 4 ust. 1 pkt. b, iż każde umawiające się Państwo podejmie w związku z przestępstwem takie środki, jakie

[260] M.N. Shaw, *Prawo*... 2006, s. 376.
[261] B.H. Oxman, *Jurisdiction of States*, [w:] R.L. Bindschedler, T. Buergenthal (red.), *Encyclopedia of Public International Law*, t. 3, Amsterdam 1997, s. 57.
[262] Ibidem, s. 57.
[263] Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi sporządzona w Hadze dnia 16 grudnia 1970 r., Dz.U. z 1972 r., Nr 25, poz. 181.

będą konieczne dla ustanowienia swej jurysdykcji w sprawach o przestępstwo oraz o każdy inny czyn użycia przemocy w stosunku do pasażerów lub załogi popełniony przez domniemanego sprawcę przestępstwa, gdy statek powietrzny, na pokładzie którego przestępstwo zostało popełnione, ląduje na jego terytorium z domniemanym sprawcą przestępstwa znajdującym się na jego pokładzie. W art. 8 ust. 4 konwencji wskazano, iż dla celów ekstradycji pomiędzy państwami - stronami konwencji przestępstwo uważa się za dokonane tak w miejscu jego popełnienia, jak i na terytorium państw zobowiązanych do ustanowienia swej jurysdykcji zgodnie z art. 4 ust 1. konwencja zawiera więc fikcję prawną rozciągającą zwierzchnictwo terytorialne i jurysdykcję na obszary, na których *de facto* przestępstwa nie popełniono[264].

Neil Boister wskazuje, że to postanowienie rozciąga zasadę terytorialności państwa na terytorium, którego statek powietrzny ląduje nawet w sytuacji, gdy przestępstwo zostało popełnione na pokładzie samolotu innego państwa (czyli na quasi-terytorium innego państwa), a domniemany sprawca został już aresztowany przed lądowaniem. W odpowiedzi na wskazane wyżej postanowienia Konwencji Stany Zjednoczone rozciągnęły swoją jurysdykcję na porwania samolotów popełnione poza granicami USA, jeżeli samolot wylądował na ich terytorium z domniemanym sprawcą na pokładzie. Stwierdzono, iż nie jest wymagany żaden łącznik terytorialny czy też personalny do rozciągnięcia swojej jurysdykcji we wskazanych przypadkach[265] .

Kolejnym zagadnieniem, które należy w tym miejscu poruszyć jest subiektywna i obiektywna „wszechobecna terytorialność" (ang. *subjective and objective territoriality ubiquity*). Zasada jurysdykcji terytorialnej przybiera postać obiektywną głównie w systemie *common law*, który wiąże możliwość wykonywania władztwa karnego z miejscem nastąpienia skutku przestępstwa. Postać subiektywna z kolei łączy jurysdykcję z miejscem czynu sprawcy[266].

Neil Boister wskazuje, iż subiektywna terytorialność (ang. *subjective territoriality*) występuje wówczas, gdy tylko część elementów przestępstwa występuje na terytorium państwa, np. gdy czyn został zapoczątkowany w państwie forum, ale skutek następuje za granicą. Boister podnosi, że nawet jeżeli w państwie, w którym według zamiaru sprawcy

[264] N. Boister, *An Introduction to Transnational Criminal Law*, Oxford 2012, s. 139-140.
[265] Ibidem, s. 139-140.
[266] A. Adamski, *Podstawy jurysdykcji cyberprzestępstw w prawie porównawczym*, [w:] T. Jasudowicz, M. Balcerzak (red.), *Księga pamiątkowa ku czci Profesora Jana Białocerkiewicza*, t. 2, Toruń 2009, s. 938-939.

skutek miał nastąpić, szkoda nie wystąpiła, to państwo może być zainteresowane ściganiem i ukaraniem sprawcy, jeżeli w państwie działania sprawcy organy sprawiedliwości nie mogą skutecznie hamować tego typu działań przestępczych[267].

Obiektywna terytorialność (ang. *objective terriroriality*) będzie miała zastosowanie wówczas, gdy transnarodowe przestępstwo jest zainicjowane za granicą, ale zostaje ukończone w państwie forum. Podobnie jak w przypadku subiektywnej terytorialności tylko jeden z elementów przestępstwa następuje w państwie forum[268].

Użycie wskazanych wyżej zasad jurysdykcyjnych może w praktyce doprowadzać do nieograniczonego rozszerzania władztwa jurysdykcyjnego państwa. Rozciągnięcie jurysdykcji może być uzasadnione chociażby w przypadku elektronicznego prania brudnych pieniędzy za pomocą banku znajdującego się na terytorium państwa forum. Jako przykład zastosowania obiektywnej i subiektywnej zasady terytorialności wskazać można przepis dotyczący prania pieniędzy w amerykańskim kodeksie karnym - art. 18 § 1956 (2) stanowiący, że amerykańską jurysdykcję stosuje się wobec każdego, kto przesyła, przewozi czy przenosi albo próbuje przesłać, przewieźć lub przenieść instrument pieniężny lub fundusze płatnicze z miejsca w Stanach Zjednoczonych do albo z miejsca poza granicami Stanów Zjednoczonych albo przez lub na terytorium Stanów Zjednoczonych z zagranicy[269].

Stały Trybunał Sprawiedliwości Międzynarodowej w sprawie *Lotus*[270], poruszając kwestię konfliktów jurysdykcyjnych stwierdził, iż „prawo międzynarodowe zabrania państwu wykonywania jurysdykcji na własnym terytorium w jakiejkolwiek sprawie, dotyczącej czynów, które miały miejsce poza granicami państwa i w odniesieniu do których nie może ono powołać się na określoną normę przyzwalającą prawa międzynarodowego”[271]. Trybunał nie przychylił się do argumentacji Francji jakoby wyłączną jurysdykcję w stosunku do statku znajdującego się na morzu pełnym miało państwo bandery, gdyż brak jest w prawie międzynarodowym normy prawnej o takiej treści. Podniesiono ponadto, iż zatopienie tureckiego statku jest równoznaczne z naruszeniem integralności terytorialnej Turcji, co dało

[267] N. Boister, op. cit., s. 140.
[268] Ibidem, s. 140.
[269] N. Boister, op. cit., s. 140- 141.
[270] Wyrok Stałego Trybunału Sprawiedliwości Międzynarodowej, z dnia 7 września 1927 r., s*prawa "Lotus" Francja v. Turcja*, sygn. akt P.C.I.J. Ser. A, nr 10, s. 4 (1927).
[271] M.N. Shaw, *Prawo*... 2006, s. 378.

temu państwu uprawnienie do wykonania jurysdykcji na podstawie obiektywnej zasady terytorialności[272].

Jak podkreśla Bernard H. Oxman Trybunał w orzeczeniu *Lotus* nie nawiązał do kwestii jurysdykcji w przypadku, gdy osoba swoim zachowaniem popełnia przestępstwo na terytorium innego państwa nie wiedząc, że postępowanie takie jest w określonym państwie karane. Trybunał w swych rozważaniach odniósł się jedynie do szkód fizycznych, pamiętać jednakże należy, iż pewne kategorie przestępstw mogą wywoływać szkody ekonomiczne również w innych państwach[273].

Zasada jurysdykcji personalnej

Podstawowym czynnikiem łączącym osobę fizyczną z danym państwem jest obywatelstwo. Na jego mocy jednostka jest uprawniona m.in. do otrzymania paszportu, opieki dyplomatycznej i konsularnej poza granicami kraju, uczestniczenia w wyborach. O sposobach nabycia obywatelstwa decyduje prawo wewnętrzne z każdego z państw. Można jednakże wyróżnić dwa podstawowe sposoby jego nabycia: poprzez urodzenie się z rodziców będących obywatelami danego państwa (*ius sanguinis*) lub też z tytułu narodzin w granicach terytorialnych państwa (*ius soli*)[274].

Należy podkreślić, iż zarówno czynna, jak i bierna zasada jurysdykcji uzależniona jest od spełnienia wymogu podwójnej karalności.

Zasada czynnej jurysdykcji personalnej

Zasada czynnej jurysdykcji personalnej (ang. *active personal jurisdiction*, fr. *compétence personnelle active*) zakłada jurysdykcję państwa obywatelstwa sprawcy, który popełnił przestępstwo poza terytorium swojego kraju. Czynna jurysdykcja ma wiele zalet, gdyż można ją stosować między innymi wobec dyplomatów posługujących się immunitetem jurysdykcyjnym czy też wobec żołnierzy, którzy w związku z pełnioną służbą popełnili

[272] Ibidem, s. 378.
[273] B.H. Oxman, op. cit., s. 57-58.
[274] M.N. Shaw, *Prawo*... 2006, s. 381.

przestępstwo poza granicami kraju[275]. Powodem stosowania zasady czynnej jurysdykcji personalnej jest przekonanie, iż obywatele mają obowiązek przestrzegać prawa danego państwa, niezależnie od tego gdzie się znajdują[276].

Zasada jurysdykcji czynnej jest stosowana w wielu państwach. Nierzadko możliwość pociągnięcia obywatela do odpowiedzialności karnej za czyn popełniony poza granicami kraju uzależniony jest od wymogu podwójnej karalności, czyli sytuacji, gdy czyn zabroniony obywatela jest również penalizowany w kraju, w którym dopuścił się przestępstwa. Państwa ograniczają możliwość stosowania tej zasady do określonego typu przestępstw lub też wyłącznie do czynów popełnionych na terytorium pozbawionym efektywnej władzy państwowej[277]. Joanna Kulesza ostrzega jednak, że „powszechne zastosowanie konstrukcji podwójnej przestępności z jednej strony przyczynić się może do zwiększenia skuteczności ścigania sprawców ataków, z drugiej zaś – wzmóc chaos prawny towarzyszący kwestii ataków cybernetycznych wobec odmiennej oceny tych działań przez władze poszczególnych państw. Jest to jedna z konsekwencji nieograniczonego zastosowania zasady jurysdykcji ochronnej wobec działań podejmowanych w cyberprzestrzeni, której zakres powinien zostać w kontekście Internetu doprecyzowany na poziomie międzynarodowym"[278].

Szczególnie silnym wyrazem stosowania zasady czynnej jurysdykcji personalnej jest stosowany w wielu państwach zakaz ekstradycji własnych obywateli państwom trzecim. Przepisy takie niejednokrotnie zostają zawarte w ustawach zasadniczych. Wprowadzenie takich norm ogranicza możliwość wykonywania kompetencji władczych przez inne państwa uznając, że obywatelstwo jest naczelną wartością uzasadniającą konieczność odpowiadania przed organami sądowniczymi własnego państwa. W literaturze wskazuje się, że zakazy ekstradycji własnych obywateli utrudniają znacząco walkę z przestępczością transgraniczną i posługiwania się takimi instrumentami jak Europejski Nakaz Aresztowania. Wiele państw zauważyło jednak potrzebę współpracy zagranicznej w przedmiocie ekstradycji i zmieniło obowiązujące w nich konstytucje tak jak między innymi Rzeczpospolita Polska w 2006 roku[279].

[275] N. Boiser, op. cit., s. 142-143.
[276] T. Ostropolski, *Zapobieganie …*, s. 100.
[277] Ibidem, s. 98.
[278] J. Kulesza, *Odpowiedzialność państw za podejmowane w cyberprzestrzeni działania zagrażające międzynarodowemu pokojowi i bezpieczeństwu*, „Studia Prawno - Ekonomiczne" 2011, t. 83, s. 161.
[279] T. Ostropolski, *Zapobieganie …*, s. 101.

Zasada biernej jurysdykcji personalnej

Zasada biernej jurysdykcji personalnej (ang. *passive personal jurisdiction,* fr. *compétence personnelle passive*) oznacza, iż państwo ma prawo do zastosowania własnej jurysdykcji karnej w stosunku do przestępstwa popełnionego poza jego granicami, jeżeli osobą poszkodowaną jest lub może być obywatel tego państwa[280]. Neil Boister akcentuje, że kraje systemu *common law* odrzuciły zasadę biernej jurysdykcji personalnej uznając, że jest ona zbyt szeroka, niedookreślona i może powodować konflikty jurysdykcyjne. Nie bez znaczenia pozostaje również fakt, iż sprawca przestępstwa może nawet nie przypuszczać, iż podejmowane przez niego działania są penalizowane w państwie trzecim[281].

Zasada jurysdykcji ochronnej

Zasada jurysdykcji ochronnej opiera się na założeniu, że państwo ma prawo wykonywać swoją jurysdykcję w odniesieniu do cudzoziemców, którzy popełnili za granicą czyn wywołujący negatywne skutki dla bezpieczeństwa danego państwa. Z czynami takimi będziemy mieli do czynienia w sytuacji, gdy cudzoziemiec popełnia w państwie trzecim czyn mogący zagrozić suwerenności, bezpieczeństwu, integralności państwa lub innym jego ważnym interesom państwowym lub gospodarczym[282]. Ogólnie przyjmuje się, że do tej kategorii czynów można zaliczyć np. szpiegostwo czy fałszerstwo dokumentów urzędowych. Za zasadzie jurysdykcji ochronnej bazują również współczesne ustawy antyterrorystyczne[283].

Malcolm N. Shaw twierdzi, iż „zasada ta znajduje odzwierciedlenie w ochronie żywotnych interesów państwa, gdyż nie można wykluczyć, iż zgodnie z prawem państwa w którym zamieszkuje cudzoziemiec mógłby on nie zostać uznany za przestępcę, a w przypadku przestępstw politycznych państwo mogłoby odrzucić wniosek o ekstradycję”[284]. W literaturze przedmiotu podnosi się, że sprawca musi działać z bezpośrednim lub nawet ewentualnym zamiarem naruszenia interesów państwa forum[285].

[280] M.N. Shaw, *Prawo*... 2006, s. 383.
[281] N. Boiser, op. cit., s. 142-145.
[282] N. Boiser, op. cit., s. 145.
[283] J. Kulesza, *Międzynarodowe…*, s. 32.
[284] M.N. Shaw, *Prawo*... 2006, s. 384.
[285] N. Boiser, op. cit., s. 145.

Również w polskim porządku prawnym uznano, w art. 112 k.k. że jurysdykcja powinna zostać rozszerzona wyłącznie w enumeratywnie wymienionych przypadkach, czyli popełnienia przestępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu RP, przeciwko polskim urzędom lub funkcjonariuszom publicznym, przestępstwa fałszywych zeznań złożonych wobec urzędu polskiego, przestępstwa, z którego została osiągnięta, chociażby pośrednio, korzyść majątkowa na terytorium Rzeczypospolitej Polskiej[286].

Zasada jurysdykcji uniwersalnej

Zasada jurysdykcji uniwersalnej, nazywana również zasadą uniwersalności, represji powszechnej lub wszechświatowej, opiera się na założeniu, iż do wykonywania kompetencji władczej państwa wobec jednostki nie jest potrzebny jakikolwiek łącznik terytorialny czy personalny. Na gruncie prawa międzynarodowego publicznego nie powstała jeszcze legalna definicja jurysdykcji uniwersalnej, jednakże można uznać, iż jest nią „upoważnienie wszystkich podmiotów prawa międzynarodowego do podejmowania czynności zmierzających do osądzenia oraz, jeżeli taki będzie wynik postępowania, do ukarania sprawcy najcięższych zbrodni w świetle prawa międzynarodowego, niezależnie od tego, kim jest sprawca i jego ofiary oraz gdzie została popełniona zbrodnia"[287]. Inna, bardziej szczegółowa, definicja została sformułowana w ust. 1 I Zasady z Princeton[288]: „przez jurysdykcję uniwersalną rozumie się jurysdykcję karną opartą wyłącznie na naturze przestępstwa, która może być wykonywana bez konieczności odwoływania się do łącznika miejsca popełnienia czynu, obywatelstwa oskarżonego, obywatelstwa ofiary lub jakiegokolwiek innego związku z państwem wykonującym jurysdykcję".

[286] Kodeks Karny, Dz.U. z 1997 r., Nr 88, poz. 553.
[287] M. Jeżewski, *Uniwersalna jurysdykcja karna w prawie międzynarodowym*, „Kwartalnik Prawa Publicznego" 2003, nr 2, s. 161.
[288] "The Princeton Project of Universal Jurisdiction" został ogłoszony 27.01.2001 roku. Jest to finalny efekt pracy prawników, specjalistów od międzynarodowego prawa karnego oraz sędziów, którzy obradowali nad możliwościami rozwoju koncepcji jurysdykcji uniwersalnej. W skład grupy roboczej weszli reprezentanci wszystkich głównych systemów prawnych połączeni ideą usprawnienia ścigania zbrodni międzynarodowych. Zasady w nim zawarte mają na celu pomoc państwom we wdrożeniu jurysdykcji uniwersalnej do ich wewnętrznych porządków prawnych, a przez to przyczynić się do skutecznego ścigania osób winnych popełnienia najpoważniejszych zbrodni. Poza aspektem legislacyjnym, projekt ten ma być pomocą dla sędziów przy interpretacji prawa krajowego oraz międzynarodowego oraz dla organizacji międzynarodowych i obywateli przy pomocy znajomości praw człowieka. Tekst w języku angielskim dostępny na oficjalnej stronie internetowej The Program in Law and Public Affairs Princeton University: https://lapa.princeton.edu/hosteddocs/unive_jur.pdf. Zob. M. Znojek, *Kilka uwag o zarzutach podnoszonych wobec jurysdykcji uniwersalnej*, „Kwartalnik Prawa Publicznego" 2007, nr 3, s. 134.

Zasadę represji wszechświatowej stosuje się jednakże jedynie do określonej kategorii czynów, uznanych za zbrodnie przez prawo międzynarodowe. Penalizacja tych czynów następuje ze względu na wagę i powszechną krytykę tego typu przestępstw, które mogą być ścigane i karane przez każde państwo. Powszechnie uznaje się, iż do zbrodni podlegających jurysdykcji uniwersalnej zalicza się: zbrodnie wojenne, ludobójstwo, zbrodnie przeciwko ludzkości, piractwo na morzu pełnym, tortury i terroryzm. Nie można jednak uznać, by był to katalog zamknięty i wyłączny.

Według Tomasza Ostropolskiego teoretyczne fundamenty jurysdykcji uniwersalnej wywodzą się z dwóch stanowisk. Pierwsze z nich opiera się na platońskim ideale obiektywnej sprawiedliwości i filozoficznym założeniu, iż wszystkie narody świata wyznają pewien katalog powszechnie akceptowanych wartości wynikających z prawa natury. Stanowisko to zakłada, iż pogwałcenie tych ogólnie akceptowalnych norm jest równocześnie skierowane przeciwko całemu rodzajowi ludzkiemu i w konsekwencji, każde z państw ma prawo do ścigania i ukarania danego sprawcy w imieniu całej społeczności międzynarodowej. Drugie opiera się na bardziej współczesnym, pragmatycznym założeniu. Konieczność istnienia represji powszechnej nabrała szczególnego znaczenia w erze globalizmu, gdzie zagrożenia o charakterze międzynarodowym niejednokrotnie mają charakter transgraniczny i transnarodowy, a tradycyjne metody ścigania najpoważniejszych zbrodni są nieefektywne. Wskazanym jest zatem, dla utrzymania międzynarodowego pokoju i bezpieczeństwa, stworzenie instrumentów umożliwiających walkę z tymi zjawiskami[289].

Inny podział jurysdykcji uniwersalnej proponuje Antonio Cassese, wyróżniając jurysdykcję absolutną i warunkową[290]. Absolutna jurysdykcja uniwersalna (ang. *absolute universal jurisdiction*) ma szerszy zakres niż jurysdykcja warunkowa, w związku z czym ma mniej zwolenników. Koncepcja ta dopuszcza możliwość ścigania oskarżonego o popełnienie zbrodni międzynarodowej niezależnie od jego obywatelstwa, narodowości ofiary, miejsca popełnienia czynu czy też przebywania na terytorium państwa, które wszczęło postępowanie karne. Absolutna jurysdykcja uniwersalna zezwala jedynie na prowadzenie postępowania przygotowawczego, zbieranie dowodów i ściganie oskarżonego, ale nie na prowadzenie postępowania sądowego. Takie sformułowanie tej zasady zostało podyktowane faktem, iż prawodawstwa wielu państw nie dopuszczają możliwość prowadzenie procesu pod

[289] T. Ostropolski, *Jurysdykcja uniwersalna w prawie międzynarodowym*, „Studia Prawno - Europejskie" 2004, t. 7, s. 259.
[290] A. Cassese, *International Criminal Law*, Oxford 2003, s. 284.

nieobecność oskarżonego. Rozwiązanie takie zostało przyjęte w takich krajach, jak Belgia, Hiszpania, Niemcy czy Włochy[291]. Warunkowa jurysdykcja uniwersalna (ang. *conditional universal jurisdiction*) z kolei przewiduje, iż organy państwa mogą prowadzić postępowanie karne i skazać sprawcę czynów zabronionych przez prawo międzynarodowe wyłącznie w przypadku, gdy osoba ta przebywa na terytorium danego państwa. Uregulowania o takim charakterze znalazły się w szeregu umów międzynarodowych[292], ale również w krajowych porządkach prawnych Austrii, Niemiec i Szwajcarii[293]. Marek Jeżewski postawił tezę, że „wykonywanie uniwersalnej jurysdykcji, nawet w jej warunkowej formie, stanowi wkroczenie w strefę suwerenności innego państwa. Granice dopuszczalności takich działań powinny być określone w sposób precyzyjny i w żadnym wypadku (na podstawie reguły interpretacyjnej *exceptiones non sunt extendendae*) nie wolno rozszerzać w drodze wykładni"[294].

Neil Boister stoi na stanowisku, że państwa przyznają absolutną jurysdykcję uniwersalną w przypadku przestępstw o charakterze pirackim popełnionych na pełnym morzu. Uznaje się bowiem, iż piraci są wrogiem wszystkich państw, a ich ściganie leży w interesie całej społeczności międzynarodowej. Boister podnosi jednak pytanie, czy piraci na gruncie prawa międzynarodowego są wrogami wszystkich państw, czy może część piratów jest wrogami tych krajów, które dopuszczają stosowanie jurysdykcji uniwersalnej jako substytut wewnętrznych zasad jurysdykcyjnych państwa - bandery[295].

Instytut Prawa Międzynarodowego dopuścił stosowanie jurysdykcji uniwersalnej wyłącznie w odniesieniu do *delicta iuris gentium*. W art. 8 projektu Rezolucji o Jurysdykcji Eksterytorialnej[296] przygotowanej w 1993 roku przez Instytut Prawa Międzynarodowego znalazły się uregulowania, które stanowią, że:

> „ust. 1. Na zasadzie jurysdykcji uniwersalnej, jurysdykcja może być wykonywana w celu ochrony pewnych interesów całej wspólnoty międzynarodowej.

[291] M. Znojek, op. cit., s. 136-137.
[292] Między innymi w Konwencji w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych 10 grudnia 1984 roku (Dz. U. z dnia 2 grudnia 1989 r.) czy też w Konwencja genewska o ochronie osób cywilnych podczas wojny (IV konwencja genewska) z dnia 12 sierpnia 1949 r. (Dz. U. z 1956 r., Nr 38, poz. 171).
[293] M. Znojek, op. cit., s. 136.
[294] M. Jeżewski, op. cit., s. 175.
[295] N. Boiser, op. cit., s. 150-151.
[296] Tekst rezolucji w języku angielskim przedrukowano [w:] "Yearbook of the Institute of International Law" 1993 t. 65.

ust. 2. Jurysdykcja oparta na zasadzie uniwersalnej obejmuje wszystkie osoby, bez względu na ich narodowość oraz miejsce popełnienia czynu.

ust. 3. Zasada uniwersalna powinna być stosowana w odniesieniu do przestępstw określonych w konwencyjnym oraz zwyczajowym prawie międzynarodowym, takich jak piractwo, uprowadzenia samolotów, terroryzm oraz handel narkotykami.

ust. 4. Jurysdykcja opisana w ust. 3 może być wykonywana bez względu na fakt, czy państwo ojczyste oskarżonego jest stroną jakiejkolwiek konwencji międzynarodowej"[297].

Podzielić należy pogląd M. Znojek, że „biorąc wszystkie te elementy pod uwagę należy stwierdzić, iż tak jak rozumiana jest jurysdykcja uniwersalna godzi w zasadę nieingerencji w sprawy wewnętrzne poszczególnych państw. Jednocześnie sprawiedliwość oraz bezpieczeństwo międzynarodowe, a więc wartości będące fundamentem pokojowej koegzystencji państw na równi z suwerennością, wymagają ukarania zbrodni międzynarodowych. W sytuacji, gdy państwo ojczyste sprawcy albo państwo, na którego terytorium czyn został popełniony nie chce albo nie może osądzić zbrodniarza, inaczej mówiąc nie występuje z wnioskiem o ekstradycje, państwo trzecie może to uczynić w oparciu o zasadę uniwersalną"[298].

Bezpośrednie stosowanie absolutnej jurysdykcji uniwersalnej pociąga za sobą kilka niebezpieczeństw. Po pierwsze istnieje możliwość stosowania tak zwanego *forum shopping*, czyli możliwości złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa w państwie, którego porządek prawny czy też stan polityczny zapewnia najbardziej dogodną sytuację ofiar przestępstw. Po drugie problemem może być panujący w wielu systemach prawnych zakaz prowadzenia postępowania karnego pod nieobecność oskarżonego. Może to prowadzić do sytuacji, gdzie mimo przeprowadzenia postępowania przygotowawczego, zebrania całego materiału dowodowego nie dojdzie do osądzenia i ewentualnego skazania winnego. Nie mniej istotny jest fakt, iż gdyby wszystkie państwa uznały absolutną jurysdykcję uniwersalną doprowadziłoby to do swoistego paraliżu sądownictwa z powodu niejednoznacznego orzecznictwa oraz braku reguł odnoszących się do pozytywnych sporów kompetencyjnych pomiędzy sądami poszczególnych krajów[299].

[297] Tekst w języku polskim za: M. Znojek, op. cit., s. 147.
[298] M. Znojek, op. cit., s. 148.
[299] Ibidem, s. 138 - 139.

Marek Jeżewski podkreśla, że na wykonywanie przez państwa uniwersalnej jurysdykcji karnej są nałożone ograniczenia dwojakiego rodzaju. Po pierwsze, pociągnięcie sprawcy do odpowiedzialności może nastąpić wyłącznie w przypadku ściśle określonych zbrodni. Podstawą ich określenia może być zarówno prawo traktatowe, jak i zwyczajowe, które określa katalog najcięższych zbrodni międzynarodowych takich, jak zbrodnia ludobójstwa, zbrodnie wojenne czy zbrodnie przeciwko ludzkości. Drugi typ ograniczeń związany jest z czynnościami, jakie mogą być podejmowane w związku z wykonywaniem jurysdykcji uniwersalnej. Wyróżnić tu należy możliwość wydawania decyzji skutkujących pociągnięciem sprawcy do odpowiedzialności (ang. *prescriptive jurisdiction*) oraz podejmowanie środków przymusu, które doprowadziłyby do skutecznego i efektywnego przeprowadzanie postępowania karnego (ang. *enforcement jurisdiction*)[300].

Możliwość zastosowania zasady uniwersalizmu trzeba odnieść do praktyki funkcjonowania międzynarodowych trybunałów karnych, by wykazać czy i w jakim zakresie zasada ta znalazła odzwierciedlenie w działalności tych instytucji. Międzynarodowy Trybunał Wojskowy Karny w Norymberdze według teoretyków prawa oparł się na dwojakiej podstawie jurysdykcyjnej. Pierwsze z założeń, podstawę działalności Trybunału wywodzi z klasycznej zasady terytorialnej. Mocarstwa Sprzymierzone Deklaracją Berlińską z 5 czerwca 1945 r. objęły suwerenną władzę i wynikające z niej uprawnienia do wykonywania władzy zwierzchniej na terytorium Niemiec, więc uzyskały również uprawnienia do ścigania i karania sprawców przestępstw popełnionych na ich terytorium. Drugie z kolei koncepcja opiera się na założeniu, że ściganie i karanie zbrodniarzy hitlerowskich było wykonywane w imieniu całej społeczności międzynarodowej, na podstawie jurysdykcji uniwersalnej. Z kolei działalność Międzynarodowego Trybunału Wojskowego dla Dalekiego Wschodu oparła się na założeniu, iż podstawą jego funkcjonowania było wyrażenie wyraźnej zgody przez Japonię na poddanie się jurysdykcji tego organu i tym samym częściowe zrzeczenie się własnych kompetencji w tym zakresie[301].

Zasada jurysdykcji uniwersalnej nie znalazła odzwierciedlenia w statucie Międzynarodowego Trybunału Karnego[302]. Statut Rzymski w art. 12 przewiduje, iż Trybunał może wykonywać jurysdykcję, jeżeli czyn został popełniony na terytorium państwa strony, osoba podejrzana o popełnienie zbrodni jest obywatelem tego państwo albo jeżeli państwo *ad*

[300] M. Jeżewski, op. cit., s. 175-176.
[301] T. Ostropolski, *Jurysdykcja…*, s. 263-265.
[302] Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r., Dz.U. z 2003 r., Nr 78, poz. 708.

hoc uznało jego jurysdykcję. Jako fundamentalną podstawę działania Międzynarodowego Trybunału Karnego uznano komplementarność. Zarówno w preambule, jak i w art. 17 Statutu stwierdzono, iż niedopuszczalne jest wszczęcie postępowania przed Trybunałem, jeżeli sprawa jest przedmiotem postępowania karnego w państwie, do którego jurysdykcji sprawa ta należy, chyba że państwo to nie wyraża woli lub jest niezdolne do rzeczywistego przeprowadzenia postępowania karnego. Tak wyrażona zasada nie pozostaje bez znaczenia dla jurysdykcji uniwersalnej. W piśmiennictwie przedmiotu wskazuje się, że „zapewnienie pierwszeństwa rozpatrywania sprawy przez sądy krajowe jest ponadto potwierdzeniem gwarancji suwerennych interesów w obszarze sprawiedliwości karnej i integralności krajowych systemów rządowych. Wydaje się zatem, że dopiero zachowanie dualizmu w postaci współdziałania sądów krajowych z trybunałami międzynarodowymi zagwarantować może powstanie zrębów spójnego, szerokiego i skutecznego systemu quasi-wszechświatowej jurysdykcji”[303].

Małgorzata Znojek wskazuje, że oponenci jurysdykcji uniwersalnej zarzucają jej:

1) „spory doktrynalne co do definicji i zakresu,
2) brak konsensusu państw co do możliwości powoływania się na nią,
3) niedookreślenie prawa właściwego,
4) możliwość negatywnego wpływu na polityczne i gospodarcze stosunki międzynarodowe,
5) zachwiania trójpodziału władzy państwowej wraz z nadmiernym wzrostem postępowania przez państwo niezwiązane z czynem lub sprawcą”[304].

Jako główny kontrargument wskazanych powyżej zarzutów podniesiono, że „precyzyjnie zdefiniowana, uznana za normę zwyczajową *ius cogens* i obowiązująca *erga omnes* zasada jurysdykcji uniwersalnej może stanowić najskuteczniejszy instrument w walce z bezkarnością sprawców *delica iuris gentium*. Ważkość tego argumentu jest na tyle przekonująca i atrakcyjna, że powinien on stanowić wystarczającą zachętę dla wspólnoty międzynarodowej do współdziałania w celu przezwyciężenia sporów i wypracowania możliwie najdoskonalszego modelu jurysdykcyjnego, stanowiącego podstawę pociągnięcia do odpowiedzialności osób winnych popełnienia najcięższych zbrodni”[305].

[303] T. Ostropolski, *Jurysdykcja …*, s. 269- 275.
[304] M. Znojek, op. cit., s. 133.
[305] Ibidem, s. 133- 134.

Zgodzić należy się z poglądem doktryny, iż oczywiście zasadne jest stosowanie warunkowej jurysdykcji uniwersalnej w przypadku, gdy sprawca zbrodni przebywa na terytorium danego państwa. Niedopuszczalne za to wydaje się uznanie za legalną absolutnej jurysdykcji uniwersalnej, gdyż „żaden z traktatów, przyjętych w celu inkryminowania najcięższych zbrodni przeciwko podstawowym wolnościom ogólnoludzkim, nie zawiera normy mogącej być podstawą prawną do działania *in absentia*. Nie można też mówić o normie zwyczajowej, gdyż pomimo sporadycznych wypadków, gdy sądy krajowe działały pod nieobecność sprawcy na terytorium, praktyka w tym zakresie nie jest jednolita. Ponadto można stwierdzić brak *opinio iuris* przemawiającego za takimi rozwiązaniami. Wydaje się również, iż przyznanie państwom uniwersalnej jurysdykcji nie jest ani możliwe ani pożądane. Bardziej wskazane byłoby raczej upoważnienie organu ponadnarodowego do działania w sposób niezależny od woli poszczególnych podmiotów".[306]

2.1.3.2. Regulacje globalne

Jurysdykcja a konwencja o cyberprzestępczości

Kwestia jurysdykcji w cyberprzestrzeni została poruszona w art. 22 ust. 1 Konwencji o cyberprzestępczości[307]. Zgodnie z tym przepisem państwa - strony Konwencji podejmą środki prawne lub inne, którą mogą być potrzebne dla ustanowienia swojej jurysdykcji, gdy przestępstwo popełnione jest:

a) na terytorium państwa - strony,
b) na pokładzie statku pływającego pod banderą tej strony,
c) na pokładzie samolotu zarejestrowanego na podstawie prawa państwa - strony, lub,
d) przez jednego z jej obywateli, jeżeli przestępstwo jest karalne według prawa miejsca jego popełnienia lub jeśli przestępstwo zostało popełnione poza jurysdykcją terytorialną jakiegokolwiek państwa.

[306] M. Jeżewski, op. cit., s. 177-178.
[307] Konwencja o cyberprzestępczości sporządzona w Budapeszcie w dniu 23 listopada 2001 r., Dz.U. z 2014 r., poz. 1514.

Według postanowień Konwencji, akt ten nie wyłącza jurysdykcji wykonywanej przez państwo zgodnie z jego prawem krajowym. Artykuł 22 ust. 4 stanowi również, że w przypadku konfliktu jurysdykcyjnego kilku państw, strony podejmą konsultacje, w celu określenia czyja jurysdykcja jest najwłaściwsza dla ścigania tego przestępstwa.

Podstawową zasadą jurysdykcyjną przyjętą Konwencji o cyberprzestępczości jest zasada terytorialności. Oczywiste jest, iż strona Konwencji może zastosować swoje prawo krajowe w przypadku popełnienia na jego terytorium cyberprzestępstwa. Sama konwencja nie rozstrzyga w jaki sposób określić *locus delicti* cyberprzestępstw. Henrik W.K. Kaspersen wskazuje jednak że, za *locus delicti* popełnienia przestępstwa należy uznać miejsce, w którym osoba fizyczna wykorzystuje urządzenia elektroniczne w celu uzyskania dostępu do środków komunikacji elektronicznej. Miejsce popełnienia przestępstwa w dużej mierze zależeć będzie od legalnej definicji przestępstwa w konkretnym państwie. Może to być zarówno miejsce przebywania sprawcy, lokalizacja serwerów czy komputerów ofiary. Tak przyjęte, nieokreślone *locus delicti* cyberprzestępstw może i będzie generować liczne konflikty jurysdykcyjne, ponieważ sprawca może przebywać w jednym miejscu, podjąć działanie przestępcze w innym, a skutek przestępstwa nastąpi w jeszcze innym miejscu. Czyn taki uzasadniałby jurysdykcję terytorialną kilku krajów, które zmuszone byłyby podjąć konsultacje w celu określenia, które z nich jest właściwe do sądzenia cyberprzestępcy.[308]

Jak słusznie zauważa Henrik W.K. Kaspersen, w Konwencji o cyberprzestępczości rozszerzono jurysdykcję na statki morskie i powietrzne pomijając całkowicie kwestię satelitów. Satelity są jednym z głównych globalnych sieci komunikacyjnych. Satelity poruszają się po określonych orbitach, jednakże do ich prawidłowego funkcjonowania potrzebna jest naziemna obsługa, która odbiera i przesyła informację do satelity. Stacja naziemna położona jest w obrębie terytorialnym konkretnego państwa - zatem, wszelkie dane odbierane czy też przesyłane za pomocą satelity podlegać będą jurysdykcji terytorialnej państwa położenia stacji naziemnej. Konwencja nie porusza też kwestii potencjalnych przestępstw popełnianych przez kosmonautów w przestrzeni kosmicznej, bowiem, wydaje się, iż na chwilę obecną jest to kwestia zbyt marginalna by wymagała prawnej regulacji[309].

Konwencja o cyberprzestępczości wprowadza zasadę jurysdykcji personalnej, zastrzegając wymóg podwójnej karalności. Kolejnym przypadkiem zastosowania tej zasady

[308] H.W.K. Kaspersen, *Jurisdiction in the Cybercrime Convention*, B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, t. 11, s 10-11.
[309] Ibidem, s. 13.

jest obywatelstwo przestępcy, który popełnia czyn znajdując się na terytorium nie podlegającym jurysdykcji żadnego z państw. Taka sytuacja wystąpi na przykład jeżeli cyberprzestępca popełni czyn przebywając na morzu pełnym na statku niezarejestrowanym w żadnym państwie[310]. W Konwencji o cyberprzestępczości zastosowano, więc tradycyjne zasady jurysdykcyjne - zasadę jurysdykcji terytorialnej i zasadę jurysdykcji personalnej.

2.1.3.3. Regulacje regionalne na przykładzie Unii Europejskiej

Unia Europejska stawia sobie za cel utworzenie wspólnej europejskiej przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Należy wyeliminować lub stworzyć mechanizmy rozwiązywania konfliktów jurysdykcyjnych, aby cel ten został osiągnięty istnieje. Służy temu:

1) wykrycie i uniknięcie na jak najwcześniejszym etapie postępowania sytuacji, że w stosunku do tej samej osoby toczą się równolegle dwa postępowania karne w różnych państwach członkowskich, jakie to działanie może doprowadzić do naruszenia zasady *ne bis in idem*,
2) zapewnienie bliższej współpracy pomiędzy państwami członkowskimi, prowadzącymi w tym samym czasie postępowanie karne w stosunku do tej samej osoby/osób, lub w sprawie tych samych lub powiązanych czynów dotyczących innej osoby/osób lub w sprawie tej samej organizacji przestępczej[311].

W Unii Europejskiej konflikty jurysdykcyjne są związane z problematyczną kwestią ustalenia, które z państw członkowskich ma prawo do rozstrzygnięcia sprawy w sposób wiążący również dla innych państw. Według Tomasza Ostropolskiego ryzyko wystąpienia konfliktu jurysdykcyjnego w Unii Europejskiej wynika z kilku czynników:

1) państwa członkowskie UE są związane umowami międzynarodowymi penalizującymi tak zwane przestępstwa konwencyjne, które to umowy mają bardzo szerokie podstawy jurysdykcyjne,

[310] Ibidem, s. 14.
[311] M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: pojęcie…*, s. 18.

2) państwa członkowskie UE są związane ponadto prawem wtórnym UE, ujmującym dość szeroko kwestie jurysdykcyjne; niektóre akty europejskiego prawa materialnego[312] zobowiązują państwa do ścigania określonych rodzajów przestępstw; by ściganie takie było efektywne zawierają one szerokie podstawy jurysdykcyjne. W przypadku niektórych rodzajów przestępstw zastosowanie szerokich podstaw jurysdykcyjnych jest absolutną koniecznością do przeprowadzenia efektywnego ścigania i skazania; chodzi tu przede wszystkim o czyny zabronione, które wymykają się standardowym łącznikom jurysdykcyjnym na przykład cyberprzestępczość, seksualne wykorzystywanie dzieci oraz handel ludźmi,
3) wprowadzenie strefy Schengen, swobodny przepływ osób w Unii Europejskiej zwiększyło ryzyko rozwoju przestępczości o charakterze transgranicznym. Fakt ten może spowodować, iż więcej niż jedno państwo może posiadać łącznik jurysdykcyjny z popełnionym przestępstwem[313].

Problem jurysdykcji karnej w Unii Europejskiej nastręczał wielu problemów. Potrzeba wypracowania odpowiednich mechanizmów w tym zakresie podyktowana była między innymi ekonomiką postępowania - tak by sprawa była prowadzona w państwie, które efektywnie może zebrać dowody i osądzić sprawcę. Nie mniej istotne było realne ryzyko naruszenia zasady *ne bis in idem* oraz potrzeba ochrony osób pokrzywdzonych przestępstwem. Początkowe propozycje rozwiązania problemu konfliktu jurysdykcyjnego były różne, od systemu jurysdykcji wyłącznej (możliwość ścigania przestępcy tylko przez jedno państwo z wyłączeniem jurysdykcji innych) do systemu hierarchii zasad kompetencyjnych (ustalenie katalogu wartości zasad kompetencyjnych, którymi kierować miałyby się państwa)[314].

[312] Przepisy takie znajdują się między innymi w: decyzji ramowej Rady 2001/413/WSiSW z 28.05.2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (Dz.Urz. WE L 149 z 02.06.2001 r. s.1; art. 9), decyzji ramowej Rady 2011/93/UE z 13.12.2011 r. w sprawie niegodziwego traktowania w celach seksualnych i wykorzystania dzieci oraz pornografii dziecięcej (Dz.Urz. UE L 335/1 z 17.12.2011 r.; art. 17), dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z 30.09.2010 r. w sprawie ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218/8 z 14.08.2013 r., art.12).
[313] T. Ostropolski, *Zapobieganie …*, s. 102-103.
[314] Ibidem, s. 105.

Decyzja ramowa Rady 2009/948/WSiSW

Ostatecznie kwestia jurysdykcji karnej w UE została uregulowana Decyzją ramową Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów[315]. Wstępny projekt decyzji ramowej w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów przedstawiony w styczniu 2009 roku przez Czechy, Polskę, Słowenię, Słowację oraz Szwecję przewidywał bardziej elastyczny model jurysdykcyjny. W projekcie postawiono sobie dwa cele. Pierwszym było jak najwszcześniejsze wyeliminowanie sytuacji, która mogłaby doprowadzić do równoległego prowadzenia postępowania w stosunku do tej samej osoby w różnych państwach członkowskich. Drugim celem miało być zacieśnienie współpracy pomiędzy państwami UE w kwestii wykonywania przez nie uprawień wynikających z postępowania karnego w odniesieniu do czynów dotyczących tej samej osoby, czynów powiązanych lub w przypadku tej samej organizacji przestępczej[316].

Wskazane wyżej cele miały być osiągnięte poprzez zastosowanie następujących kroków:

1) wymianę informacji pomiędzy państwami członkowskimi UE na temat toczących się spraw, które mogą mieć związek z inną jurysdykcją - na jak najwcześniejszym etapie,
2) stworzenie możliwości przeprowadzania bezpośrednich konsultacji pomiędzy państwami zainteresowanymi w celu ustalenia, która jurysdykcji będzie najodpowiedniejsza do efektywnego prowadzenia postępowania karnego,
3) ustalenie kryteriów i zasad, którymi kierować się będą państwa członkowskie przy wyborze najodpowiedniejszej jurysdykcji[317].

Celem decyzji ramowej jest ustanowienie procedur wymiany informacji pomiędzy organami państw członkowskich o toczących się postępowaniach karnych w ściśle określonych sprawach. W przypadku ustalenia prowadzenia równoległych postępowań należy niezwłocznie podjąć bezpośrednie konsultacje w celu ustalenia najbardziej odpowiedniej

[315] Decyzja ramowa Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów, Dz.Urz. UE L 328 z 15.12.2008 r.
[316] T. Ostropolski, *Zapobieganie …*, s. 116.
[317] Ibidem, s. 116.

jurysdykcji[318]. Zaproponowane w projekcie rozwiązania nie znalazły uznania państw członkowskich. W wyniku negocjacji zawężono zakres decyzji ramowej Rady 2009/948/WSiSW jedynie do przypadków, w których istnieje obawa naruszenia zasady *ne bis in idem*. Nie zdecydowano się jednak na objęcie zakresem decyzji postępowań które dotyczą tego samego zdarzenia, jednakże prowadzone są w stosunku do innych osób[319].

Artykuł 5 decyzji ramowej Rady 2009/948/WSiSW wprowadza nowy mechanizm obowiązku nawiązania kontaktu. Artykuł ten stanowi, że jeżeli właściwy organ w państwie członkowskim ma uzasadnione powody, by przypuszczać, że w innym państwie członkowskim toczy się postępowanie równoległe, ma on obowiązek nawiązania kontaktu z właściwym organem państwa drugiego, w celu potwierdzenia, czy faktycznie takie postępowanie jest prowadzone. W przypadku otrzymania odpowiedzi pozytywnej państwa zainteresowane przeprowadzają konsultacje. Artykuł 6 nakłada na organ państwa, do którego zgłoszono się z wnioskiem, obowiązek udzielenia nań odpowiedzi w rozsądnym terminie wskazanym przez organ nawiązujący kontakt, a jeżeli terminu takiego nie wskazano - bez nieuzasadnionej zwłoki. W przypadku ustalenia, że toczą się postępowania równoległe, właściwe organy w państwach członkowskich winny podjąć bezpośrednie konsultacje w celu wypracowania porozumienia, które pozwoli uniknąć naruszenia zasady *ne bis in idem* (artykuł 10).

Decyzja ramowa Rady 2009/948/WSiSW przewiduje współpracę z Eurojustem. Uruchomienie działania Eurojustu w procedurze przewidzianej w decyzji może nastąpić po spełnieniu dwóch warunków:

1) pierwszy z nich przewidziany został w art. 12 ust. 2 decyzji ramowej Rady 2009/948/WSiSW i ma zastosowanie gdy wypracowanie porozumienia w trybie art. 10 decyzji okazało się niemożliwe (rola Eurojustu ma wówczas charakter subsydiarny),
2) gdy Eurojust jest właściwy do podjęcia działań na mocy art. 4 ust 1 decyzji o Eurojuście (gdy prowadzone postępowanie mieści się w materialnym zakresie działalności organu)[320].

Decyzja ramowa Rady WSiSW 2009/948/WSiSW nie jest aktem, który można uznać za kompleksową regulację w zakresie wykonywania jurysdykcji karnej w UE. W dokumencie

[318] M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: propozycja …*, s. 145.
[319] T. Ostropolski, *Zapobieganie …*, s. 116.
[320] Ibidem, s. 118.

tym brak jest przepisów obejmujących tzw. negatywny konflikt jurysdykcyjny[321]. Komentatorzy decyzji ramowej podnieśli, że „mechanizmy ustanowione w omawianej decyzji ramowej mają charakter miękki. Szereg zobowiązań uregulowanych jest w sposób pozostawiający stosunkowo szeroki zakres elastyczności dla organów państw członkowskich. Dotyczy to również terminów, które zostały określone w sposób nieostry. Można uznać, że taki kształt przyjętych mechanizmów wynika z chęci uniknięcia nadmiernych obciążeń biurokratycznych, które mogłyby powstać w przypadku bezwzględnego obowiązku konsultacji pomiędzy organami w sytuacji jakiegokolwiek potencjalnego łącznika jurysdykcyjnego"[322]. Ponadto, w przypadku nie osiągnięcia porozumienia w drodze konsultacji, omawiana decyzja ramowa nie przewiduje możliwości zmuszenia państwa do rezygnacji z wykonywanej jurysdykcji.

Mimo pewnego zakresu regulacji zgodzić się należy z tezą, że „dotąd brak jest w UE instrumentarium, które obejmowałoby problem zapobiegania i rozwiązywania sporów jurysdykcyjnych w sposób kompletny. Mamy raczej do czynienia z systemem fragmentarycznym i wielopłaszczyznowym, gdzie zespół mechanizmów funkcjonujących w ramach różnorodnych instrumentów może determinować wybór jurysdykcji"[323]. Rozważyć zatem należy podjęcie kolejnych działań legislacyjnych w tym przedmiocie.

Inne akty prawne Unii Europejskiej

Przykładem jednego z wielu aktów prawnych Unii Europejskiej, który w swych postanowieniach porusza zagadnienie jurysdykcji karnej jest Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW[324].

[321] M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: propozycja*… , s. 153.
[322] A. Grzelak, T. Ostropolski, *Współpraca wymiarów sprawiedliwości w sprawach karnych i współpraca policyjna,* t. 9.,cz. 1, wyd. 2 zm., Warszawa 2011, s. 122-123.
[323] T. Ostropolski, *Zapobieganie …*, s. 106.
[324] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW, Dz. Urz. UE L 335 z 17.12.2011 r.

Nie należy również pominąć postanowień Decyzji Rady 2008/913/WSiSW z 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych[325]. Klauzula jurysdykcyjna we wskazanym akcie prawnym oparła się na zasadzie terytorialnej (obiektywnej i subiektywnej) oraz na zasadzie personalnej. Artykuł 9 ust. 2 decyzji zawiera ponadto przepis odnoszący się do systemu informatycznego, który został wykorzystany do popełnienia przestępstwa. Według decyzji każde państwo członkowskie może rozszerzyć swoją jurysdykcję na sytuacje, w których czyny zabronione zostały popełnione w obrębie systemu informacyjnego, a ich sprawca znajduje się na terytorium tego państwa, niezależnie od tego, czy czyny te dotyczą materiału zawartego w systemie informacyjnym kontrolowanym z jego terytorium. Oznacza to, że za miejsce popełnienia przestępstwa uznano terytorium któregokolwiek państwa członkowskiego Unii Europejskiej, na którym znajduje się sprawca w tracie umieszczania na serwerze znajdującym się w państwie trzecim treści propagujących rasizm[326]. W art. 9 ust. 2 pkt. b za *locus delicti* uznano miejsce położenia systemu informacyjnego, czyli serwera na terytorium państwa członkowskiego, niezależnie od tego czy sprawca popełniając czyn zabroniony jest fizycznie obecny na terytorium tego państwa[327].

Uznaje się, że wskazane wyżej dokumenty odgrywają istotną rolę nie tylko w zakresie ustanowienia standardów normatywnych, w szczególności dotyczących rodzaju i wysokości kar za popełnione przestępstwa, ale również w zakresie ustanowienia obligatoryjnych przesłanek jurysdykcyjnych. Analizując przedmiotowe akty prawne można dojść do przekonania, iż celem Unii Europejskiej było nie tylko przeciwdziałanie cyberprzestępczości występującej na terytorium poszczególnych państw członkowskich, ale również stworzenia ogólnych ram bezpieczeństwa dla całej Unii[328].

[325] Decyzja Rady 2008/913/WSiSW z 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych, Dz. Urz. UE L 328 z 06.12.2008 r.
[326] A. Adamski, *Podstawy …*, s. 950-951.
[327] Ibidem, s. 951.
[328] M. Siwicki, *Podstawy …*, s. 23.

2.1.3.4. Jurysdykcja karna w cyberprzestrzeni w aspekcie prawnoporównawczym

Ostatnie dwie dekady doprowadziły do rozwoju Internetu na skalę globalną. Nowa, wirtualna przestrzeń ukazała liczne problemy, z jakimi społeczność międzynarodowa musi się zmierzyć, zwłaszcza w aspekcie ustalenia jurysdykcji właściwej do czynów przestępczych popełnianych w cyberprzestrzeni oraz ewentualnego rozstrzygnięcia konfliktów w tym zakresie. Część z porządków prawnych dotyczących cyberprzestępczości wprowadziła zasadę terytorialną w czystej postaci, obejmując swoim prawem wszelkie zdarzenia w których chociażby jeden element wystąpił na terytorium danego państwa. Inne kraje z kolei, zwłaszcza w przypadkach związanych z pornografią dziecięcą, zdecydowały sie zastosować zasadę jurysdykcji uniwersalnej[329].

W przypadku cyberprzestępstw szczególne trudności powoduje ustalenie miejsca popełnienia przestępstwa. Nie wykształciła się w tym przedmiocie jeszcze jednolita praktyka, jednakże zauważalną tendencją jest fakt, iż państwa europejskie opierają swoje ustawodawstwo na tradycyjnej doktrynie wielomiejscowości przestępstwa (ang. *doctrine of ubiquity*) zakładającej, iż cyberprzestępstwo zostało popełnione w miejscu czynu, skutku bądź też miejsca, gdzie skutek według zamiaru sprawcy miał nastąpić. Z kolei systemy pozaeuropejskie skłaniają się do poglądu, iż miejscem popełnienia przestępstwa dokonanego z wykorzystaniem systemów informatycznych jest miejsce położenia systemu komputerowego (czyli serwera, danych, oprogramowania), na który wpływa za pomocą sieci telekomunikacyjnej znajdujący się za granicą sprawca[330].

Podstawowym problemem transnarodowych przestępstw popełnianych za pomocą cyberprzestrzeni jest kwestia jurysdykcji - które państwo ma podstawy prawne do sądzenia i skazania sprawcy. Nasuwa się także pytanie co zdarzy się w sytuacji, gdy więcej niż jedno państwo będzie chciało objąć czyn swoją jurysdykcją - czy któreś z nich będzie miało pierwszeństwo. Problemem jest nie tylko ustalenie podstawy prawnej do wszczęcia

[329] Idem, *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęciu prawno porównawczym*, cz. 1, „Europejski Przegląd Sądowy" 2011, nr 9, s. 23.
[330] A. Adamski, *Podstawy jurysdykcji …*, s. 940-941.

postępowania, ale również możliwość zebrania dowodów, przesłuchania świadków czy też przeprowadzanie postępowania sądowego w obecności sprawcy[331].

Ustalenie jurysdykcji właściwej w cyberprzestrzeni nie jest zagadnieniem łatwym. Wiele państw nie ma szczegółowych uregulowań prawnych w tym przedmiocie. Kraje te w głównej mierze polegają na tradycyjnych zasadach jurysdykcyjnych w celu określenia czy w konkretnym przypadku posiadają jurysdykcję. Duża część państw uzasadniając swoje zwierzchnictwo w cyberprzestrzeni posiłkuje się zasadą jurysdykcji terytorialnej, co może prowadzić do ekstremalnych przypadków na przykład w Malezji, gdzie władze mogą w teorii stwierdzić swoją jurysdykcję w przypadku każdego cyberprzestępstwa popełnionego gdziekolwiek na świecie. Artykuł 9 *Malaysia Computer Crimes Act*[332] stanowi, że ustawę tę stosuje się co do popełnionych przestępstw, komputerów znajdujących się czy też danych przepływających w danym czasie przez terytorium Malezji. Oznacza to, że wszelkie dane, które przepłynęły przez malezyjskie serwery będą podlegały pod malezyjską jurysdykcję[333].

Regulacje europejskie

Belgia

Belgijska ustawa dotycząca przestępstw seksualnych z 1995 roku wskazywała, iż ich sprawca może być sądzony przez władze krajowe, jeżeli czyn popełniony został za granicą przez Belga lub obcokrajowca, nawet jeżeli belgijskie władze nie otrzymały zawiadomienia o podejrzeniu popełnienia przestępstwa przez władze innego kraju. Pornografia dziecięca produkowana lub rozpowszechniana w innych krajach lub umieszczona w Internecie może od tej pory, na mocy wymienionej ustawy, podlegać pod jurysdykcję belgijską. Z kolei belgijska ustawa o przestępczości komputerowej z 2000 roku nie zawiera konkretnych postanowień poruszających kwestie jurysdykcji. W opinii Paula de Hert cyberprzestępstwa bez żadnych wątpliwości należy zakwalifikować jako przestępstwa międzynarodowe. Niezrozumiały jest

[331] B.J. Koops, S. Brenner, *Cybercrime jurisdiction - an introduction*, [w:] B.J. Koops, S.W. Brenner (red.), *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006 t. 11, s 2.
[332] Malaysia Computer Crimes Act 1997, http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf [22.05.2015].
[333] B.J. Koops, S. Brenner, op. cit., s. 3.

wobec tego dla autora brak kroków legislacyjnych w celu uregulowania kwestii jurysdykcji w prawie belgijskim w odniesieniu do cyberprzestępstw[334].

Podstawową zasadą ustalenia jurysdykcji karnej w prawie belgijskim jest zasada terytorialna. Artykuł 3 belgijskiego kodeksu karnego stanowi, że czyn zabroniony uważa się za popełniony na terytorium Belgii, niezależnie od tego czy popełnił go obywatel kraju czy obcokrajowiec. Zastosowana jurysdykcja terytorialna została dopełniona zasadą wielomiejscowości przestępstwa, co oznacza, że do rozciągnięcia belgijskiej jurysdykcji karnej jest wymagany by chociaż jeden z elementów przestępstwa wystąpił na terytorium Belgii. Uznaje się, iż elementem tym jest również skutek przestępstwa, co oznacza, iż uzyskanie samej możliwości dostępu za pomocą Internetu do treści zakazanych przez prawo belgijskie jest wystarczające do rozciągnięcia belgijskiego władztwa karnego[335].

To prowadzi do kwestii rozszerzenia kwestii jurysdykcji terytorialnej przez belgijskie sądy. W sądownictwie Królestwa Belgii istnieje zauważalna tendencja by interpretować zasadę jurysdykcji terytorialnej szeroko. Sądy belgijskie nie są, z wyjątkiem przypadków szczegółowo wskazanych w ustawach, właściwe do rozstrzygania spraw eksterytorialnych. Praktyka wskazuje jednakże, że sędziowie mają wielkie pole manewru by wskazać jurysdykcję belgijską jako właściwą w przypadku, gdy przestępstwo popełniono poza terytorium Belgii, jeżeli ono ma wpływ na szeroko pojęte belgijskie interesy[336]. Co więcej, przepisy belgijskie dopuszczają nawet ściganie cudzoziemców, którzy pomagali bądź podżegali do popełnienia przestępstwa przez obywatela belgijskiego na terytorium Królestwa[337].

System prawa belgijskiego do określenia *locus commissi delicti* przyjmuje kilka różnych kryteriów. Są nimi:

1) kryterium miejsca popełnienia przestępstwa (ang. *activity criterion*) rozumiane jako terytorium gdzie czyn miał miejsce,
2) kryterium położenia narzędzia przestępstwa (ang. *critertion of the instrument*),

[334] P. de Hert, *Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - whose Sovereignty is at stake?,* [w:] B.J. Koops, S.W. Brenner (red.), *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, t. 11, s. 94 -95.
[335] M. Siwicki, *Pojęcie …*, s. 24.
[336] P. de Hert, op. cit., s. 96.
[337] S. W. Brenner, B. Jaap Koops, *Approaches to Cybercrime Jurisdiction,* "Journal of High Technology Law" 2004, t. 1, s. 25.

3) kryterium wystąpienia konstruktywnego skutku przestępstwa (ang. *criterion of the constitutive consequence*),
4) kryterium wielomiejscowości przestępstwa (ang. *ubiquity criterion*) - *locus delicti* będzie występował w każdym państwie, gdzie nastąpił konstruktywny element przestępstwa, w tym przypadku zachodzi wysokie prawdopodobieństwo, że czyn będzie podlegać jurysdykcji więcej niż jednego kraju[338].

W przeciwieństwie do Niemiec czy Francji belgijski kodeks karny możliwość wyboru jednego z kryteriów pozostawia sądom powszechnym, nie wskazując które z nich winno się stosować w pierwszej kolejności. Badania pokazują, że w większości przypadków sędziowie zawsze znajdują podstawę do zastosowania własnej jurysdykcji, niezależnie od tego jakiego kryterium zdecydują się użyć. W szczególności kryterium wielomiejscowości przestępstwa pozwala osądzić osoby rozpowszechniające wirusy komputerowe, czy też treści rasistowskie z komputerów położonych poza granicami kraju. Elastyczność kryterium wielomiejscowości przestępstwa tłumaczy zatem brak przepisów prawnych w zakresie jurysdykcji[339]. Co istotne, w belgijskiej doktrynie uważa się, że najpoważniejsze cyberprzestępstwa, czyli dziecięca pornografia winny być objęte jurysdykcją uniwersalną[340].

Dania

W Danii cyberprzestępstwa są nazywane również przestępczością IT (da. *IT-kriminalietet*, ang. *IT crime*) lub przestępczością danych (da. *datakriminalitet*, ang. *data crime*). Zgodnie z duńskim prawem karnym za przestępstwo można uznać tylko czyn zakazany przez ustawę karną[341]. Przepisy karne dotyczące cyberprzestępczości znajdziemy nie tylko w duńskim kodeksie karnym, ale również w ustawach szczegółowych. Oprócz prawa wewnętrznego Dania jest stroną Konwencji o cyberprzestępczości, która została ratyfikowana 21 czerwca 2005 roku z zastrzeżeniem art. 9, 14 i 38 konwencji oraz art. 3, 5, 6 i 14 Protokołu Dodatkowego do Konwencji o cyberprzestępczości dotyczącego penalizacji

[338] P. de Hert, op. cit., s. 96.
[339] Ibidem, s . 96-97.
[340] S. W. Brenner, B.J. Koops, op. cit., s. 28.
[341] H. Spang - Hansen, *Cybercrime and Jurisdiction in Denmark*, [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 11, Haga 2006, s. 157-158.

czynów o charakterze rasistowskim, ksenofobicznym popełnionych przy użyciu systemów komputerowych[342].

W §6 duńskiego kodeksu karnego została ustanowiona zasada jurysdykcji terytorialnej, według której ustawa ta znajdzie zastosowanie, jeżeli: „sprawca działał lub zaniechał działania:

1. w Królestwie Danii (podstawowa zasada terytorialna),
2. na duńskim statku znajdującym się poza terytorium innego państwa w rozumieniu prawa międzynarodowego publicznego,
3. na duńskim statku znajdującym się na terytorium obcego państwa w rozumieniu prawa międzynarodowego publicznego popełnione przez osobę należącą do obsługi tego statku albo podróżującą jako pasażer na pokładzie"[343].

W Danii za miejsce popełnienia przestępstwa uważa się miejsce, gdzie skutek nastąpił, lub według zamiaru sprawcy miał nastąpić. Oznacza to, że obok jurysdykcji terytorialnej wprowadzono zasadę skutkową[344]. Co więcej §7 wprowadza zasadę jurysdykcji personalnej, która stanowi, że duńskiej jurysdykcji podlega osoba z duńskim obywatelstwem lub domicylem, która popełniła czyn zabroniony poza terytorium Danii jeżeli:

1) aktu dokonano poza terytorium podlegającym jurysdykcji jakiegokolwiek państwa według prawa międzynarodowego, jeżeli przestępstwo zgodnie z duńskim prawem podlega karze minimum 4 miesięcy pozbawienia wolności,
2) jeżeli czyn popełniony na terytorium innego państwa jest również uznany za przestępstwo w tym państwie (wymóg podwójnej karalności)[345].

Punkt 2 §7 stanowi, że punkt 1 stosuje się również do czynów popełnionych przez obywateli Finlandii, Islandii, Norwegii i Szwecji przebywających w Danii. Co więcej §8 duńskiego kodeksu karnego duńską jurysdykcję stosuje się do czynów przygotowywanych poza terytorium Danii, bez względu na to, z którego kraju pochodzi sprawca przygotowań, jeżeli:

1) czyn zagraża niepodległości, bezpieczeństwu, konstytucji lub władzom publicznym Danii lub też duńskim interesom państwowym,

[342] Ibidem, s. 159.
[343] M. Siwicki, *Pojęcie …*, s. 24.
[344] Ibidem.
[345] H. Spang - Hansen, op. cit., s 173.

2) czyn skierowany jest przeciwko obywatelowi lub rezydentowi Danii, a czyn według prawa duńskiego zagrożony jest karą co najmniej 4 miesięcy pozbawienia wolności,
3) w przypadku przygotowań do porwania samolotu, statku lub innego środka publicznego transportu,
4) Dania jest zobowiązania do jego ścigania na mocy umów międzynarodowych,
5) gdy odmówiono ekstradycji do innego kraju, spełniony jest wymóg podwójnej karalności a według prawa duńskiego czyn podlega karze co najmniej jednego roku pozbawienia wolności[346].

Niemcy

W 1986 roku do niemieckiego Kodeksu Karnego (niem. *Strafgesetzbuch*) wprowadzono penalizację przestępstw komputerowych takich, jak hacking, nieuprawniona zmiana danych, sabotaż komputerowy, oszustwo komputerowe oraz fałszerstwo komputerowe. Niemiecka ustawa karna wprowadzając zasadę jurysdykcji terytorialnej przewidziała, wielomiejscowość popełnienia czynu, czyli uznano, iż miejscem popełnienia przestępstwa jest zarówno miejsce działania sprawcy jak i miejsce wystąpienia skutku czynu zabronionego. Przepisy ustawy stanowią ponadto, iż podstawą wykonywania jurysdykcji jest zasada personalna, odnosząca się do niemieckiego obywatela, który popełnił przestępstwo poza granicami kraju. Jak wskazuje Maciej Siwicki, zasadę terytorialną stosuje się wobec obywatela niemieckiego, który dopuścił się czynu przestępczego za pomocą mediów elektronicznych. Bez znaczenia pozostaje wówczas fakt, czy popełniając czyn, np. wprowadzając zakazane przez prawo niemieckie dane do Internetu, znajdował sie na terytorium Niemiec czy też w państwie trzecim[347].

W pewnych przypadkach przestępstw komputerowych z łatwością można zastosować zasadę jurysdykcji terytorialnej czy też zasadę wielomiejscowości popełnienia przestępstwa, a taka sytuacja wystąpi, gdy sprawca przebywając na terytorium Niemiec manipuluje danymi znajdującymi się na komputerze podlegającym pod jurysdykcję innego państwa. Wówczas - jak i w odwrotnym przypadku, gdy sprawca zza granicy niszczy dane na komputerze

[346] Ibidem, s 173-174.
[347] M. Siwicki, *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęciu prawnoporównawczym (cz. I),* „Europejski Przegląd Sądowy" 201,1 nr 9, s. 25.

znajdującym się na terytorium Niemiec - niemiecki wymiar sprawiedliwości będzie mógł zastosować własną jurysdykcję[348].

Sekcją 6 § 4-7 niemieckiego kodeksu karnego wprowadzono zasadę jurysdykcji uniwersalnej, zgodnie z którą prawo niemieckie stosuje się do niewolnictwa, handlu narkotykami, rozpowszechnianiu pornografii dziecięcej niezależnie od miejsca popełnienia przestępstwa. Tę samą zasadę stosuje się wobec nieuprawnionego dostępu i ujawnienia tajemnicy handlowej przedsiębiorstw mających siedzibę na terytorium Niemiec czy też nielegalnego handlu organami (również za pomocą Internetu)[349].

Zastosowanie zasady terytorialności w odniesieniu do różnych rodzajów przestępstw, czyli na przykład nienawiści czy też pornografii w Internecie oraz możliwości zastosowania prawa niemieckiego wzbudziły rozbieżności w doktrynie. Pierwsze - restrykcyjne podejście (ang. *restrictive approach*) - zakłada, że sprawca, który umieścił na przykład treści pornograficzne na zagranicznym serwerze, rozesłał e-maile do niemieckich użytkowników czy też zamieścił materiały o określonej treści w grupach dyskusyjnych zlokalizowanych na niemieckich serwerach - nie podlegałby jurysdykcji niemieckiej. Z kolei drugie szerokie podejście (ang. *extensive approach*) zakłada, że miejscem popełnienia czynu są wszystkie te miejsca, gdzie czyn abstrakcyjnie mógł nastąpić. Zwolennicy tej teorii stoją na stanowisku, że prawo niemieckie można będzie zastosować nie tylko w stosunku do osoby, która znajdując się w innym kraju rozsyła e-mailem treści pornograficzne do Niemiec, ale również w stosunku do danych znajdujących się na zagranicznym serwerze, mimo że nie miałby on żadnego związku z Niemcami. Argumentują oni, że międzynarodowe oddziaływanie sieci komputerowych spowodowane rozwojem Internetu skutkuje pojawieniem się możliwości, iż dane te mogą być dostępne na terytorium Niemiec. Fakt możliwości pojawienia się potencjalnego zagrożenia według zwolenników szerokiego podejścia jest wystarczający do możliwości zastosowania prawa niemieckiego. Inni teoretycy prawa wskazują na dodatkowe kryteria warunkujące możliwość zastosowania prawa niemieckiego. Będą nimi świadomość domniemanego sprawcy, iż udostępniane przez niego dane mogą być dostępne na terytorium

[348] U. Sieber, *Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions*, [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, t. 11, s. 188.
[349] Ibidem, s. 187-188.

Niemiec, działanie sprawcy w celu udostępnienia danych na terytorium Niemiec oraz język w którym dane i treści są udostępnianie[350].

Problematyczna okazała się kwestia określenia jurysdykcji w internetowych sprawach, w których udostępnia się treści czy też nawołuje do nienawiści na tle rasowym, propaguje partie i organizacje, które w swojej działalności głoszą treści zabronione lub nielegalne lub też pochwalają, umniejszają czy usprawiedliwiają czyny dokonane przez nazistów za pomocą treści zamieszczonych na zagranicznych serwerach. Punktem wyjścia do dalszych rozważań powinien być § 9 ust. 1 niemieckiego kodeksu karnego, który określa miejsce przestępstwa jako miejsce, gdzie sprawca działał lub zaniechał działania, do którego był obowiązany lub też gdzie skutek przestępczy nastąpił lub gdzie według zamiaru sprawcy miał nastąpić[351].

Zagadnienie udostępniania w cyberprzestrzeni treści o charakterze nazistowskim zostało podjęte w niemieckim orzecznictwie w sprawie *Geralda Fredericka Tőbena*, obywatela australijskiego, który za pomocą stworzonej przez siebie strony internetowej, umieszczonej na australijskim serwerze, publicznie znieważał osoby pochodzenia żydowskiego, rewidował i usprawiedliwiał zbrodnie nazistowskie oraz obrażał pamięć osób zmarłych, jakie to czyny są karane w prawie niemieckim. Maciej Siwicki wskazuje, iż *Bundesgerichtshof* (Federalny Trybunał Sprawiedliwości, BGH) po rozpoznaniu sprawy stwierdził, iż „adresatami jego rewizjonistycznych artykułów udostępnianych z wykorzystaniem Internetu, pomimo, że były one w języku angielskim, byli obywatele Niemiec. (...) Sąd podkreślił również, że oskarżony zamieszczając informacje w Internecie, musiał liczyć sie z ich ogólnodostępnością oraz z tym, iż mogą być one dalej bezproblemowo rozpowszechniane w Niemczech, stanowiąc realne zagrożenie dla porządku prawnego w tym państwie. (....) miejscem skutku przestępnego było terytorium Niemiec, ponieważ policjanci prowadzący dochodzenie zapoznali się z tymi treściami w czasie przeglądania zawartości strony internetowej. BGH podkreślił również, że § 130 niemieckiego kodeksu karnego [dotyczący znieważenia społeczności żydowskiej] może - w ograniczonym zakresie - znaleźć zastosowanie zarówno do zagranicznych usługodawców świadczących usługi drogą elektroniczną, jak i użytkowników będących obywatelami innych krajów, którzy udostępniają informacje zakazane przez prawo lub pomagają w dostępie do nich”[352].

[350] Ibidem, s.189 -191.
[351] M. Siwicki, *Pojęcie* ..., s. 25.
[352] Ibidem, s. 25.

Polska

Ustawodawca w polskim kodeksie karnym[353] (k.k.) uregulował kwestię swojej jurysdykcji karnej dość szeroko. Artykułem 5 k.k. wprowadzono zasadę terytorialności, która stanowi, iż polską ustawę karną stosuje się do sprawcy, który popełnił czyn zabroniony na terytorium Polski, ale również na polskim statku wodnym lub powietrznym, chyba że umowa międzynarodowa, której Rzeczpospolita Polska jest stroną stanowi inaczej.

Zasada jurysdykcji skutkowej znalazła odzwierciedlenie w art. 6 § 2 k.k., który przewiduje, iż miejscem popełnienia przestępstwa jest miejsce, w którym sprawca działał lub zaniechał działania do którego był obowiązany, albo gdzie skutek stanowiący znamię czynu zabronionego nastąpił, lub według zamiaru sprawcy miał nastąpić. W polskim porządku prawnym przyjęto więc zasadę wielomiejscowości czynu zabronionego. Andrzej Wąsek i Marek Kulik wskazują, iż sporne w polskiej doktrynie jest zagadnienie czy tak szeroko ujęte *locus delicti* czynu obejmuje również tak zwane przestępstwa tranzytowe, czyli takie, których związek przyczynowy przebiega przez terytorium RP, ale zarówno miejsce popełnienia czynu jak i skutek przestępstwa leżą poza granicami Polski[354]. Marian Cieślak odrzuca na gruncie prawa polskiego koncepcję przestępstwa tranzytowego uzasadniając, iż nie pozwalają na to względy legalizmu[355].

Zasada obywatelstwa (zasada narodowości podmiotowej) znajduje odzwierciedlenie w art. 109 k.k., który stanowi, że polską ustawę karną stosuje się do obywatela polskiego, który popełnił przestępstwo za granicą. Pociągnięcie sprawcy do odpowiedzialności karnej uzależnione jest jednak od spełnienia warunku podwójnej karalności czynu. Polska ustawa karna będzie miała zastosowanie wówczas, gdy przestępstwo zostało popełnione poza granicami Polski przez obywatela polskiego. Bez znaczenia jest wówczas fakt, czy sprawca posiada podwójne obywatelstwo. Czynnikiem decydującym jest tu okoliczność, iż sprawca w czasie popełnienia czynu legitymował sie polskim obywatelstwem. Późniejsze zrzeczenie się obywatelstwa pozostaje bez wpływu na możliwość stosowania polskiej jurysdykcji karnej.[356]

[353] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz. U. z 1997 r. nr 88, poz. 553 z późn. zm.
[354] A. Wąsek, M. Kulik, *Zasady odpowiedzialności karnej (art. 1-12)*, [w:] M. Filar (red.), *Kodeks Karny. Komentarz*, Warszawa 2010, s. 36.
[355] M. Cieślak, *Polskie prawo karne. Zarys systemowego ujęcia*, Warszawa 1994, s. 100.
[356] W. Wróbel, A. Zoll, *Polskie prawo karne. Część ogólna*, Kraków 2010, s. 143.

Artykuł 112 k.k. wprowadza zasadę jurysdykcji ochronnej, która stanowi, że polską ustawę karną stosuje się do polskiego obywatela i cudzoziemca, niezależnie od obowiązujących w miejscu popełnienia przestępstwa przepisów, jeżeli popełniają oni:

1) przestępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu Polski,
2) przestępstwa przeciwko polskim urzędom lub funkcjonariuszom publicznym,
3) przestępstwa przeciwko istotnym polskim interesom gospodarczym,
4) przestępstwa fałszywych zeznań złożonych wobec urzędu polskiego,
5) przestępstwa, z którego została chociażby pośrednio osiągnięta korzyść majątkowa na terytorium Polski.

Artykuł 112 k.k. ustanawia zasadę narodowości przedmiotowej nieograniczonej nazywanej również zasadą ochronną nieograniczoną. Przepis ten pozwala na pominięcie warunku podwójnej karalności czynu w przypadku popełnienia za granicą przestępstwa enumeratywnie wymienionego w tym przepisie przez obywatela polskiego lub cudzoziemca[357].

Zasada jurysdykcji uniwersalnej znalazła z kolei odzwierciedlenie w art. 113 k.k., który w swych postanowieniach zakłada, iż Rzeczpospolita Polska ma prawo do wykonywania swojej jurysdykcji karnej w stosunku do obywatela polskiego lub cudzoziemca, który popełnił przestępstwo poza terytorium kraju, do którego ścigania Polska jest zobowiązana na mocy umowy międzynarodowej lub przestępstwa określonego w Rzymskim Statucie Międzynarodowego Trybunału Karnego. Przepis ten stanowi odstępstwo od wyrażonego w art. 111 § 1 k.k. warunku podwójnej przestępczości czynu. Pociągnięcie sprawcy do odpowiedzialności karnej uzależnione jest od tego, czy dany czyn został spenalizowany na mocy umowy międzynarodowej, której Rzeczpospolita Polska jest stroną[358].

Wielka Brytania

W angielskim systemie prawa jurysdykcja ma charakter terytorialny i w głównej mierze opiera się na kryterium miejsca popełnienia czynu zabronionego w znaczeniu jego

[357] P. Hofmański, *Komentarz do art. 112 K.K.*, [w:] M. Filar (red.), *Kodeks Karny. Komentarz*, Warszawa 2010, s. 560.
[358] Kodeks karny, art. 111-113.

skutku. Sądem właściwym do rozpoznania sprawy będzie siedziba sądu, w obrębie którego czyn nastąpił lub też wystąpiła jego znaczna część. Sądy brytyjskie z zasady nie poddają pod swoją jurysdykcję przestępstw popełnionych poza granicami Anglii i Walii, nawet jeżeli ich sprawcą był obywatel brytyjski. Wyjątki od reguły stosowania zasady terytorialnej mają charakter ustawowy i dotyczą wyszczególnionej kategorii przestępstw popełnionych z użyciem systemów informatycznych, czyli rozpowszechnianie pornografii dziecięcej[359].

Maciej Siwicki podkreśla, że „w Wielkiej Brytanii, podobnie jak na tle polskiego czy niemieckiego ustawodawstwa rozróżnia się pomiędzy *initiatory* (porównywalne „miejsce działania", niem. *Ort der Tathandlung*) a *terminatory* (porównywalne z „miejscem skutku" niem. *Ort der Taterfolg*). Dla określenia miejsca popełnienia przestępstwa decydujące jest to, czy dla danego przestępstwa niezbędne jest wywołanie skutku, czy też same przestępne zachowanie się (charakter popełnionego czynu). Problematyczne są przy tym przypadki, w których miejsce działania sprawcy nie jest tożsame z miejscem nastąpienia skutku przestępnego. Według orzecznictwa, w powyższej sytuacji dla określenia właściwości podstawową przesłanką określającą jurysdykcję jest miejsce, gdzie ostatnie działania sprawcy nastąpiły lub gdzie doszło do realizacji znaczącej części znamion czynu zabronionego"[360].

Pierwszym aktem prawnym regulującym kwestię przestępstw popełnianych przy użyciu komputera był *Computer Misuse Act*[361] z 1990 roku. Ustawa powstała jako oddolna inicjatywa, która z czasem zdobyła poparcie rządu i stała się pełnoprawnym aktem prawnym. Wprowadziła penalizację trzech rodzajów przestępstw przeciwko integralności systemów komputerowych: pierwszy - nieuprawniony dostęp do danych komputerowych, drugi - nieuprawniony dostęp do danych komputerowych z zamiarem popełnienia lub ułatwienia popełnienia innego przestępstwa, trzeci - nieuprawniona zmiana danych komputerowych[362].

W związku z szybkim rozwojem Internetu i pojawieniem się nowych metod popełniania przestępstw w lipcu 2003 roku rząd brytyjski zreformował *Computer Misuse Act* z 1990 roku. W przypadku przestępstw transnarodowych jurysdykcja uzależniona jest od wystąpienia wystarczającego związku (ang. *significiant link*) z „krajem macierzystym/krajem pochodzenia", czyli Anglią, Walią lub Irlandią Północną. W przypadku popełnienia

[359] A. Adamski, *Podstawy …*, s. 939- 940.
[360] M. Siwicki, *Pojęcie …*, cz. 2, „Europejski Przegląd Sądowy" 2011, nr 10, s. 27.
[361] Tekst dostępny na: http://www.legislation.gov.uk/ukpga/1990/18 [28.04.2014].
[362] I. Walden, *Cybercrime and Jurisdiction in United Kingdom*, [w:] B.J. Koops, S.W. Brenner (red), *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, nr 11, s. 296.

przestępstwa uzyskania nieuprawnionego dostępu do danych komputerowych za wystarczający związek uznany jest fakt, że:

1) oskarżony był w kraju pochodzenia w chwil gdy dokonał czynu nieuprawnionego dostępu do komputera,
2) komputer zawierający dane lub program zabezpieczający przed nieuprawnionym dostępem znajdował się w kraju pochodzenia w czasie popełnienia czynu[363].

„W świetle angielskiego orzecznictwa można zauważyć, że z jednej strony, zarówno w stosunku do przestępstw polegających na naruszeniu integralności komputera (ang. *computer integrity crimes*), jak i pozostałych przestępstw popełnianych z wykorzystaniem komputera (ang. *computer - related crimes*) zauważalna jest tendencja do rozszerzenia zakresu obowiązywania angielskiego prawa z wykorzystaniem zasady terytorialnej. Na tym tle pojawia się ryzyko dynamicznej interpretacji *actus reus* i karania nieświadomych obcokrajowców, jedynie na podstawie natury środowiska technologicznego, z którego korzystają. Z drugiej strony, angielskie sądy z reguły nie zajmują się sprawami przestępstw popełnianych poza granicami Anglii i Walii, nawet, gdy sprawcą przestępstwa jest obywatel brytyjski. Odstępstwa od tej zasady są wyjątkowe i mają charakter ustawowy"[364].

Jedną z pierwszych spraw, w której podniesiony był problem jurysdykcji w Internecie była sprawa oszustwa na szkodę amerykańskiego banku Citybank[365]. W 1994 roku stał się ofiarą cyberprzestępców, którzy zdołali przelać, na swoje konto, z rachunków bankowych klientów banku kwotę około 12 milionów dolarów. Po przeprowadzeniu śledztwa i dzięki międzynarodowej współpracy organów ścigania zidentyfikowano sprawcę. Władimir Levin został aresztowany w Anglii i mimo składanych apelacji, dokonano jego ekstradycji na terytorium Stanów Zjednoczonych[366].

Podstawowym problemem w sprawie *Levin* była kwestia konfliktu jurysdykcyjnego kilku państw. Obrońca oskarżonego twierdził, iż czyn został popełniony w Rosji, ponieważ sprawca przebywając w Sankt Petersburgu wprowadził do swojego komputera program, który umożliwił dokonanie oszustwa. Stąd też - w opinii obrońcy *Levina* - sąd brytyjski winien zastosować prawo rosyjskie. Z kolei pełnomocnik popierający amerykański wniosek

[363] Ibidem, s. 297.
[364] M. Siwicki, *Pojęcie locus delicti …*, cz. 2, s. 29.
[365] Wyrok Sądu Apelacyjnego House of Lords, z dnia 10 kwietnia 1997 r.,w sprawie *R.przeciwko Governor of Brixton Prison and another, ex parte Levin,* sygn. akt. 4 All ER 350, All ER 289.
[366] I. Walden, op. cit., s. 294.

ekstradycyjny twierdził, że przestępstwo miało miejsce tam, gdzie nastąpiły zmiany w systemie komputerowym banku Citybank, czyli w Parsippany stan New Jersey, USA. Sędzia przychylił się do wniosku ekstradycyjnego argumentując, że podejrzany wprowadzając w swoim komputerze program - w czasie rzeczywistym - spowodował skutek w serwerach Citybanku[367]. Sąd uznał zatem, że czyn popełniono w miejscu wystąpienia skutku przestępstwa (ang. *termination*).

Regulacje pozaeuropejskie

Australia

Australia posiada system prawa federalnego, lokalnego i związkowego[368]. Złożoność australijskiego ustawodawstwa dotyczącego cyberprzestępczości jest związana z faktem, iż na poziomie państwowym, sześciu stanów i trzech terytoriów panuje różnorodne prawo karne, w tym prawo dotyczące cyberprzestępczości[369].

Stany i terytoria mają prawo legislacyjne, wykonawcze i sądowe. Uprawnienia legislacyjne Związku Australijskiego jako państwa zostały ograniczone do określonych materii takich, jak sprawy międzynarodowe, międzystanowy handel, podatki, sprawy zagraniczne, kwestie waluty, bankowości czy własności intelektualnej. Państwo jako takie nie ma mocy legislacyjnej w sprawach karnych, które z zasady przysługują wyłącznie stanom i terytoriom. Władze państwowe jednak mogą uchwalać przepisy karne w ramach przyznanego zakresu kompetencji wprowadzając karalność niektórych form oszustw, czy też penalizując przestępstwa telekomunikacyjne, terroryzm, piractwo praw autorskich czy też własności przemysłowej. Oczywiste jest, że część z tych przestępstw może więc dotyczyć cyberprzestrzeni[370]. Australijczycy uznają, że prawo karne, tak jak edukacja czy zdrowie

[367] Ibidem, s. 295.
[368] Państwo to dzieli sie na sześć stanów: Australię Południową, Australię Zachodnią, Nową Południową Walię, Queensland, Tasmanię i Wiktorię. Wskazane stany zostały przekształcone w 1901 roku z kolonii w Związek Australijski (ang. *Commonwealth of Australia*). Terytorium kraju podzielić również można na trzy terytoria federalne: Australijskie Terytorium Stołeczne, Terytorium Północne i Terytorium Jarvis Bay.
[369] G. Urbas, P. Grabosky, *Cybercrime and Jurisdiction in Australia*, [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, t. 11, s. 49.
[370] Ibidem, s 50.

winne być stanowione przez stanowych prawodawców. Co ciekawe, w niektórych stanach oparto się na systemie *common law*, w innych zaś większą rolę odgrywają regulacje kodeksowe.[371]

Podstawową zasadą jurysdykcyjną stosowaną w Australii jest zasada jurysdykcji terytorialnej. Prawo państwowe wyróżnia standardową jurysdykcję geograficzną (ang. *standard geographical jurisdiction*) i cztery rodzaje przedłużonej jurysdykcji geograficznej (ang. *extended geographical jurisdiction*). Standardowa jurysdykcja geograficzna stosowana jest gdy:

1) czyn w całości lub w części wystąpił na terytorium Australii, albo na pokładzie australijskiego statku morskiego lub powietrznego,
2) czyn popełniono poza terytorium Australii, jednakże skutek przestępstwa wystąpił w całości lub w części na terytorium Australii, albo na pokładzie australijskiego statku morskiego lub powietrznego,
3) przestępstwo ma charakter pomocniczy, a jego dokonanie nastąpiło lub ma nastąpić w całości lub w części na terytorium Australii, albo na pokładzie australijskiego statku morskiego lub powietrznego[372].

Pamiętać należy, że australijskie prawo opiera się na systemie *common law*. Prawo precedensowe oraz system federalny wpływa negatywnie na bardzo zróżnicowaną judykaturę w różnych rejonach kraju[373]. Z tych powodów zdecydowano się wprowadzić normy o charakterze pozytywnym. Australijski *Cybercrime Act 2001* stanowi, że do zasad rozszerzonej jurysdykcji geograficznej kategorii A stosuje się odpowiednio przepisy *Criminal Code Act 1995*, według których państwową jurysdykcję stosuje się, jeżeli stanowa jurysdykcja nie znajduje zastosowania, do czynów popełnionych poza terytorium Australii, jeżeli sprawca, w czasie jego popełnienia był obywatelem Australii. Do cyberterroryzmu na poziomie państwowym stosuje się przedłużoną jurysdykcję geograficzną kategorii D, która stanowi, że osoba popełnia przestępstwo w rozumieniu przepisu, jeżeli czyn lub nawet skutek czynu wystąpił na terytorium Australii. Z kolei w systemie prawa stanowego czyn podlega pod jurysdykcję stanową w przypadku wystąpienia „wystarczającego czynnika terytorialnego" (ang. *sufficient territorial nexus*), czyli jeżeli czyn popełniono lub skutek

[371] J. Broome, *Comonwealth / State Boundaries in Crime and Justice*, artykuł dostępny online: http://www.aic.gov.au/media_library/conferences/outlook99/broome.pdf [10.09.2016].
[372] G. Urbas, P. Grabosky, op. cit., s. 61.
[373] M. Weinberg, *The criminal jurisdiction of the Federal Court*, artykuł dostępny online: http://www.austlii.edu.au/au/journals/NSWBarAssocNews/2008/53.pdf, [10.09.2016].

wystąpił w całości lub w części na terytorium stanu[374]. Australia od 2013 roku jest stroną Konwencji o cyberprzestępczości wobec czego przepisy krajowe są w znacznym stopniu zharmonizowane z międzynarodowymi standardami.

Stany Zjednoczone Ameryki

Praktyka legislacyjna poruszająca kwestię cyberprzestępczości ukształtowała się nieco inaczej w Stanach Zjednoczonych niż w Europie. Państwa europejskie podjęły próbę penalizacji zachowań w przestrzeni wirtualnej dotyczących funkcji komunikacyjnych związanych z udostępnianiem i przekazywaniem określonych, zakazanych przez prawo treści takich, jak „twarda" pornografia, propagowanie treści nazistowskich czy rasistowskich. Jak wskazuje Andrzej Adamski, podobnych rozwiązań prawnych nie ma w legislaturze USA. Wyrażanie nawet kontrowersyjnych opinii jest uważane w Stanach za wolność słowa i jest chronione Pierwszą Poprawką do Konstytucji, zabraniającą wydawania ustaw ograniczających wolność słowa i prasy[375].

Maciej Siwicki podnosi, że „również w tym państwie podstawową zasadą określenia jurysdykcji jest zasada terytorialna. Podobnie jak w innych państwach systemu *common law*, odstępstwa od tej zasady są wyjątkowe i mają charakter ustawowy. I tak, przykładowo, według *Restatment (Third) of Foreign Relations Law of the United States* z 1987 r. zastosowanie zasady personalnej przy określeniu jurysdykcji uzasadnione jest, tylko wtedy jeżeli jest ku temu uzasadniony powód. Podkreśla się przy tym, że jurysdykcja w pozaterytorialnym sporze musi być podejmowana rozsądnie. Zastosowanie zasady terytorialnej jest zazwyczaj uzasadnione istnieniem związku pomiędzy czynem sprawcy a terytorium państwa, np. podjęcie działania na danym terytorium, również gdy skutek nastąpił poza nim, oraz wystąpienie skutku na terytorium danego państwa, nawet jeżeli czyn został popełniony za granicą. W państwie tym, ze względu na prawo precedensowe, będzie miało zastosowanie wiele różnych reguł kolizyjnych służących określeniu miejsca popełnienia przestępstwa, obejmujących zarówno doktrynę najściślejszego powiązania, jak i zasadę prawa sądu (ang. *lex fori*)"[376].

[374] G. Urbas, P. Grabosky, op. cit., s. 62-64.
[375] A. Adamski, *Podstawy* …, s. 955.
[376] M. Siwicki, *Pojęcie …,* cz. 2, s. 29.

W literaturze przedmiotu analizującej amerykańskie ustawodawstwo i orzecznictwo uznano, że „można zauważyć oparcie linii orzeczniczej sądów amerykańskich na stanowisku, że sama dostępność do wykorzystywanych przez sprawcę usług świadczonych drogą elektroniczną (np. strony www) z terytorium USA nie jest wystarczająca do ustanowienia jurysdykcji. Aby amerykański sąd mógł uznać swoją jurysdykcję, powinien zwrócić uwagę przede wszystkim na wolę i aktywność na tym terenie osoby, której zarzucone jest popełnienie przestępstwa. W tym celu kluczowe okazuje się przede wszystkim ustalenie potencjalnego adresata informacji. Niewątpliwie najważniejszą cechą jest rezygnacja z jednoznacznych norm kolizyjnych na rzecz indywidualnej analizy okoliczności każdego przypadku. Z reguły prowadzi to jednak do uprzywilejowania własnego prawa”[377].

2.2 Próba identyfikacji właściwych przedmiotowo norm wobec cyberprzestrzeni

Rozważając kwestie rozwoju odpowiednich regulacji dotyczących jurysdykcji w cyberprzestrzeni należy pamiętać, że Internet stawia przed nami wyzwania nieznane tradycyjnemu ujęciu jurysdykcji. Transgraniczny, transnarodowy charakter cyberprzestrzeni spowodował, iż strony stosunków prawnych mogą być oddalone od siebie o miliony kilometrów. Wykonywanie kompetencji jurysdykcyjnej jest ściśle związane z określoną przestrzenią - terytorium - i zazwyczaj tam jest realizowane. Władztwo państwa ma wówczas charakter zupełny i wyłączny[378]. Jest to podstawowa zasada przyjmowana przy ustalaniu prawa właściwego do rozstrzygnięcia sporu - zarówno w aspekcie karnym, jak i cywilnym. We współczesnym obrocie prawdziwy problem powstaje jednak, gdy postawi się pytanie, jak zachować się jednak w przestrzeni, która fizycznie nie istnieje, nie ma określonego obszaru, ale charakteryzuje się miliardami użytkowników z każdego zakątka ziemi, z nieograniczoną liczbą codziennie zawieranych transakcji, w tym o charakterze przestępczym.

Powszechnie przyjmuje się, że sądem właściwym dla rozstrzygnięcia sprawy jest sąd właściwy według miejsca zamieszkania powoda. Zasada ta znajdzie odzwierciedlenie również w odniesieniu do sporów internetowych. Zarówno normy międzynarodowe, jak i regulacje

[377] Ibidem, s. 31.
[378] J. Kulesza, *Międzynarodowe …*, s. 30-31.

europejskie często wskazują jednak wyjątki od tej zasady chociażby w odniesieniu do konsumentów, którzy będąc słabszą stroną stosunku mogą wytoczyć powództwo przed sądem właściwym dla swojego miejsca zamieszkania. Łącznikami jurysdykcyjnymi mogą być: miejsce wykonania umowy, świadczenia usługi, miejsce dostawy i inne.

Wydaje się, że łącznikiem określającym jurysdykcję właściwą w cyberprzestrzeni nie powinien być wyłącznie łącznik dostępności przekazów internetowych. Rozwiązanie takie jest szeroko krytykowane między innymi przez Gwendoline Lardeux. Tak szeroko rozumiany łącznik jurysdykcyjny spowodowałoby podleganie cyberprzestrzeni pod jurysdykcję równocześnie wszystkich państw świata i wszystkich porządków prawnych. Coraz większa część naszego życia i obrotu gospodarczego jest dokonywana w cyberprzestrzeni. Konieczne jest zapewnienie bezpieczeństwa i stabilności tego obrotu. Jest to niezwykle trudne zadanie. Cechy charakterystyczne cyberprzestrzeni powodują, że trudno jest wypracować jeden efektywny i skuteczny łącznik jurysdykcyjny, który miałby zastosowanie w przypadku wszystkich sporów mogących mieć miejsce w przestrzeni wirtualnej.

Brak międzynarodowych norm prawnych regulujących jednoznacznie problem jurysdykcji w cyberprzestrzeni oraz niewielkie szanse na zmianę *status quo* w najbliższym czasie powodują, że wiele państw rozciąga swoją jurysdykcję na czyny dokonywane w cyberprzestrzeni. Wydaje się, że trend ten będzie się utrzymywał dopóty dopóki nie zostanie przyjęte racjonalne rozstrzygnięcie problemu. Właściwe jest posiłkowanie się rozwiązaniami przyjętymi w ramach Unii Europejskiej. Akty prawne takie, jak Rzym I i Rzym II mogą być stosowane również poza granicami Unii Europejskiej. Przyjęte w nich rozwiązania są nieco kazuistyczne, lecz niezmiernie przydane do rozstrzygnięcia sporów.

Sprawy dotyczące dystrybucji nielegalnych treści w Internecie pokazują, że interesy narodowe państw bywają zagrożone nie tylko czynami popełnionymi na ich terytoriach, ale również czynami popełnionymi lub mającymi skutek w innych krajach. Internet zapewnia szybki i nieskomplikowany dostęp do danych elektronicznych przechowywanych zarówno w kraju, jak i za granicą. Dla interesów państwa nie ma zatem znaczenia fakt, czy treści zawarte *on-line* są dostępne w kraju czy poza jego granicami. Podstawowym kryterium określania jurysdykcji jest zasada terytorialności - co stanowi również odzwierciedlenie równości państw i poszanowania granic terytorialnych. Mimo to, zasada ta okazuje się być niewystarczająca do skomplikowanych stanów faktycznych mogących mieć miejsce w przestrzeni wirtualnej.

Z tych też względów zrozumiałe jest, że krajowe systemy prawne chcą *de lege ferenda* rozszerzyć swoją jurysdykcję na dane przechowywane na zagranicznych serwerach, lecz dostępnych za pośrednictwem Internetu. Rozważając przypadki eksterytorialnego stosowania prawa krajowego należy stwierdzić, że powinno się dążyć do ich zminimalizowania i zakreślenia konkretnych okoliczności, w których państwa będą mogły stosować prawo krajowe poza swoim terytorium. Kryterium te przyjęte na podstawie obiektywnych okoliczności zewnętrznych lub subiektywnych celów sprawcy prowadzić powinno do konkluzji, czy treści umieszczone w Internecie były skierowane bezpośrednio do odbiorów w danym kraju. Możliwe jest również zastosowanie zasady jurysdykcji uniwersalnej w odniesieniu do szczególnych rodzajów przestępstw popełnianych przy pomocy cyberprzestrzeni takich, jak pornografia dziecięca czy cyberterroryzm. Dystrybucja nielegalnych treści, czyli przesyłanie wirusów, robaków, ataków DDoS wskazuje, że czyny te popełniane przez cyberprzestępców mogą wpływać lub być związane z wieloma państwami równocześnie. Konieczne jest więc wprowadzenie dodatkowych regulacji wskazujących prawo właściwe w przypadku konfliktów jurysdykcyjnych. Specyficzna konstrukcja cyberprzestrzeni wymyka się spod klasycznych norm jurysdykcyjnych. Niezbędna jest więc opracowanie nowych praw i zasad regulujących prawo i jurysdykcję w cyberprzestrzeni[379].

Omawiany temat nie ogranicza się jedynie do możliwości stosowania przez państwa sankcji karnych. Wiele z przestępstw popełnianych za pomocą systemu komputerowego ma transgraniczny charakter. Granice rozumiane w tradycyjnym tego słowa znaczeniu nie mają i nie mogą mieć zastosowania do przestrzeni wirtualnej. Cyberprzestępstwa nie mogą być regulowane wyłącznie przez prawa krajowe poszczególnych państw. Obecnie, ani kompleksowe środki kontroli, ani rozległe przepisy krajowe dotyczące jurysdykcji nie mogą zapobiec temu, by na przykład polski użytkownik sieci ściągnął z amerykańskiego serwera nielegalne według prawa polskiego, a legalne według prawa USA, treści. Internauta nie ma możliwości sprawdzenia przepisów prawnych państw z każdego zakątku globu dotyczących korzystania z zasobów cyberprzestrzeni.

Podstawą jurysdykcji jest kilka podstawowych zasadach opartych na łączniku obywatelstwa, miejsca działania, miejsca skutku lub też miejsca, gdzie według zamiaru skutek sprawcy miał nastąpić. W przypadku cyberprzestepstw dokładne określenie miejsca ostatniej z tych kategorii może nastręczyć wielu problemów. Cyberprzestrzeń bowiem sprzyja

[379] U. Sieber, op. cit., s. 207-208.

przypadkowości, ale również wielomiejscowości miejsca skutku. Osoba umieszczająca określone treści w Internecie nie jest w stanie przewidzieć, gdzie skutek działania nastąpi lub też czy działanie zgodne z prawem w jego kraju, nie jest kryminalizowane w innym państwie[380].

Prawo międzynarodowe zgodnie z zasadą eksterytorialności przewiduje również możliwość wyłączenia spod jurysdykcji państwa miejscowego w trybie umów międzynarodowych pewnego obszaru jego terytorium, na przykład baz wojskowych, okrętów, misji dyplomatycznych. Znajdująca się w tych jednostkach cyber - infrastruktura (serwery, komputery i inne) będzie wówczas korzystać z immunitetu państwa wysyłającego. Satelity w przestrzeni kosmicznej będą mogły korzystać z immunitetu jedynie, jeżeli będą użytkowane wyłącznie do celów wojskowych. W doktrynie podkreśla się, że jeżeli dany satelita wykorzystywany jest zarówno do celów komercyjnych, jak i wojskowych nie będzie on podlegał ochronie[381].

Stosowanie prawa w cyberprzestrzeni to kwestia nie tylko przepisów związanych z jurysdykcją materialną. Również procesowe aspekty ścigania cyberprzestępstw mogą nastręczyć wielu trudności. W wielu przypadkach tylko jedno z kilku państw dotkniętych przestępstwem będzie miało faktyczną możliwość podjęcia efektywnego ścigania i skazania sprawcy według swojego prawa krajowego. Oprócz wprowadzania regulacji krajowych umożliwiających stosowanie sankcji karnych powinien być stworzony system ułatwiający ściganie poważnych cyberprzestępstw na poziomie międzynarodowym. Najpoważniejszym problemem jest stworzenie minimalnych standardów prawa materialnego i proceduralnego mającego na celu regulację najpoważniejszych przestępstw popełnianych przy użyciu systemów komputerowych. Równocześnie należy zapewnić skuteczną i efektywną współpracę międzynarodową w przeciwdziałaniu, ale również szybkim ściganiu cyberprzestępstw. Nieocenionym aktem prawnym, który w znacznym stopniu przyczynił się do zharmonizowania niektórych przepisów dotyczących przestępstw komputerowych, była Konwencja Rady Europy o cyberprzestępczości. Dalsza kooperacja takich organów, jak Rada Europy czy też grupa robocza G8 High - Tech Crime, może w przyszłości znacząco wpłynąć

[380] M. Siwicki, *Podstawy …*, s. 20.
[381] M.M. Schmitt, *Tallinn Manual on the International law applicable to the cyber warfare*, Cambridge 2013, s. 23-24.

na harmonizację przepisów i zwiększenie efektywności ścigania przestępstw popełnianych w cyberprzestrzeni[382].

Odnosząc się do kwestii regulacji jurysdykcji w sprawach cywilnych w ocenie autorki pracy najlepszym sposobem rozwiązania potencjalnego konfliktu jest zawarcie w umowie klauzuli jurysdykcyjnej. Rozstrzygnięcie takie jest zgodne z zasadą swobody umów, należy bowiem respektować prawo stron do możliwości kształtowania łączącego je stosunku prawnego, czyli wyboru prawa i sądu właściwego do rozstrzygnięcia ewentualnego sporu. Rozwiązanie takie daje pewność i stabilność stosunku łączącego strony. Dopiero w przypadku, gdy klauzula taka nie została zawarta w umowie należy zastanowić się, w jaki sposób ustalić jurysdykcję właściwą.

Trafny wydaje się pogląd Joanny Kuleszy, która stwierdza, że „żadne inne medium nie wpłynęło na obraz dzisiejszego prawa i regulacji stosunków międzynarodowych tak bardzo jak sieć globalna. Okazało się bowiem, że tradycyjne kryterium terytorialności zupełnie nie znajduje zastosowania do relacji nawiązywanych pomiędzy obywatelami różnych państw w obszarze nazywanym cyberprzestrzenią. Stało się jasne, że to nowe miejsce międzyludzkich relacji wymaga regulacji prawnej, oraz że dotychczasowe regulacje nie wystarczą do konfrontacji z domeną elektroniczną. To właśnie Internet postawił przed krajowymi ustawodawcami działającymi na arenie międzynarodowej, setki pytań, na które tradycyjne normy prawa nie dawały odpowiedzi. To on wymógł konieczność ponownej interpretacji takich pojęć, jak granice władzy jurysdykcyjnej czy prawodawczej państw. Aterytorialny i zdecentralizowany Internet, tworzący nową, ponadnarodową przestrzeń wzajemnych interakcji, zlokalizowanych na wielu terytoriach ludzi, wymaga nowych rozwiązań prawnych czy to też głębokiej rekapitulacji tych już istniejących”[383].

[382] U. Sieber, op. cit., s. 208.
[383] J. Kulesza, *Międzynarodowe …*, s. 54.

CZĘŚĆ II

PRAWNOMIĘDZYNARODOWY WYMIAR CYBERPRZESTRZENI

- STATUS QUO

Rozdział 3

Identyfikacja regulacji prawnych cyberprzestrzeni z perspektywy międzynarodowej

Postęp techniki, rozwój nowych technologii, a cyberprzestrzeni w szczególności prowadzi do powstania nowych wyznań w zakresie ochrony jednostki. Podstawowym instrumentem takiej ochrony jest prawo, regulujące te obszary, w których kodeksy etyczne czy też samoregulacja nie mogą być efektywnym rozwiązaniem[384]. W rozdziale zostaną opisane podstawowe akty prawne i dokumenty związane z prawem cyberprzestrzeni. W pierwszej kolejności zostaną przedstawione regulacje wypracowane w systemie ONZ - zarówno traktatowe, jak i te o niewiążącym charakterze, które znacznie przyczyniły się do unifikacji ustawodawstw krajowych. Następnie zostaną przedstawione wybrane regulacje regionalne, poczynając od dorobku Rady Europy, która opracowując Konwencję o cyberprzestępczości wywarła największy wpływ na unifikację przepisów dotyczących cyberprzestępczości. Nie mniej istotne są liczne akty prawne Unii Europejskiej, regulujące wiele spraw - od kwestii cyberbezpieczeństwa, po handel elektroniczny, bazy danych czy własność intelektualną.

Badając regulacje dotyczące cyberprzestrzeni nie sposób jest nie odnieść się do dokumentów organizacji wyspecjalizowanych np. NATO, które w ostatnich latach uznało cyberprzestrzeń za kolejną, czwartą przestrzeń działalności militarnej państw (oprócz sił morskich, lądowych i powietrznych). Zwrócić należy uwagę na dokumenty Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (w kwestii wspierania cyberbezpieczeństwa) oraz Organizacji Współpracy Gospodarczej i Rozwoju (dotyczących różnych aspektów działalności człowieka w cyberprzestrzeni). Konieczne jest zaciśnienie międzypaństwowej współpracy organów ścigania - Interpolu, Europolu i Europejskiego Centrum do spraw Walki

[384] K. Chałubińska-Jentkiewicz, *Wstęp,* [w:] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 19.

z Cyberprzestępczością, by regulacje międzynarodowe dotyczące cyberprzestępczości były skutecznie wykonywane.

W dysertacji opisano przepisy krajowe państw wybranych, aby zrozumieć kierunek zmian regulacji prawnych cyberprzestrzeni, ponieważ w wielu przypadkach wywarły (bądź mogą wywrzeć w przyszłości) wpływ na kształtowanie się norm międzynarodowych. Doświadczenia krajów, które stały się ofiarami ataków wpłynęły bezpośrednio na międzynarodowe postrzeganie kwestii cyberbezpieczeństwa państwa. Równie znaczące są dokumenty supermocarstw: USA, Rosji czy Chin, które w sposób mniej lub bardziej jawny wykorzystują cyberprzestrzeń do realizacji swoich celów. Ciekawe może okazać się porównanie przepisów krajów wysoko rozwiniętych, które szybko dostosowują prawo do zmieniającego się cyfrowego świata.

Regulacje prawne i dokumenty organizacji międzynarodowych oraz postulaty wysuwane przez różnorakie instytucje i samych użytkowników kształtują współczesny obraz cyberprzestrzeni. Nie jest to przestrzeń łatwej regulacji, analiza starszych aktów prawnych ukazuje jak szybko dezaktualizują się, w obliczu postępu technologicznego, normy prawne dotyczące przestrzeni wirtualnej, oraz które postulaty zmian zyskały aprobatę społeczności międzynarodowej. W rozdziale zostaną opisane pokrótce regulacje dotyczące najważniejszych zagadnień działalności człowieka w cyberprzestrzeni - cyberprzestępczości, handlu elektronicznego, własności intelektualnej oraz cyberbezpieczeństwa państwa. Pozostałe problemy (związane chociażby z prawem bankowym czy podatkami) nie zostaną poruszone w niniejszej rozprawie z uwagi na mniejsze ich znaczenie oraz chęć uniknięcia zbytniej kazuistyczności prezentowanych zagadnień.

3.1. Prawnomiędzynarodowe regulacje cyberprzestrzeni

Pod koniec lat dziewięćdziesiątych XX wieku społeczność międzynarodowa dostrzegła potrzebę regulacji nowej przestrzeni - przestrzeni wirtualnej, która zaczynała w tym okresie zdobywać coraz więcej zwolenników i użytkowników. Transgraniczny charakter

cyberprzestrzeni spowodował, że podejmowane w niej działania bez problemu w ciągu kilku sekund przenikały granice państwowe. Z tych też powodów organizacje takie, jak Organizacja Narodów Zjednoczonych, Rada Europy, Unia Europejska i Organizacja Współpracy Gospodarczej i Rozwoju zaczęły podejmować kroki prawne w celu regulacji nowego, nieznanego wcześniej zjawiska cyberprzestrzeni. Ustanowione dokumenty stały się ramą prawną dla zwalczania różnych form cyberprzestępczości, rozwiązywania problemów związanych z prawami własności intelektualnej czy nowymi technologiami, czyli chociażby podpis elektroniczny czy pieniądz wirtualny. Akty prawne o charakterze międzynarodowym słały się również wskazaniem drogi legislacyjnej dla krajowych organów ustawodawczych.

Szczególne znaczenie mają prace Rady Europy i opracowana przez nią Konwencja o cyberprzestępczości sporządzona 23 listopada 2001 roku w Budapeszcie. Wskazana umowa międzynarodowa jest w chwili obecnej najistotniejszym aktem prawnym poruszającym tematykę zwalczania cyberprzestępczości. O jej doniosłym znaczeniu i potrzebie regulacji zjawiska świadczy chociażby fakt, przystąpienia do Konwencji państw spoza Rady Europy. W niniejszym rozdziale wskazany zostanie również bogaty dorobek legislacyjny Unii Europejskiej, która nie tylko kształtuje prawo państw członkowskich, ale również wyznacza trendy legislacyjne dla innych państw i organizacji międzynarodowych.

W niniejszym rozdziale zostaną omówione regulacje międzynarodowe, regionalne oraz krajowe, które mają zastosowanie do cyberprzestrzeni. Szczegółowo zostaną przedstawione akty prawne oraz inicjatywy podejmowane przez różne organizacje międzynarodowe, podmioty zajmujące się przestrzenią wirtualną oraz zagrożeniami i problemami w niej występującymi.

3.1.1. Regulacje wypracowane w systemie Organizacji Narodów Zjednoczonych

Największą organizacją międzynarodową zrzeszającą ponad 190 państw członkowskich jest Organizacja Narodów Zjednoczonych (ONZ). Głównymi celami ONZ

wyrażonymi w art. 1 Karty Narodów Zjednoczonych[385] jest utrzymanie międzynarodowego pokoju i bezpieczeństwa za pomocą zbiorowych i pokojowych wysiłków, rozwijanie przyjaznych stosunków między narodami opartych na poszanowaniu zasady równouprawnienia i samostanowienia narodów, rozwiązywanie międzynarodowych problemów na zasadzie współpracy oraz stanowienie ośrodka uzgadniania działań narodów w imię wspólnych celów.

3.1.1.1. Dorobek Organizacji Narodów Zjednoczonych

Jednym z pierwszych dokumentów ONZ, które odnosiły się do czynów dokonywanych za pośrednictwem przestrzeni wirtualnej, czyli przestępstw komputerowych, była Rezolucja Zgromadzenia Ogólnego ONZ nr 45/121[386] dotycząca przestępstw związanych z wykorzystaniem komputerów. Została przyjęta 14 grudnia 1990 roku w wyniku obrad VIII Kongresu Narodów Zjednoczonych na temat Zapobiegania Przestępczości i Postępowania z Przestępcami, który miał miejsce od 28 sierpnia do 7 września 1990 roku w Hawanie. Rezolucja Zgromadzenia Ogólnego ONZ nr 45/121: „wzywa państwa członkowskie do intensyfikacji wysiłków, skierowanych na skuteczne zwalczanie nadużyć komputerowych, w szczególności przez:

- wprowadzenie odpowiednich zmian do ustawodawstwa karnego materialnego i procesowego, w celu dostosowania istniejących definicji przestępstw oraz przepisów, dotyczących środków przymusu i dopuszczalności dowodów do ścigania nadużyć komputerowych i pozbawienia ich sprawców nielegalnie uzyskanych korzyści;
- usprawnienie zabezpieczeń systemów komputerowych, uwzględniając przy tym problemy związane z ochroną prywatności oraz praw i wolności obywatelskich;
- podjęcie kroków, mających na celu uwrażliwienie opinii publicznej oraz organów ścigania i wymiaru sprawiedliwości na znaczenie problemu zapobiegania przestępczości komputerowej;

[385] Karta Narodów Zjednoczonych, Dz.U. 1947, Nr 23, poz. 90.
[386] Rezolucja Zgromadzenia Ogólnego ONZ - A/RES/45/121 z 15.12.1990 r., dokument dostępny online, na oficjalnej stronie internetowej ONZ: http://www.un.org/documents/ga/res/45/a45r121.htm [10.10.2016].

- organizację szkolenia sędziów i funkcjonariuszy agend rządowych, odpowiedzialnych za zapobieganie, ściganie i sądzenie spraw o przestępstwa gospodarcze, związane z wykorzystaniem komputera;
- wypracowanie, we współpracy z zainteresowanymi organizacjami kodeksów etyki użytkowników komputerów i nauczenia tych zasad w ramach kształcenia informatyków;
- przyjęcie określonej polityki wobec ofiar przestępstw komputerowych, która byłaby zgodna z Deklaracją ONZ nt. Podstawowych Zasad Sprawiedliwości dla Ofiar Przestępstw i Nadużyć Władzy i obejmowała restytucję nielegalnie uzyskanych korzyści oraz zachęcała ofiary przestępstw komputerowych do składania zawiadomień o tych przestępstwach"[387].

Rezolucja nr 45/121 kładła duży nacisk na kwestie wprowadzenia do krajowych porządków legislacyjnych przepisów penalizujących nadużycia komputerowe. Wskazany dokument był podstawą do wydania w 1994 roku poradnika na temat zapobiegania i kontroli społecznej cyberprzestępstw *International review of criminal policy - United Nations Manual on the prevention and control of computer - related crime*, który odnosił się do problemów legislacyjnych w zakresie penalizacji przestępstw komputerowych[388].

W Wiedniu w 2000 roku odbył się X Kongres ONZ, w trakcie którego powołano grupę roboczą omawiającą zagadnienie cyberprzestępczości. Po zakończeniu obrad stwierdzono, że zachodzi potrzeba penalizacji nadużyć komputerowych, międzynarodowej współpracy pomiędzy organami ścigania i sektorem prywatnym oraz udzielania organom sprawiedliwości wsparcia technicznego i legislacyjnego koniecznego do efektywnej walki z przestępczością komputerową[389]. Konsekwencją X Kongresu ONZ było uchwalenie 22 stycznia 2001 roku przez Zgromadzenie Ogólne ONZ Rezolucji 55/63[390] Przeciwdziałanie przestępczym nadużyciom technologii informacyjnej (ang. *Combating the criminal misuse of information technologies*). Stanowi ona, że państwa winny zapewniać, aby prawo i praktyka obowiązująca na ich terytorium eliminowały sytuacje, w których cyberprzestępcy mogliby znaleźć tam bezpieczne schronienie, a same systemy prawne powinny posiadać regulacje chroniące poufność, integralność i dostępność danych i systemów komputerowych oraz

[387] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 9-10.
[388] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 28-29.
[389] Ibidem, s. 29.
[390] Rezolucja dostępna online na oficjalnej stronie internetowej ITU: http://www.itu.int/ITU-D/cyb/ cybersecurity/docs/UN_resolution_55_63.pdf [01.07.2015].

karalność czynów polegających na zdobyciu do nich nieuprawnionego dostępu[391]. Rezolucja w dużej mierze jest realizacją dziesięciopunktowego planu działania grupy G8 przyjętego w 1997 roku.

Dokument rezolucja Zgromadzenia Ogólnego ONZ (ZO ONZ) z 23 stycznia 2002 roku nr 56/121[392] dotycząca przeciwdziałania przestępnemu nadużywaniu technologii informacyjnych wzywa państwa, by przy opracowaniu regulacji krajowych, polityk i praktyk wprowadziły przepisy dotyczące zwalczania przestępstw popełnionych przy użyciu technologii informacyjnych. Zarekomendowano w nim, by państwa członkowskie w trakcie prac legislacyjnych na poziomie krajowym wzięły również pod uwagę osiągnięcia Komisji Zapobiegania Przestępczości i Wymiaru Sprawiedliwości[393]. Po raz kolejny podkreślono konieczność współpracy na poziomie międzynarodowym oraz wagę i rolę organizacji międzynarodowych, w tym ONZ, w zwalczaniu i przeciwdziałaniu zjawisku cyberprzestępczości.

W trakcie 57 sesji 31 stycznia 2003 roku ZO ONZ przyjęło Rezolucję nr 57/239 w sprawie stworzenia globalnej kultury cyberbezpieczeństwa[394] (ang. *Creation of global culture of cybersecurity*). W dokumencie podkreślono, że szybkie zmiany technologiczne znacząco wpływają na władzę państwową, biznes, organizacje i użytkowników sieci. Stwierdzono konieczność promowania kultury bezpieczeństwa posługiwania się sieciami informatycznymi, informowania o incydentach w sieci, zapewniania wolność wypowiedzi i wyrażania poglądów, nieskrępowanego przepływ informacji i komunikacji z odpowiednią ochroną danych osobowych. 30 stycznia 2004 roku ZO ONZ przyjęło Rezolucję nr 58/199[395] w sprawie stworzenia globalnej kultury cyberbezpieczeństwa i ochrony informatycznej infrastruktury krytycznej (*Creation of a global culture of cybersecurity and the protection of critical information infrastructures*)[396].

W trakcie kolejnego, XI Kongresu ONZ w sprawie Zapobiegania Przestępczości i Wymiaru Sprawiedliwości Karnej ONZ w Bangkoku w Tajlandii w 2005 roku przedmiotem

[391] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 216.
[392] Rezolucja dostępna online na oficjalnej stronie internetowej ITU: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf [01.07.2015].
[393] J. Kosiński, *Paradygmaty …*, s. 216.
[394] Rezolucja dostępna online na oficjalnej stronie internetowej ITU: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf [20.10.2016].
[395] A/RES/58/199.
[396] Rezolucja dostępna online na oficjalnej stronie internetowej ITU: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf [22.10.2016].

rozważań objęto analizę użycia systemów komputerowych w działalności przestępczej oraz ponadnarodowy charakter tych działań[397]. Wynikiem obrad było wydanie deklaracji końcowej (tak zwanej Deklaracji bangkockiej), która została zatwierdzona 20 marca 2006 roku Rezolucją Zgromadzenia Ogólnego ONZ nr 60/177[398]. Punkt 16 deklaracji poruszył kwestię wykorzystania nowych technologii do czynów przestępczych. Zachęcano do poszerzenia współpracy międzynarodowej, ale również partnerstwa z sektorem prywatnym w zakresie ścigania i zwalczania cyberprzestępczości.

W trakcie odbywającego się od 12 do 19 kwietnia 2010 roku XII Kongresu Narodów Zjednoczonych na temat Zapobiegania Przestępczości i Wymiaru Sprawiedliwości Karnej w Salvadorze w Brazylii zwrócono szczególną uwagę na konieczność monitorowania tendencji rozwoju cyberprzestępczości i wprowadzania odpowiednich nowelizacji przepisów karnych w zakresie cyberprzestępczości, prywatności, danych osobowych, podpisów cyfrowych, kryptografii oraz prawa handlowego. W czasie obrad poruszono problem stworzenia międzynarodowych standardów penalizacji przestępstw komputerowych, wspierania państw w walce i przeciwdziałaniu zjawisku. Eksperci debatowali, w jaki sposób można byłoby zunifikować na poziomie międzynarodowym kryminalizację cyberprzestępstw: czy przez opracowanie przez ONZ kompleksowych standardów normatywnych, czy może przez zalecenie implementacji przepisów Konwencji Rady Europy o cyberprzestępczości. Wobec ograniczonego zasięgu Konwencji o cyberprzestępczości postanowiono nie nakazywać implementacji Konwencji, lecz wzmocnić rolę ONZ w obszarach opisanych w art. 41 i 42 Deklaracji Salwadorskiej[399].

W dokumencie końcowym XII Kongresu ONZ - nazywanym Deklaracją Salwadorską[400] wezwano członków społeczności międzynarodowej do podejmowania wysiłków na rzecz zapobiegania, wykrywania i ścigania wszelkich form cyberprzestępczości. Współpraca ta miałaby polegać na współdziałaniu państw członkowskich, organizacji międzynarodowych oraz sektora prywatnego przez przeprowadzanie szkoleń, udzielanie wsparcia technicznego, wprowadzenie odpowiedniej legislatury w celu zwiększenia i

[397] M. Siwicki, *Cyberprzestępczość*…, s. 30.
[398] Deklaracja odstępna online na oficjalnej stronie internetowej UNODC: http://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2005/General_Assembly/A-RES-60-177.pdf [01.07.2015].
[399] M. Siwicki, *Cyberprzestępczość* …, s. 30.
[400] Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, dokument dostępny online na oficjalnej stronie internetowej UNDOC: https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf [01.07.2015].

ulepszenia bezpieczeństwa cyberprzestrzeni (art. 41). Kolejnym postulatem skierowanym do Komisji Zapobiegania Przestępczości i Wymiaru Sprawiedliwości był apel o powołanie pod auspicjami ONZ międzyrządowej grupy ekspertów w celu podjęcia studiów nad problemem przestępczości popełnianej w przestrzeni wirtualnej (art. 42)[401].

Zgromadzenie Ogólne ONZ 17 marca 2010 roku przyjęło Rezolucję nr 64/211[402] dotyczącą stworzenia globalnej kultury cyberbezpieczeństwa i zbilansowania wysiłków krajowych w celu ochrony informatycznej i infrastruktury krytycznej. Artykuł 13 Rezolucji wzywa się państwa członkowskie do weryfikacji krajowych przepisów legislacyjnych w zakresie cyberprzestępczości, prywatności, ochrony danych osobowych, podpisów cyfrowych i prawa handlowego, które mogą być nieaktualne lub przestarzałe w wyniku szybkiego rozwoju technologii informacyjnych i komunikacyjnych oraz dostosowanie ich do nowego stanu faktycznego, zwracając szczególną uwagę na Konwencję RE o cyberprzestępczości oraz Rezolucje Zgromadzenia Ogólnego ONZ nr 55/63 i 56/121[403].

Oprócz wyżej wymienionych regulacji również inne akty prawne i dokumenty przyjęte na forum Organizacji Narodów Zjednoczonych odnoszą się do przestępczości popełnianej w cyberprzestrzeni. Są to:

1. Konwencja ONZ przeciwko międzynarodowej przestępczości zorganizowanej (UNTOC)[404] przyjęta przez Zgromadzenie Ogólne ONZ 15 listopada 2000 roku - jest to umowa międzynarodowa zawarta w celu zapobiegania i zwalczania międzynarodowej przestępczości zorganizowanej. Opisano w niej międzynarodowe standardy walki z międzynarodowymi zorganizowanymi grupami przestępczymi oraz korupcją i praniem brudnych pieniędzy. Nie ulega wątpliwości, iż Internet daje niemal nieograniczone możliwości transferu środków pieniężnych, ukrywania i zatajania nielegalnego pochodzenia mienia. Konwencja nakłada na strony obowiązek wprowadzenia odpowiedniego reżimu prawnego dla banków i innych instytucji finansowych, które mogą być podatne na pranie pieniędzy, w taki sposób, by podmioty te wprowadziły odpowiednie procedury identyfikacji klienta, prowadzenia

[401] M. Siwicki, *Cyberprzestępczość* …, s. 30-31.
[402] Rezolucja dostępna online na oficjalnej stronie internetowej ONZ: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211 [01.07.2015].
[403] M. Siwicki, *Cyberprzestępczość*…, s. 31.
[404] Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r., Dz.U. z 2005 r., Nr 18, poz. 158.

dokumentacji oraz informowania o podejrzanych transakcjach. Państwa-strony konwencji zobowiązały się również do poszerzenia współpracy międzynarodowej, wymiany informacji oraz przeprowadzania szkoleń dla organów ścigania w zakresie inwigilacji elektronicznej, metod wykorzystywanych w zwalczaniu międzynarodowej przestępczości zorganizowanej popełnianej przy wykorzystaniu komputerów, sieci telekomunikacyjnych lub innych form nowoczesnych technologii.

2. Rezolucja Zgromadzenia Ogólnego ONZ z grudnia 1998 roku nr 53/70 dotycząca przestępczości cybernetycznej, cyberterroryzmu i wojen cybernetycznych zatytułowana Rozwój w dziedzinie informacji i telekomunikacji w kontekście międzynarodowego bezpieczeństwa[405]. Wzywa państwa do informowania Sekretariatu Generalnego o rezultatach i ocenach obserwacji w następujących zakresach: bezpieczeństwa informacji, określenia standardów bezpieczeństwa i opracowania zasad na poziomie międzynarodowym mających na celu wzmocnienie światowego systemu informacji, telekomunikacji i zwalczania przestępczości oraz terroryzmu[406].

3. Rezolucja Zgromadzenia Ogólnego ONZ nr 16/2 dotycząca skutecznego zapobiegania i ścigania seksualnego wykorzystania małoletnich[407]. Odniesiono się do w niej problemu dziecięcej pornografii, również w kontekście przepisów i instrumentów zawartych w Konwencji o cyberprzestępczości. Rezolucja zachęca państwa członkowskie do podjęcia odpowiednich kroków prawnych w prawodawstwie krajowym w celu zapobiegania wykorzystania mass mediów, technologii informacyjnych, w tym Internetu, do seksualnego wykorzystania małoletnich. W tym celu państwa powinny między innymi nawiązać współpracę z dostawcami usług sieciowych, którzy winni informować organy sprawiedliwości o podejrzeniu udostępniania pornografii dziecięcej.

4. Rezolucja Rady Gospodarczej i Społecznej ONZ nr 2004/26 w sprawie międzynarodowej współpracy w celu zapobiegania, dochodzenia, ścigania i karania

[405] Ang. *Developments in the Field of Information and Telecommunication in the Context of International Security.*
[406] B. Hołyst, *Terroryzm,* t. 1, Warszawa 2011, s. 963.
[407] CCRCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Dokument dostępny na oficjalnej stronie internetowej UNODC: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2007/CCPCJ/Resolution_16-2.pdf [01.07.2015].

oszustw, nadużyć i fałszerstwa tożsamości i związanych z tym przestępstw[408]. Zwrócono w niej uwagę, że postęp technologii komunikacyjnych stworzył liczne, nowe możliwości oszustw i nadużyć w sprawach karnych, czyli kradzieży tożsamości czy też prania brudnych pieniędzy.

5. Rezolucja Rady Gospodarczej i Społecznej ONZ w sprawie współpracy międzynarodowej w zakresie zapobiegania dochodzenia, ścigania i karania oszustw ekonomicznych i przestępstw związanych z tożsamością[409]. Odnosi się nie tylko do tradycyjnej formy przestępstw, ale również tych związanych z oszustwami i fałszerstwami komputerowymi oraz innych form cyberprzestępczości, która może przyczynić się do popełnienia oszustw gospodarczych, kradzieży tożsamości, prania brudnych pieniędzy czy też innych pokrewnych bezprawnych działań w sieci. Dokument zachęca państwa, które tego jeszcze nie uczyniły, do związania się postanowieniami Konwencji o cyberprzestępczości, ale również innymi międzynarodowymi instrumentami prawnymi, które mogą wspomóc walkę z oszustwami ekonomicznymi oraz przestępstwami związanymi z tożsamością.

W swojej praktyce legislacyjnej wobec cyberprzestrzeni Organizacja Narodów Zjednoczonych nie ogranicza się jedynie do podejmowania tematów związanych z problemem cyberprzestępczości. Akty stanowione ONZ odnoszą się również do innych form działalności człowieka w cyberprzestrzeni. Wśród aktów prawnych o szczególnym znaczeniu wymienić należy zwłaszcza Konwencję Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów, sporządzoną w Wiedniu 11 kwietnia 1980 roku.

Konwencja wiedeńska z dnia 11 kwietnia 1980 roku weszła w życie 1 stycznia 1988 roku, a w chwili obecnej jej stroną jest 85 państw, w tym Polska[410]. Celem konwencji wyrażonym w art. 2 było wprowadzenie nowoczesnego, jednolitego i sprawiedliwego systemu międzynarodowej sprzedaży towarów i tym samym wprowadzenie pewności

[408] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. Dokument dostępny na na oficjalnej stronie internetowej ONZ: http://www.un.org/en/ecosoc/docs/2004/resolution%202004-26.pdf [01.07.2015].
[409] ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identityrelated crime. Dokument dostępny na oficjalnej stronie internetowej ONZ: http://www.un.org/en/ecosoc/docs/2007/resolution%202007-20.pdf [01.07.2015].
[410] Dane z oficjalnej strony internetowej UNCITRAL: http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG_status.html [30.05.2016].

wymiany handlowej i zmniejszenie kosztów transakcyjnych. Ma zastosowanie ona do sprzedaży towarów między stronami mającymi siedziby handlowe w różnych państwach (art. 3). Konwencja w art. 4 wyłącza jej stosowanie w odniesieniu do sprzedaży towarów zakupionych do użytku osobistego, rodzinnego lub do użytku w gospodarstwie domowym oraz w stosunku do sprzedaży w drodze licytacji, egzekucji, sprzedaży energii elektrycznej, okrętów statków oraz udziałów, akcji, papierów wartościowych, tytułów inwestycyjnych i pieniędzy. Konwencji nie stosuje się również do umów o świadczenie usług.

3.1.1.2. Dorobek Biura Narodów Zjednoczonych do spraw Narkotyków i Przestępczości

Biuro Narodów Zjednoczonych do spraw Narkotyków i Przestępczości (ang. *United Nations Office on Drugs and Crimne*, UNODC) jest główną instytucją światową powołaną do walki z przestępczością międzynarodową, nielegalnym handlem narkotykami oraz terroryzmem. UNODC wspiera państwa członkowskie w efektywniejszym zwalczaniu i zapobieganiu cyberprzestępczości, w tym również przez zapewnienie współpracy na poziomie krajowym i regionalnym. Świadczy również pomoc w reformie wymiaru sprawiedliwości oraz w zwalczaniu międzynarodowej przestępczości zorganizowanej i korupcji[411].

Realizując założenia punktu 42 Deklaracji Salwadorskiej, na mocy rezolucji Zgromadzenia Ogólnego ONZ nr 65/230[412] została powołana grupa ekspercka, która miała za zadanie przeprowadzić dogłębną analizę zagadnienia cyberprzestępczości. Wynikiem prac grupy było przeprowadzenie kompleksowych badań w zakresie cyberprzestępczości. W opublikowanym dokumencie *Comprehensive Study on Cybercrime. UNODC 2013*[413] poruszono osiem zasadniczych kwestii:

- rewolucję w łączności i cyberprzestępczości (ang. *connectivity and cybercrime*),
- globalny obraz cyberprzestrzeni (ang. *the global picture*),

[411] Dane z oficjalnej strony internetowej UNODC: https://www.unodc.org/ [11.06.2015].
[412] Dokument dostępny na oficjalnej stronie internetowej ONZ: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/65/230 [11.06.2015]
[413] Comprehensive Study on Cybercrime. Undoc 2013, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [11.06.2015].

- ustawodawstwa i ramy prawne (ang. *legislation and frameworks*),
- kryminalizację (ang. *criminalization*),
- organy ścigania i dochodzenia (ang. *law enforcement and investigations*),
- dowody elektroniczne i wymiar sprawiedliwości (ang. *electronic evidence and criminal justice*),
- współpracę międzynarodową (ang. *international cooperation*),
- zapobieganie cyberprzestępczości (ang. *cybercrime prevention*)[414].

Raport wskazuje, że już w 2011 roku jedna trzecia populacji globu uzyskała dostęp do Internetu. Ponad 60% wszystkich użytkowników sieci pochodzi z krajów rozwiniętych, a 45% internautów nie ukończyło jeszcze 25 roku życia. Prognozuje się, że do 2017 roku aż 70% populacji światowej będzie miało dostęp do mobilnych usług szerokopasmowych, a do 2020 roku liczba urządzeń elektronicznych podłączonych do sieci będzie sześciokrotnie przewyższała liczbę ludzkości. Tak pojęta globalna rewolucja w zakresie łączności ma znaczący wpływ na problem cyberprzestępczości. Uznano, że przestępczość popełniana w sieci wirtualnej jest problemem, rozwijającym się tak dynamicznie jak Internet[415]. W raporcie uznano, że istnieje zauważalny wzrost poziomu cyberprzestępczości popełnianej przez indywidualne jednostki, ale też przez zorganizowane grupy przestępcze. Szacuje się, że 80% cyberprzestępstw ma związek z przestępczością zorganizowaną lub cybernetycznym czarnym rynkiem, na którym można nabyć dane osobowe w celu przywłaszczenia czyjejś tożsamości, kupić złośliwe oprogramowanie czy też sieć botnetów[416]. Popełnienie części z wymienionych wyżej przestępstw jest łatwiejsze do dokonania w cyberprzestrzeni niż w świecie realnym. Transnarodowy charakter, brak wspólnych definicji i niewystarczające prawodawstwo powoduje realny problem z efektywnym ściganiem i sądzeniem sprawców tych przestępstw[417].

Środki prawne odgrywają zatem kluczową rolę w zapobieganiu i zwalczaniu cyberprzestępczości. Część państw od lat wprowadza zmiany do krajowych porządków prawnych między innymi dzięki współpracy międzynarodowej harmonizują przepisy karne, proceduralne, jurysdykcyjne oraz regulacje dotyczące gromadzenia dowodów elektronicznych. Mniej niż połowa badanych w raporcie państw uznała swoje ustawodawstwo

[414] J. Kosiński, *Paradygmaty …*, s. 219-220.
[415] Comprehensive Study on Cybercrime. Undoc 2013, s. Xvii.
[416] Ibidem, s. XVIII-XVIII.
[417] K. Jaishankar, *Identity related Crime in the Cyberspace: Examining Phishing and its impact*, "International Journal of Cyber Criminology" 2008, t. 2, nr 1, s. 11.

wewnętrzne za wystarczające do efektywnego zwalczania cyberprzestępczości. Zaobserwować również można znaczne różnice wśród badanych regionów. Dwie trzecie państw europejskich uznało, że obowiązujące w ich kraju ramy prawne są wystarczające. Diametralnie inna sytuacja panuje w Afryce, obu Amerykach, Azji i Oceanii, gdzie ponad dwie trzecie krajów uznało swoje przepisy za tylko częściowo lub zupełnie niewystarczające, podkreślając równocześnie, iż istnieje pilna potrzeba wprowadzenia nowych, odpowiednich uregulowań w tym przedmiocie[418].

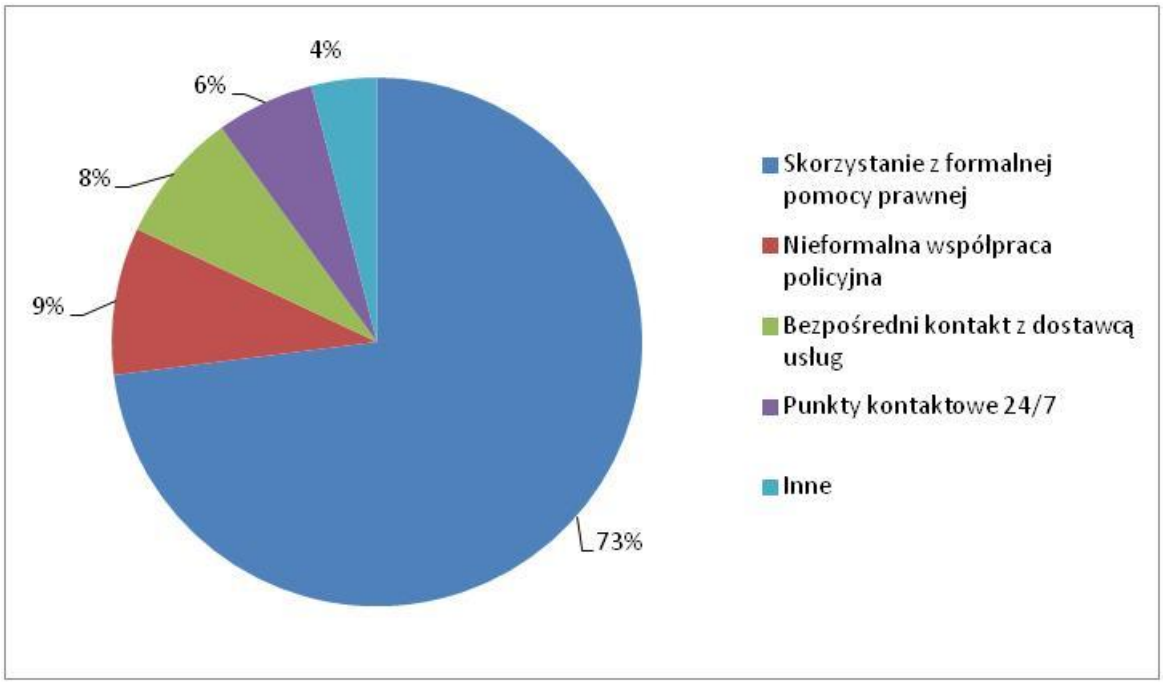
Specjaliści UNODC w swym kompleksowym badaniu nad zjawiskiem przestępczości wskazują na problem przechowywania i gromadzenia dowodów cyfrowych. Dowody takie są często niestabilne i łatwo ulegają zniszczeniu. Badane państwa zgłaszały, że sprawcy często szyfrują podejmowane przez siebie czynności, co powoduje, że uzyskanie dowodów przez organy ścigania jest procesem czasochłonnym, kosztownym i niejednokrotnie bardzo trudnym. Zgłaszanym problemem okazał się również brak odpowiedniego wyszkolenia prokuratorów i sędziów, którzy stykając się z cyberprzestępstwem nie wiedzą, w jaki sposób przeprowadzać postępowanie, w którym część dowodów jest cyfrowa[419]. W związku z występującym problem w 2014 roku UNODC wydało dokument zawierający podstawowe wskazówki dla śledczych i prokuratorów w zakresie żądania przeprowadzenia dowodów elektronicznych w innych państwach[420].

Badane przez UNODC kraje wskazywały, że 30-70% cyberprzestępstw zawierało w sobie element ponadnarodowy, gdzie konieczne było zbadanie jurysdykcji, przeprowadzenie eksterytorialnych dowodów, ekstradycji, udzielenie pomocy prawnej czy podjęcie w inny sposób współpracy międzynarodowej. Ponad 70% krajów korzysta z tradycyjnych form kooperacji międzynarodowej, czyli z pomocy prawnej. Aż w 60% przypadków podstawą takiej pomocy międzynarodowej są umowy bilateralne, a w 20% przypadków - umowy wielostronne[421]. Cyberprzestępcy rzadko działają samotnie, badania pokazują, że są to raczej zorganizowane grupy przestępcze, z szerokimi sieciami i zasobami[422].

---

[418] *Comprehensive Study* ... 2013, s. XVIII.
[419] Ibidem, s. XXIII-XXIV.
[420] Dokument o nazwie *Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions* jest dostępny online na oficjalnej stronie internetowej UNODC: https://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf [10.10.2016].
[421] *Comprehensive Study*..., s. Xxiv.
[422] B. Watkins, *The Impact of Cyber Attacks on the Private Sector*, s. 9, http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf [10.10.2016].

Rysunek 2. Sposoby pozyskiwania dowodów cyfrowych z czynnikiem eksterytorialnym



Źródło: Comprehensive Study…

Zapobieganie cyberprzestępczości w badanych krajach polega w głównej mierze na zmniejszeniu ryzyka występowania cyberprzestępstw oraz łagodzeniu potencjalnych negatywnych skutków. Większość krajów wprowadziła politykę cyberbezpieczeństwa, edukuje pracowników wymiaru sprawiedliwości i internautów oraz dostosowuje legislaturę do międzynarodowych standardów. Przeprowadzane przez UNODC badania mają istotne znaczenie pod względem zrozumienia skali zjawiska cyberprzestępczości oraz jej realnych rozmiarów. Fakt, że od 30 do 70% przestępstw popełnianych w cyberprzestrzeni zawiera element ponadnarodowy w sposób naturalny stawia pytanie o status jurysdykcyjny oraz prawo właściwe.

3.1.1.3 Dorobek Komisji Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego

Brak jest multilateralnej umowy międzynarodowej regulującej holistycznie zagadnienie obrotu gospodarczego w cyberprzestrzeni. Można jednakże wyszczególnić kilka aktów prawnych Organizacji Narodów Zjednoczonych, które mogą mieć zastosowanie do

internetowego obrotu gospodarczego, na przykład Konwencję ONZ o umowach międzynarodowej sprzedaży towarów. Wiele organizacji międzynarodowych pracuje nad problemem umów zawieranych za pośrednictwem cyberprzestrzeni. Największe znaczenie (ze względu na globalny zasięg i nowatorskie podejście) mają prace Komisji Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego (ang. *United Nations Commission on International Trade Law* - UNCITRAL) oraz prace Unii Europejskiej.

Komisja Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego została powołana do życia 17 grudnia 1996 roku uchwałą Zgromadzenia Ogólnego ONZ w celu harmonizacji i usuwania przeszkód w międzynarodowej wymianie handlowej. UNCITRL opracowuje modelowe akty prawne w postaci rekomendacji, konwencji i ustaw, które mogą stać się aktami prawa międzynarodowego[423].

Choć ustawy modelowe UNCITRAL nie są wiążące, niewątpliwie mogą służyć państwom członkowskim oraz organizacjom międzynarodowym jako pewien wzór służący harmonizacji i unifikacji przepisów dotyczących handlu elektronicznego. W modelowej ustawie o handlu elektronicznym po raz pierwszy opisano uznanie ochrony prawnej wiadomości elektronicznej w okresie, gdy w ustawodawstwach krajowych wciąż była wymagana tradycyjna forma pisemna. Ustawa przyznała też taką samą moc prawną czynnościom dokonanych w formie elektronicznej i tradycyjnej[424].

Wśród najważniejszych dokumentów przyjętych pod auspicjami UNICITRAL należy wymienić:

1. **Ustawa modelowa UNCITRAL z 12 czerwca 1996 r. w sprawie handlu elektronicznego (ang. *Model Law on Electronic Commerce*)[425].**

Ustawodawstwo oparte lub przyjęte pod wpływem niewiążącej ustawy modelowej zostało uchwalone w 68 krajach takich, jak Francja, Irlandia, Wielka Brytania czy Arabia

[423] J. Janowski, *Podpis elektroniczny w obrocie prawnym*, Warszawa 2007, s. 89.
[424] K. Kowalik-Bańczyk, *Sposoby regulacji handlu elektronicznego w prawie wspólnotowym i międzynarodowym*, Kraków 2006, s. 122-123.
[425] Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/51/628)] 51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law, New York 1996.

Saudyjska (na liście brak Polski)[426]. Ustawa modelowa może być implementowana do krajowych porządków prawnych w drodze inkorporacji. W założeniu ma stanowić wzorzec dla organów legislacyjnych państw członkowskich ONZ, umożliwiający im wprowadzenie jednolitych przepisów dotyczących elektronicznego przesyłania i wymiany danych.

Dokument zawiera dość ogólne postanowienia mające na celu stworzenie globalnej płaszczyzny rozwoju handlu elektronicznego. Ma ono zostać osiągnięty przez harmonizację krajowych porządków za pomocą wprowadzenia na poziomie międzynarodowym powszechnie akceptowalnego zestawu reguł, który będzie usuwać przeszkody prawne i zwiększy przewidywalność prawną handlu elektronicznego. Ustawa modelowa ma szczególne znacznie, ponieważ była pierwszym dokumentem wprowadzającym fundamentalne zasady niedyskryminacji i neutralności technologicznej. Zasada niedyskryminacji odnosi się do przyznania takich samych skutków prawnych oświadczeniom woli, zawieraniu i wykonywaniu umów, zawieranych w formie tradycyjnej jak i elektronicznej. Zasada neutralności technologicznej nakazuje przyjęcie przepisów neutralnych wobec stosowanej technologii. Twórcy ustawy wyszli z założenia, że wprowadzenie bardzo szczegółowych terminów i definicji jest niekorzystne z powodu szybko postępujących zmian technologicznych, albowiem, pociągające za sobą konieczność częstych nowelizacji[427].

Zakres zastosowania omawianego dokumentu został określony alternatywnie. Artykuł 1 umowy modelowej stanowi, iż stosuje się ją do jakichkolwiek informacji w formie zbioru danych, użytych w zakresie działalności handlowej - wynika z tego, iż umowa znajdzie zastosowanie do obrotu handlowego. Ustawodawca zezwala jednak na ograniczenie jej zastosowania wyłącznie do oświadczeń woli, w szczególności umów zawieranych za pomocą elektronicznie przetwarzanej informacji, odnoszących się do handlu międzynarodowego. Umowa będzie też miała zastosowanie do udzielania i odwoływania pełnomocnictw handlowych[428].

Ustawa modelowa została oparta na zasadzie neutralności technologicznej, niedyskryminacji elektronicznej formy, autonomii stron oraz funkcjonalnej równoważności. Mimo niewiążącej mocy dokument stworzył procedury i zasady, które ułatwiły korzystanie z nowoczesnych technologii. Państwa, które oparły swoje wewnętrzne ustawodawstwo na

[426] Dane z oficjalnej strony internetowej UNCITRAL: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_ commerce/1996Model_status.html [01.03.2017].
[427] A. Stosio, *Umowy zawierane przez Internet*, Warszawa 2002, s. 30-33.
[428] Ibidem, s. 33.

ustawie modelowej musiały jednak we własnym zakresie uregulować kwestie techniczne[429]. Ustawa modelowa została przyjęta pod koniec lat dziewięćdziesiątych XX wieku w okresie, gdy znaczna część przepisów krajowych wymagała do swojej ważności formy pisemnej dokumentu. Wprowadzenie w art. 5 po raz pierwszy zasady prawnego uznawania dokumentów elektronicznych, zgodnie z którym nie można było odmówić skuteczności, ważności i wykonalności dokumentu wyłącznie z powodu jego elektronicznej formy. Podejście to było nowatorskie, w trafny sposób przewidujący przyszłość handlu elektronicznego z coraz większą liczbą transakcji przeprowadzanych w przestrzeni cyfrowej.

2. Ustawa modelowa UNCITRAL o podpisach elektronicznych z 12 grudnia 2001 r. (ang. *Model Law on Electronic Signature*)

Prace nad przygotowaniem ustawy modelowej o podpisach elektronicznych rozpoczęto już w 1996 roku. Początkowo rozważano wprowadzenie szczegółowej regulacji dokładnie określającej wymagania techniczne, które podpis elektroniczny miałby spełniać. W wyniku jednak doświadczeń innych państw, które w latach dziewięćdziesiątych XX wieku wprowadziły przepisy o znacznym stopniu skonkretyzowania technologicznego, odstąpiono od tego pomysłu na rzecz zasady neutralności technologicznej. Ostatecznie Grupa Robocza UNICITRAL do spraw handlu elektronicznego w 2000 roku zakończyła przygotowanie tekstu ustawy modelowej, która została przyjęta w 2001 roku wraz z memorandum wyjaśniającym. Memorandum miało na celu posłużyć za komentarz dla ustawodawców poszczególnych państw chcących wprowadzić tożsame regulacje w krajowych porządkach prawych[430]. Ustawa modelowa nie ma mocy wiążącej, stanowi wyłącznie projekt, dzięki któremu państwa mogą wprowadzić do swojego porządku prawnego minimalne standardy dotyczące podpisów elektronicznych[431]. Przepisy ustawy modelowej o podpisach elektronicznych mają za zadanie harmonizację i unifikację międzynarodowego prawa handlowego, w szczególności przepisów dotyczących podpisów elektronicznych opartych na zasadach technologicznej neutralności.

W doktrynie wskazuje się, że: „Intencją UNICITRAL było przestrzeganie zasady neutralności medialnej oraz technologicznej. Neutralność medialna polega na tym, że

[429] M. Maciejewska-Szałas, *Forma pisemna i elektroniczna czynności prawnych. Studium prawnoporównawcze*, Warszawa 2014, s. 19.
[430] A. Stosio, op. cit., s. 167.
[431] M. Maciejewska-Szałas, *Forma …*, s. 28.

wszystkie nośniki informacji muszą mieć równy status prawny, jeżeli są funkcjonalnymi odpowiednikami. Podkreśla ona konieczność zrównania „papierowego" obrotu prawnego z obrotem dokonującym się za pomocą elektronicznych nośników informacji. Zasada neutralności technologicznej odnosi się natomiast do metod podpisywania dokumentów i nakazuje nie faworyzować żadnej techniki elektronicznych podpisów (oraz każe zrównywać podpisy własnoręczne z elektronicznymi). Zasada ta odnosi się też do przyszłych technologii, które mogą również gwarantować bezpieczeństwo obrotu"[432]. Zaaprobować należy wyrażony pogląd, ponieważ wprowadza on pewność obrotu prawnego w szybko zmieniającym się świecie nowych technologii.

Ustawa modelowa zawiera dość krótki, sześciopunktowy katalog definicji zawarty w art. 2. Za podpis elektroniczny uznano dane w formie elektronicznej dołączone lub logicznie powiązane z przekazem danych, które mogą być użyte do identyfikacji podpisującego w związku z przekazem danych oraz do oznaczenia aprobaty informacji zawartych przekazie danych. W kolejnych punktach są definicje certyfikatu, przekazu danych, podpisującego, podmiotu usług certyfikujących oraz podmiotu podlegającego.

Artykuł 5 ustawy odzwierciedla podstawową zasadę swobody umów i autonomii stron. Zgodnie z postanowieniami tego przepisu wymogi określone w ustawie mogą być uchylone lub zmienione w drodze umowy, chyba że umowa nie byłaby prawnie obowiązująca lub skuteczna pod rządami stosowanego prawa. Jest to najistotniejszy przepis ustawy wprowadzający pierwszeństwo zasady swobody kontraktowania przed postanowieniami ustawy UNCITRAL[433]. Wynika on z możliwości szerokiego zastosowania ustawy, również w odniesieniu do środowisk zamkniętych. Z dokumentów Komisji wynika, że przepisy dotyczące podpisów elektronicznych winne być odpowiednio stosowane do tak zwanych środowisk otwartych (ang. *open environments*) oraz środowisk zamkniętych (ang. *closed environments*). Środowiska otwarte to na przykład sieci komputerowe, które umożliwiają użytkownikom wymianę informacji bez konieczności uprzedniego wyrażenia zgody na przestrzeganie z góry określonych zasad - takim środowiskiem jest na przykład Internet. Termin środowiska zamknięte odnosi się do sieci zazwyczaj używanych w obrocie profesjonalnym, gdzie obowiązują z góry ustalone reguły[434].

[432] A. Stosio, op. cit., s. 168.
[433] M. Świerczyński, *Podpis elektroniczny*, [w:] P. Podrecki, *Prawo Internetu*, Warszawa 2007, s. 72.
[434] A. Stosio, op. cit., s. 168.

Artykułem 6 ust. 1 ustawy wprowadzono przepis, że przypadkach, w których prawo wymaga podpisu osoby, wymaganie to jest spełnione dla przekazu danych, jeśli użyty podpis elektroniczny jest godny zaufania, jako odpowiedni do celu, dla którego przekaz danych został stworzony lub przekazany, w świetle wszystkich okoliczności, włączając w to jakiekolwiek stosowne porozumienie stron. Podkreśla się, że: „zasada ta miałaby zastosowanie zarówno w sytuacji, gdy prawo pozytywnie wymaga złożenia podpisu, jak i w sytuacji, gdy ustawa określa skutki braku podpisu. Złożenie podpisu odpowiadającego tym wymaganiom nie może zostać „zignorowane" i uznane za nie wywołujące skutków prawnych"[435]. Przyjęcie na podstawie zasad niedyskrymianacji szerokiego określenia podpisu elektronicznego zasługuje na aprobatę, podkreślić jednak należy, że nie wyłącza ona zastosowania innych postanowień zgodnie z autonomią stron[436]. Zaakcentować należy, że już obecnie podpis taki może zostać złożony nie tylko w formie elektronicznego podpisu kwalifikowanego odpowiednim certyfikatem, ale również w prostszych formach, na przykład przez złożenie podpisu cyfrowym piórem na tablecie (rozwiązanie to jest powszechnie stosowane w firmach kurierskich czy przy doręczaniu korespondencji sądowej w Polsce).

Kolejne postanowienia umowy modelowej (art. 6 ust. 3) stanowią, że podpis elektroniczny jest uznany za odpowiedni i wystarczająco niezawodny w świetle celu, w jaki zbiór danych został stworzony, jeżeli:

- dane niezbędne do stworzenia podpisu elektronicznego są, w kontekście w jakim są one używane, powiązane wyłącznie z podpisującym,
- dane niezbędne do stworzenia podpisu elektronicznego były w momencie jego zastosowania pod wyłączną kontrolą podpisującego,
- jakakolwiek zmiana w podpisie elektronicznym uczyniona po momencie zastosowania podpisu jest możliwa do wykrycia,
- jeżeli celem prawnych wymogów dla podpisu elektronicznego jest gwarancja integralności informacji, do której dany podpis sie odnosi, jakakolwiek zmiana dokonana na tej informacji po momencie zastosowania podpisu jest możliwa do wykrycia.

W artykule 7 wprowadzono możliwość potwierdzenia przez upoważniony podmiot (organ - urząd publiczny, prywatny określony jako właściwy), który podpis elektroniczny spełnia wymagania określone w art. 6 ustawy. Kolejne trzy artykuły wprowadzają obowiązki

[435] A. Stosio, op. cit., s. 169.
[436] M. Maciejewska-Szałas, *Forma …*, s. 29.

ciążące na podpisującym, świadczącym usługi certyfikacyjne oraz podmiocie podlegającym. Artykuły 9 i 10 nakładają szereg wymagań na podmioty świadczące usługi certyfikacyjne. Artykuł 11 reguluje obowiązki podmiotu podlegającego. Artykuł 12 wprowadza przepisy dotyczące uznawania zagranicznych certyfikatów i podpisów elektronicznych[437].

3. Konwencja Organizacji Narodów Zjednoczonych z 23 listopada 2005 r. o korzystaniu z komunikacji elektronicznej w kontraktach międzynarodowych (ang. *United Nations Convention on the Use of Electronic Communications in International Contracts*)

Konwencja o korzystaniu z komunikacji elektronicznej w kontaktach międzynarodowych z dnia 23 listopada 2005 r., weszła w życie 1 marca 2013 roku. Konwencja została podpisana przez 20 państw, z czego w siedmiu z nich[438] weszła w życie[439]. Na liście państw, które podpisały umowę międzynarodową brak jest europejskich krajów, co wydaje się być spowodowane szerokim dorobkiem UE w zakresie regulowanym omawianą konwencją. Konwencja ma na celu ułatwienie korzystania z komunikacji elektronicznej w handlu międzynarodowym przez zapewnienie, by wymieniane komunikaty i zawierane elektronicznie umowy były ważne i skuteczne, tak jak ich tradycyjne odpowiedniki w formie papierowej. Celami dodatkowymi są harmonizacja przepisów i ułatwienie korzystania z komunikacji elektronicznej w handlu międzynarodowym (ust. 4 preambuły). Podkreślić należy, że konwencja nie zawiera zbyt wielu przepisów prawa materialnego regulującego kwestię zawierania umów w cyberprzestrzeni oraz praw i obowiązków stron. Większość przepisów ma charakter norm interpretacyjnych[440].

Konwencja z 2005 roku ma zastosowanie do wykorzystywania komunikacji elektronicznej w związku z zawarciem lub wykonaniem umowy między stronami posiadającymi siedziby handlowe w różnych państwach. Definicja zawarta w art. 4(c) wskazuje, że konwencja będzie miała zastosowanie nie tylko do umów zawieranych przez Internet. Przesyłanie danych może nastąpić za pomocą środków elektronicznych, magnetycznych, optycznych lub podobnych, takich jak systemy Elektronicznej Wymiany

[437] A. Stosio, op. cit., s. 170-171.
[438] Kongo, Dominikana, Honduras, Czarnogóra, Rosja, Singapur, Sri Lanka.
[439] Dane z oficjalnej strony internetowej UNCITRAL: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html [30.05.2016].
[440] P.P. Polański, *Wprowadzenie do konwencji ONZ o kontraktach elektronicznych*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych*, Warszawa 2008, s. 407.

Danych (EDI), poczta elektroniczna, telegram, teleks lub telefaks. Równie szeroki zakres interpretacyjny pozostawiono pojęciu zawieraniu i wykonywaniu umów. Według art. 4(2) za komunikat uważane jest jakiekolwiek twierdzenie, deklaracja, żądanie, zawiadomienie czy też prośba, wliczając ofertę i przyjęcie oferty w związku z zawarciem albo wykonaniem umowy[441].

Istotne jest, by strony miały siedziby handlowe w różnych państwach w czasie zawarcia kontraktu. Późniejsza zmiana siedziby nie ma znaczenia dla wykonania umowy. W art. 4 wprowadzono definicję siedziby handlowej, za którą uznano jakiekolwiek miejsce, gdzie strona utrzymuje stałą infrastrukturę dla prowadzenia działalności gospodarczej, z wyłączeniem działalności polegającej na tymczasowym dostarczaniu towarów lub usług z określonego miejsca. Postanowienia art. 6 stanowią, że strona wskazuje swoją siedzibę handlową, chyba że druga strona wykaże, że tak nie jest. W sytuacji, gdy siedziba nie została wskazana lub też strona posiada więcej niż jedną siedzibę handlową, za siedzibę handlową uważa się tę, która ma najściślejszy związek z umową ze względu na okoliczności znane stronom lub rozważane przez nie w jakimkolwiek czasie przed zawarciem lub w chwili zawarcia umowy. Jeżeli nie da się ustalić siedziby w przedstawiony sposób za siedzibę strony uważa się miejsce jej stałego zamieszkania. Co istotne, nie można ustalić siedziby handlowej posiłkując się tylko miejscem, w którym znajduje się sprzęt i system informatyczny wykorzystywany przez stronę w związku z zawarciem umowy oraz miejscem w którym strony mogą uzyskać dostęp do tego systemu. Obalone zostało również domniemanie posiadania siedziby handlowej w kraju, w którym strona wykorzystuje krajową domenę czy adres poczty elektronicznej. Znawcy doktryny wskazują, iż nie można wysnuć takiego domniemania również w odniesieniu do domen regionalnych, na przykład domeny „eu”[442].

Omawiana umowa międzynarodowa odnosi się wyłącznie do umów zawieranych pomiędzy profesjonalistami; art. 2 wyłącza zastosowanie konwencji do umów zawartych dla celów osobistych, rodzinnych i do użytku w gospodarstwie domowym. Wyłączeniu na mocy podlegają również transakcje międzybankowe, giełdowe, wynikające z obrotu papierami wartościowymi oraz wekslami.

Konwencja w art. 8 zapewnia umowom zawieranym w postaci elektronicznej taką samą ważność i skuteczność jak w przypadku umów tradycyjnych. Przepis ten jest realizacją

[441] Ibidem, s. 408.
[442] D. Szostek, M. Świerczyński, *Wybór prawa właściwego dla zobowiązań z umów elektronicznych zawieranych w postaci elektronicznej,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego” 2007, z. 100, s. 494.

fundamentalnej zasady prawa Internetu - technologicznej neutralności i niedyskryminacji, która została wcześniej wyrażona w art. 5 modelowej ustawy UNCITRAL o handlu elektronicznym z 1996 roku[443]. Konwencja określa wymagania odnośnie formy zawarcia umowy, podpisu, komunikacji elektronicznej oraz elektronicznych metod uwierzytelniania (art. 9). Brak jest obowiązku zachowania lub utrwalania komunikatu lub umowy w określonej formie dla celów dowodowych.

Podobnie w art. 10 został określony czas oraz miejsce wysłania oraz doręczenia elektronicznych komunikatów. Moment wysłania komunikatu elektronicznego będzie zależał od tego, czy mamy do czynienia z jednym czy z kilkoma systemami informatycznymi. Gdy przedsiębiorcy posługują się dwoma różnymi systemami uznaje się, że komunikat został wysłany w momencie opuszczenia systemu informatycznego znajdującego się pod kontrolą wysyłającego. W przypadku posługiwania się tym samym systemem informatycznym - wysłanie komunikatu następuje w momencie otrzymania wiadomości przez adresata. Artykuł 10 ust 2. Konwencji za moment doręczenia wyznacza chwilę, w której adresat będzie mógł odebrać komunikat pod wskazanym przez niego elektronicznym adresem[444].

Artykuł 11 reguluje kwestię zaproszenia do składania ofert. Przyjęto, że propozycję zawarcia umowy złożona nieokreślonemu kręgowi adresatów za pomocą jednego lub więcej elektronicznych komunikatów, ogólnie dostępnych dla osób korzystających z systemów informacyjnych, włączając w to propozycje wykorzystujące interaktywne aplikacje do składania zamówień za pomocą takich systemów, należy traktować jako zaproszenie do składania ofert, chyba że jasno wskazuje ona na zamiar składającego do bycia związanym swoją propozycją w przypadku jej przyjęcia (stanowczy zamiar zawarcia umowy). Przemysław P. Polański, komentując omawianą regulację, twierdzi, że: „twórcy konwencji nie zauważyli, iż dzisiejsze sklepy internetowe oraz aukcje elektroniczne wymagają uprzedniej rejestracji, której skutkiem jest kierowanie oferty do konkretnego, indywidualnie oznaczonego adresata”[445].

Dość ciekawy zapis wprowadzony został art. 14 dotyczącym błędu w komunikacji elektronicznej. Stanowi on, że jeżeli osoba fizyczna popełni błąd przy wprowadzaniu danych do automatycznego systemu informacyjnego drugiej strony, a system ten nie umożliwi jej poprawienia tego błędu, osoba ta, bądź jej pełnomocnik, ma prawo odwołania wadliwego

[443] P.P. Polański, *Wprowadzenie …*, s. 410-411.
[444] Ibidem, s. 416-417.
[445] P.P. Polański, *Wprowadzenie …*, s. 418-419.

fragmentu elektronicznego komunikatu. Odwołanie komunikatu może nastąpić pod jednym z dwóch warunków. Po pierwsze, osoba ta lub osoba, którą reprezentowała, w najkrótszym możliwym czasie od chwili, w którym dowiedziała się o wystąpieniu błędu powiadomi o nim drugą stronę i zaznaczy, że go popełniła. Po drugie, warunkiem jest też okoliczność, że osoba ta lub osoba, którą reprezentowała nie skorzystała bądź nie odniosła żadnych materialnych korzyści z towarów lub usług dostarczonych przez drugą stronę.

Konwencja zawiera dość ogólne uregulowania, co spowodowane jest jej międzynarodowym charakterem. Postanowienia omawianej umowy międzynarodowej „znajdują zastosowanie do zawarcia lub wykonania umowy w związku z wykorzystaniem i posługiwaniem się środkami komunikacji elektronicznej, do których stosuje się postanowienia konwencji międzynarodowych[446]. W ten sposób regulacje konwencji UNCITRAL stają się niejako nadrzędne w stosunku do w stosunku do konwencji wyżej wymienionych, i to wyłącznie w związku z faktem zawarcia umowy w postaci elektronicznej. W konsekwencji do dwóch identycznych umów, ale zawartych w różny sposób, zastosowanie mogą mieć różne przepisy"[447].

Zgodzić należy się z tezą Przemysława P. Polańskiego, który stwierdza, że: „choć omawiana konwencja nie stanowi szczytowego osiągnięcia w dziedzinie regulacji handlu elektronicznego, mimo wszystko jest ona jednak istotnym krokiem naprzód w tym obszarze. Przede wszystkim modernizuje język starszych konwencji, dzięki czemu bez wątpienia przyczynia się do wzrostu pewności prawnej w odniesieniu do obrotu gospodarczego.[448]" podobnie Natalia Błażiwska stwierdza, że konwencja UNCITRAL jest „nadbudową nad już istniejącym międzynarodowym mechanizmem prawnym regulowania międzynarodowych umów handlowych"[449]. Autorka podnosi, że konwencja nie wprowadza żadnych innowacyjnych regulacji, lecz może przyczynić się do ujednolicenia i uzupełnienia

[446] Konwencja o uznawaniu i wykonywaniu zagranicznych orzeczeń arbitrażowych (Nowy York, 10 czerwca 1958 r.); Konwencja o przedawnieniu międzynarodowej sprzedaży towarów (Nowy York, 14 czerwca 1974r.) wraz z protokołem do niej (Wiedeń, 11 kwietnia 1980 r.); Konwencja Organizacji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów (Wiedeń, 11 kwietnia 1980 r.); Konwencja Organizacji Narodów Zjednoczonych o odpowiedzialności operatorów terminali transportowych w handlu międzynarodowym (Wiedeń, 19 kwietnia 1991 r.); Konwencja Organizacji Narodów Zjednoczonych w sprawie gwarancji bankowych płatnych na żądanie i akredytyw zabezpieczających (Nowy York, 11 grudnia 1995 r.); Konwencja Organizacji Narodów Zjednoczonych o przelewie wierzytelności w handlu międzynarodowym (Nowy York, 12 grudnia 2001 r.).

[447] D. Szostek, M. Świerczyński, *Wybór …*, s. 496.

[448] P.P. Polański, *Wprowadzenie …*, s. 423.

[449] N. Błażiwska, *Konwencja UNICITRAL o wykorzystywaniu komunikacji elektronicznej w kontraktach międzynarodowych a ustawodawstwo ukraińskie*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych*, Warszawa 2008, s. 122.

standardów w przedmiocie zawierania międzynarodowych umów w formie elektronicznej[450]. Konwencja z całą pewnością porusza ważne zagadnienia, regulując kwestię określenia siedziby przedsiębiorcy, możliwości wycofania się z transakcji czy skorygowania błędu.

3.1.1.4. Dorobek Forum Zarządzania Internetem

Rozważania na temat Forum Zarządzania Internetem (ang. *Internet Governance Forum* - IGF) należy rozpocząć od Światowego Szczytu Społeczeństwa Informacyjnego (ang. *The World Summit on the Information Society* - WSIS), który pierwotnie odbył się jako konferencja sponsorowana przez Organizację Narodów Zjednoczonych, na której poruszono problemy informacji, komunikacji oraz ogólnie rozumianego społeczeństwa informacyjnego. Pierwsza konferencja odbyła się w 2003 roku w Genewie, a kolejna w 2005 roku w Tunisie. Jednym z głównych celów WSIS było zlikwidowanie cyfrowej przepaści dzielącej kraje biedne i bogate. Miał on być zrealizowany za pomocą rozpowszechniania dostępu do Internetu w krajach rozwijających się. Zgromadzenie Ogólne Narodów Zjednoczonych uchwałą 56/183 zatwierdziło zorganizowanie Światowego Szczytu Społeczeństwa Informacyjnego 21 grudnia 2001 roku w celu omówienia możliwości i wyzwań społeczeństwa informacyjnego.

Podczas pierwszego szczytu w Genewie wzięło w nim udział 175 delegatów oraz przyjęto Deklarację Zasad oraz Plan Działania, która ma prowadzić do rozwoju społeczeństwa informacyjnego dostępnego dla wszystkich i opartego na wspólnej wiedzy. Podczas Szczytu w 2003 roku nie zdołano wypracować porozumienia w kwestii zarządzania Internetem, wobec czego powołano Grupę Roboczą do spraw Zarządzania Internetem (ang. *The Working Group on Internet Governance* - WGIG) mającą na celu opracowanie strategii w tym przedmiocie. Z kolei w trakcie Światowego Szczytu Społeczeństwa Informacyjnego w Tunisie w 2005 roku poruszono kwestię finansowania i zarządzania Internetem. Ponadto, powołano Forum Zarządzania Internetem (ang. *The Internet Governance Forum*). Od 2006 roku Forum WSIS odbywa się w Genewie po Światowego Dania Społeczeństwa Informacyjnego (17 maja) i jest współorganizowane przez organizacje takie, jak: ITU, UNSESCO, UNPAD oraz UNCTAD. Ostatnio odbyło się również spotkanie WSIS+10 High

[450] Ibidem, s. 122.

Level Event 2010 Światowy Szczyt Społeczeństwa Informacyjnego, będące rozszerzoną wersją Forum WSIS. W trakcie spotkania oceniono dotychczasowy stopień wdrażania społeczeństwa informacyjnego wskazując jednocześnie na nowe cele[451].

Forum Zarządzania Internetem to forum wielostronnego dialogu na temat kluczowych kwestii zarządzania Internetem takich, jak trwałość, stabilność, bezpieczeństwo i niezakłócony rozwój sieci. Sekretarz Generalny ONZ oficjalnie ogłosił utworzenie IGF w lipcu 2006 roku, a pierwsze spotkanie odbyło się zaledwie po kilku miesiącach na przełomie października i listopada 2006 roku. Celem IGF jest maksymalizacja szans na otwarty dialog i wymianę poglądów na temat zarządzania Internetem i najistotniejszych kwestii z tym związanych. W Forum biorą udział organizacje i podmioty indywidualne z różnych obszarów geograficznych i dziedzin specjalności, podmioty akredytowane przy Światowym Szczycie Społeczeństwa Informacyjnego, jak również innych instytucjach, ale również osoby z udokumentowanym doświadczeniem i wiedzą fachową w sprawach związanych z zarządzaniem Internetem.

Podczas kolejnych spotkań Forum Zarządzania Internetem poruszano następujące kwestie:

1. 2006 Ateny (Grecja) - ustalono merytoryczny zakres pracy IGF oraz aspekty jego funkcjonowania W spotkaniu wzięło udział ponad 1500 ekspertów zarówno z krajów rozwiniętych, jak i krajów rozwijających się. W kolejnych latach liczba ta stopniowo zwiększała się. Spotkanie odbyło się pod nazwą „Zarządzenie Internetem dla rozwoju", obradowano w obszarze pięciu grup tematycznych:
    a. otwartość - wolność słowa, wolność przepływu informacji, wiedzy i pomysłów,
    b. bezpieczeństwo - tworzenie zaufania przez współpracę,
    c. różnorodność - promowanie wielojęzyczności i treści lokalnych,
    d. dostęp - łączność internatowa, polityka i koszty,
    e. pojawiające się problemy z budowaniem potencjału, jako priorytet przekrojowy[452].

[451] Dane z oficjalnej strony WSIS http://www.itu.int/net/wsis/index.html [11.09.2016].
[452] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/cms/documents/igf-meeting/igf-2006-athens/128-igf-2006-summary-final/file: [10.10.2016].

2. 2007 Rio de Janeiro (Brazylia) - podobnie jak w 2006 roku tematem głównym było „Zarządzenie Internetem dla rozwoju". W trakcie pięciu sesji tematycznych poruszano problemy: krytycznych zasobów Internetu, dostępności, różnorodności, otwartości oraz bezpieczeństwa[453].
3. 2008 Hyderabad (Indie) spotkanie odbyło się pod hasłem „Internet dla wszystkich". Głównymi tematami poszczególnych sesji były kwestie związane z lawinowym wzrostem liczby internautów, zarządzeniem krytycznymi zasobami Internetu, promowaniem bezpieczeństwa cybernetycznego i zaufania oraz nowymi problemami - Internetem jutra[454].
4. 2009 Sharm El Sheikh (Egipt) - głównym tematem było „Zarządzanie Internetem tworzenie możliwości dla wszystkich". Oprócz tematów poruszanych na wcześniejszych spotkaniach, czyli zarządzania krytycznymi zasobami Internetu czy też kwestii bezpieczeństwa, otwartości i prywatności sieci poruszono nowy, dopiero narastający problem - wpływu sieci społecznościowych na Internet oraz kwestii zarządzania cyberprzestrzenią w świetle zasad Światowego Szczytu Społeczeństwa Informacyjnego[455].
5. 2010 Wilno (Litwa) - głównym tematem spotkania było „Kształtowanie wspólnej przyszłości", a tematami pobocznymi: zarządzenie Internetem na rzecz rozwoju, kwestia chmury komputerowej, ale również poruszane wcześniej kwestie, otwartości, prywatności, dostępu i różnorodności w sieci wirtualnej[456].
6. 2011 Nairobi (Kenia) - uczestnicy forum obradowali nad tematem „Internet jako katalizator zmian: dostępu, rozwoju, wolności i innowacji", poruszając również kwestie opracowywane co roku (bezpieczeństwo, dostępność)[457].
7. 2012 Baku (Azerbejdżan) - tematem spotkania było: „Zarządzanie Internetem na rzecz zrównoważonego rozwoju gospodarczego, społecznego i ludzkiego". Spotkanie zostało zorganizowane wokół tradycyjnych sześciu tematów:

[453] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/cms/documents/igf-meeting/igf-2007-rio/129-igf-2007-chairman-summary-final-16-11-2007/file [10.10.2016].
[454] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/cms/hydera/Chairman%27s%20Summary.10.12.2.pdf [10.10.2016].
[455] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/cms/documents/igf-meeting/igf-2009-sharm-el-sheikh/165-chairman-summary-2009/file [10.10.2016].
[456] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://intgovforum.org/cms/2010/The.2010.Chairman's.Summary.pdf [10.10.2016].
[457] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/cms/2011/IGF.2011.%20Chair's%20Summary%20copy.pdf [10.10.2016 r.].

a. zarządzania Internetem na rzecz rozwoju,
b. zidentyfikowania problemów,
c. zarządzania krytycznymi zasobami Internetu,
d. bezpieczeństwem, otwartością i prywatnością,
e. dostępem i różnorodnością,
f. podsumowaniem obrad i omówieniem perspektywy[458].

8. 2013 Bali (Indonezja) - główny temat spotkania określony został jako „Budowanie mostów - wzmocnienie współpracy wielostronnej na rzecz wzrostu gospodarczego i zrównoważonego rozwoju". Omawiano szczegółowo sześć grup tematycznych:
   a. dostęp i różnorodność - Internet, jako motor wzrostu gospodarczego i zrównoważonego rozwoju,
   b. otwartość - prawa człowieka, wolność wypowiedzi i swobodny przepływ informacji w Internecie,
   c. bezpieczeństwo - ramy prawne: spam, włamania i cyber-przestępczość,
   d. ściślejsza współpraca międzynarodowa,
   e. zasady współpracy wielostronnej,
   f. zasady zarządzania Internetem.

   Coraz częściej zauważano problemy związane z naruszeniem bezpieczeństwa i nadzorem rządowym w przestrzeni wirtualnej. Szczególnie burzliwą dyskusję wśród uczestników spotkania wzbudziła kwestia konieczności zapewnienia lepszej ochrony wszystkich obywateli w środowisku *on-line* oraz zapewnienia odpowiedniej równowagi pomiędzy działaniami związanymi z krajowym cyberbezpieczeństwem i szacunkiem dla uznanych międzynarodowo praw człowieka takich, jak prawo do prywatności i wolności wypowiedzi[459].
9. 2014 Istambuł (Turcja) - głównym tematem spotkania było: "Łączenie kontynentów dla ściślejszej wielopodmiotowej współpracy nad zarządzaniem Internetem". Dyskusję prowadzono w ośmiu grupach tematycznych:
   a. zasady umożliwiające dostęp,
   b. tworzenie treści, rozpowszechnianie i wykorzystywanie,
   c. Internet jako motor wzrostu i rozwoju,
   d. Forum Zarządzania Internetem i przyszłość „ekosystemu Internetu",

[458] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/cms/2012/Book/Chairs.Summary.IGF.2012.pdf [10.10.2016].
[459] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/multilingual/content/igf-2013 [10.10.2016].

e. wzmacnianie cyfrowego zaufania,
f. Internet a prawa człowieka,
g. krytyczne zasoby Internetu,
h. pojawiające się problemy[460].

10. 2015 Joao Pessoa (Brazylia) - dziesiąte spotkanie odbyło się pod hasłem „Ewolucja zarządzania Internetem. Wzmocnienie zrównoważonego rozwoju". Wśród nowych tematów pojawiły się takie kwestie, jak ekonomia Internetu (ang. *Internet Economy*) oraz wzmacnianie współpracy wielostronnej[461].

Finalny wynik spotkań w ramach Forum Zarządzania Internetem nie jest jeszcze znany i dostatecznie klarowny, ale sama forma IGF i jej organizacja jest nowym modelem tworzenia wspólnej polityki na poziomie międzynarodowym. Mimo, że Forum odbywa się już od dziesięciu lat, trudno jest jednoznacznie stwierdzić, w jaki sposób problemy poruszane na IGF zostaną rozwiązane. Być może z Forum Zarządzania Internetem wyewoluuje zupełnie nowy organ, bądź dalsze prace zostaną przekształcone w kodeks najlepszych praktyk. Możliwe jest również, że państwa zrezygnują ze ścisłej regulacji cyberprzestrzeni w imię wolnościowych idei Internetu. Nie ulega wątpliwości, że żaden podmiot czy też pojedynczy kraj nie jest w stanie sam rozwiązać wyzwań związanych z cyberprzestrzenią i jej zastosowaniem. Internet jest bez wątpienia przestrzenią polityczną, w której państwa muszą zaakceptować swoją współzależność i współodpowiedzialność[462].

Część podmiotów biorąca udział w Forum wyrażała niezadowolenie, że IGF nie ma zdolności podejmowania decyzji merytorycznych. Brak formalizacji w tym stopniu był jednak warunkiem części rządów do przyjęcia zasady otwartości i równego statusu wszystkich uczestników, co więcej tak przyjęta organizacja IGF ma najbardziej otwartą strukturę ze wszystkich podmiotów powiązanych z ONZ. Mimo pozornie prostej formuły Forum Zarządzania Internetem jest międzynarodową przestrzenią komunikacji i wymiany poglądów przedstawicieli rządów, ale również zainteresowanych obywateli, w zakresie polityki publicznej odnoszącej się do cyberprzestrzeni. Nie mniej ważna jest możliwość debaty o najistotniejszych problemach - wolności wypowiedzi, ochrony prywatności czy prawa w odniesieniu do portali społecznościowych.

[460] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/multilingual/content/igf-2014-4 [10.10.2016].
[461] Dane z oficjalnej stronty internetowej Forum Zarządzania Internetem. Więcej informacji na: http://www.intgovforum.org/cms/10th%20IGF%20Chairs%20Summary_Finalv2.pdf [10.10.2016].
[462] J. Kulesza, *Międzynarodowe* …, s. 328-330.

3.1.1.5. Dorobek Światowej Organizacji Własności Intelektualnej

Światowa Organizacja Własności Intelektualnej (ang. *World Intellectual Property Organization* - WIPO) jest jedną z wyspecjalizowanych agencji ONZ zajmującą się koordynacją i tworzeniem regulacji dotyczących systemu ochrony własności intelektualnej. Organizacja powstała w latach siedemdziesiątych jednakże boom technologiczny związany z rozwojem techniki komputerowej oraz pojawieniem się cyberprzestrzeni zrodził potrzebę wypracowania nowych międzynarodowych norm, odpowiadających eksploatacji utworów w przestrzeni wirtualnej. W Genewie 20 grudnia 1996 roku uchwalono pod auspicjami WIPO dwie międzynarodowe konwencje nazywane czasami „internetowymi" traktatami WIPO. Są nimi:

Traktat WIPO o prawie autorskim (ang. *WIPO Copyright Treaty* - WCT)

Traktat Światowej Organizacji Własności Intelektualnej o Prawie Autorskim, sporządzony w Genewie dnia 20 grudnia 1996 roku[463] odwołuje się bezpośrednio do konwencji berneńskiej[464], wprowadza jednak przepisy mające zastosowanie również do cyberprzestrzeni. Przede wszystkim omawiana umowa międzynarodowa przyznaje ochronę programom komputerowym na równi z utworami literackimi, niezależnie od sposobu lub formy ich wyrażania. Podstawową funkcją tej regulacji było założenie, że programy komputerowe należy traktować tak samo jak utwory literackie i artystyczne (poprzednio nie były one bezpośrednio wymienione w katalogu ochrony). Omawiany art. 4 spełnia więc dwojaką funkcję. Po pierwsze identyfikuje programy komputerowe jako dzieła spełniające wymogi ochrony przyznanej przez konwencję berneńską, a po drugie uznaje je za dzieła literackie i tym samym determinuje najszerszy zakres ochrony[465]. W art. 5 traktatu WIPO ochronę przyznano również zbiorowi danych lub innych materiałów, które ze względu na dobór lub układ treści stanowią wytwory intelektu. Przepis ten przyznaje szerszą ochronę niż

[463] Dz.U. z 2005 r., Nr 3, poz. 12.
[464] Konwencja berneńska o ochronie dzieł literackich i artystycznych z dnia 9 września 1886 r. (obecnie obowiązujący tekst – Akt paryski Konwencji berneńskiej o ochronie dzieł literackich i artystycznych sporządzony w Paryżu dnia 24 lipca 1971 r.), Dz.U. z 1990 r., Nr 82, poz. 474.
[465] M. Huczkowski, *Ochrona autorskich praw osobistych w powszechnym prawie międzynarodowym*, Warszawa 2013, s. 243 -244.

konwencja berneńska, ponieważ za „dane" uznaje elementy, które nie stanowią utworów literackich w rozumieniu konwencji berneńskiej, lecz są to dane możliwe do wyodrębnienia, czyli informacje biologiczne, geograficzne, historyczne, fakty, liczby, imiona czy adresy internetowe. Z kolei za „inne materiały" rozumie się zarówno utwory objęte przez Konwencję berneńską, jak i inne rezultaty wkładu intelektualnego, który nie jest pojmowany jako utwór[466].

Traktat WIPO o prawach autorskich reguluje i uzupełnia przepisy konwencji berneńskiej w zakresie autorskich praw majątkowych, czyli przez przepisy dotyczące prawa wprowadzenia do obrotu (art. 6), prawa najmu (art. 7) oraz prawa publicznego komunikowania (art. 8). W traktacie znalazły się postanowienia dotyczące czasu trwania ochrony utworów fotograficznych (art. 9), ograniczeń i wyjątków od praw ochronnych przyznanych autorom (art. 10), zapewnieniu odpowiednich środków technicznych związanych z wykonywaniem traktatu (art. 11), przyjęto też zobowiązania dotyczące elektronicznego zarządzania prawami autorskimi (art. 12) oraz dochodzenia i egzekwowania praw wynikających z traktatu (art. 14).

Janusz Barta i Ryszard Markiewicz zaakcentowali, że w omawianym akcie prawnym po raz pierwszy w międzynarodowych konwencjach prawo do dystrybucji objęło wszystkie rodzaje utworów oraz pozwoliło na wprowadzenie w państwach stronach umowy międzynarodowego wyczerpania prawa autorskiego. Podnoszą oni, że „postanowienie w sprawie art. 6 zawarte w tzw. uzgodnionych ustaleniach do WCT przesądza o tym, że wyczerpanie prawa może odnosić się wyłącznie do materialnych kopii dzieła. Chodzi tu zatem o wyraźną eliminację możliwości konstruowania wyczerpania prawa w odniesieniu do eksploatacji utworu w Internecie (...). Niewątpliwe podstawowe znaczenie WCT wyraża się objęciem wyłącznym prawem do publicznego rozpowszechniania utworów, także udostępniania ich w ten sposób, że osoby posiadają dostęp do tych dzieł z miejsc i w czasie indywidualnym przez siebie wybranym. Wkroczeniem w to prawo jest działanie umożliwiające osobom trzecim dostęp do utworu[467]. W ten sposób przesądzono, że przekaz w sieci komputerowej „na życzenie" objęty jest konwencyjnym minimum ochrony.

[466] J. Reinbothe, M. Prat, S. von Lewinski, *The New WIPO Treaties: A first Résumé,* "EIPR" 1997, nr 7, s. 74-75.
[467] A nie samo zapewnienie dostępu do serwera, łączy komunikacyjnych lub urządzeń przekazujących sygnały.

Naruszeniem prawa autorskiego jest przy tym już samo umożliwienie dostępu do utworu w opisany sposób"[468].

Szczególną uwagę należy zwrócić na postanowienia zakazujące usuwania środków technicznych przeznaczonych do ochrony praw przewidzianych w konwencji berneńskiej i traktacie WIPO o prawie autorskim, czyli środków uniemożliwiających kopiowanie utworów. W trakcie prac nad traktatem przepis ten budził kontrowersję, dlatego zdecydowano się pozostawić państwom znaczną swobodę w przedmiocie określenia środków technicznych objętych ochroną, katalogu zakazanych działań oraz sankcji za ich naruszenie. Innowacyjnym rozwiązaniem było również wprowadzenie nakazu ochrony przed usuwaniem lub zmianą informacji przeznaczonych do elektronicznego zarządzania prawami autorskimi. Przepis ten został przyjęty z powodu coraz większego rozpowszechniania utworów w sieciach wirtualnych[469].

Traktat WIPO o artystycznych wykonaniach i fonogramach (ang. *WIPO Performances and Phonograms Treaty* - WPPT)

Traktat WIPO o artystycznych wykonaniach i fonogramach, sporządzony w Genewie 20 grudnia 1996 roku[470] udziela ochrony artystom, wykonawcom i producentom będącym obywatelami państw - stron traktatu. WPPT przyjmuje zasadę traktowania krajowego, ale wyłącznie w zakresie regulacji w nim objętych oraz z zapewnieniem odpowiedniego wynagrodzenia. Rozdział II Traktatu WIPO o artystycznych wykonaniach i fonogramach (art. 1-10) porusza kwestię prawa artystów i wykonawców - praw osobistych, praw majątkowych. Artykuł 7 przewiduje, iż wyłącznie artystom przysługuje prawo zezwalania na bezpośrednie lub pośrednie zwielokrotnianie ich artystycznych wykonań, w jakikolwiek sposób i w jakiejkolwiek formie - w tym za pośrednictwem przestrzeni wirtualnej. Zgodnie z postanowieniami traktatu artystom wykonawcom przysługuje wyłączne prawo zezwalania na publiczne udostępnianie swoich utworów drogą przewodową i bezprzewodową, w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym.

[468] J. Barta, R. Markiewicz, *Prawo autorskie*, Warszawa 2016, s. 577.
[469] Ibidem, s. 578.
[470] Dz. U. z 2004 r., Nr 41, poz. 375.

Podobne prawa zostały też przyznane producentom fonogramów (w art. 11-14) - mają oni wyłączne prawo do zezwalania na pośrednie oraz bezpośrednie zwielokrotnienie wyprodukowanych utworów, prawo wprowadzania ich do obrotu, prawo najmu oraz publicznego ich udostępniania.

3.1.1.6 Dorobek Międzynarodowego Związku Telekomunikacyjnego

Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union*, ITU), z siedzibą w Genewie, jest jedną z organizacji wyspecjalizowanych ONZ działających w celu standaryzowania i regulowania rynku telekomunikacyjnego i radiokomunikacyjnego. Podkreślić należy, że ITU to jedyna organizacja międzynarodowa działająca pod auspicjami ONZ, która opiera się na szczególnym rodzaju partnerstwa publiczno - prywatnego. W skład ITU wchodzi 198 państw i około 700 członków powiązanych z przemysłem, głównie łączności elektronicznej[471]. Międzynarodowa Unia Telekomunikacji przyczyniła się do standaryzacji kryminalizacji cyberprzestępstw, ale również do kształtowania reguł handlu elektronicznego. ITU była organizatorem Światowego Szczytu dotyczącego Społeczeństwa Informacyjnego.

17 maja 2007 roku sekretarz generalny ITU, na skutek inicjatyw zapoczątkowanych w czasie konferencji WSIS[472], utworzył Globalną Agendę Cyberbezpieczeństwa (ang. *Global Cybersecurity Agenda*, GCA), która za pomocą dialogu i współpracy międzynarodowej ma zamiar zwiększyć zaufanie i bezpieczeństwo w społeczeństwie informacyjnym. Siedzibą GCA jest siedziba organizacji IMPACT (ang. *International Multilateral Partnership Against Cyber Threats*), która jest organem wykonawczym ITU[473].

Globalna Agenda Cyberbezpieczeństwa opiera się na pięciu strategicznych filarach, nazywanych również obszarami roboczymi. Zaliczyć do nich należy: środki prawne (ang. *legal measures*), środki techniczne i proceduralne (ang. *technical and procedural measures*),

[471] K. Kowalik-Bańczyk, op. cit., s. 128.
[472] M. Siwicki, *Cyberprzestępczość* …, s. 33.
[473] Dane z oficjalnej strony internetowej ITU http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx [10.06.2015].

struktury organizacyjne (ang. *organizational structures*), budowanie potencjału (ang. *capacity building*) oraz współpracę międzynarodową (ang. *international cooperation*)[474].

Głównym celem strategicznym dla środków prawnych jest opracowanie strategii rozwoju modelu prawodawstwa związanego z cyberprzestępczością. Miałby on posłużyć harmonizacji istniejących już norm prawnych na poziomie krajowym, jak i regionalnym oraz międzynarodowym. Do realizacji tego celu w październiku 2007 roku powołano Grupę Ekspertów Wysokiego Poziomu (ang. *High -Level Expert Group*, HLEG), w której skład wchodzą przedstawiciele państw członkowskich, nauki i przemysłu[475]. Działania HLEG obejmują doradzanie Sekretarzowi Generalnemu ONZ w kwestii cyberbezpieczeństwa oraz przygotowywania długoterminowych strategii cyberbezpieczeństwa w pięciu kluczowych obszarach roboczych. HLEG analizuje bieżące wydarzenia w sieci, monitoruje i wykrywa zagrożenia, mogące zaburzyć bezpieczeństwo sieci[476].

Drugi filar strategiczny - środki techniczne i proceduralne - koncentrują się na kluczowych wyzwaniach technicznych wynikających z cyberbezpieczeństwa. Sprawcy cyberprzestępstw wciąż poszukują luk w aplikacjach i oprogramowaniu w celu uzyskania nieautoryzowanego dostępu oraz naruszenia integralności, autentyczności i poufności systemów informatycznych i komunikacyjnych. Wraz ze wzrostem złożoności złośliwego oprogramowania, możliwych zagrożeń nie należy bagatelizować, ponieważ może to mieć tragiczne konsekwencje w przypadku ataku na urządzenia teleinformatycznej infrastruktury krytycznej. Działania GCA koncentrują się na rozwoju standardów dotyczących środków technicznych i proceduralnych zwalczających zagrożenia bezpieczeństwa w tym przedmiocie[477].

Obszar roboczy struktury organizacyjnej jest związany monitorowaniem i zapobieganiem cyberatakom. Zdolność państw do efektywnego radzenia sobie z zagrożeniami w dużej mierze zależy od szybkości reakcji, ostrzegania i posiadanych procedur. Obszar ten koncentruje się na wypracowaniu optymalnych strategii reagowania i instytucji, które mogą

[474] J. Kosiński, *Paradygmaty …*, s. 217-218.
[475] Ibidem, s. 218.
[476] ITU Global CybersecurityAgenda (GCA) High - Level Experts Group (HLEG) Report of the Chairman of HLEG, http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf [01.07.2015].
[477] Filar strategiczny „środki techniczne i proceduralne" GCA - http://groups.itu.int/cybersecurity-gateway/WorkAreas/TechnicalandProceduralMeasures.aspx [01.07.2015].

pomóc krajom w zarządzaniu kryzysowym w przypadku ataków, czy też w ochronie infrastruktury krytycznej[478].

Z kolei budowanie potencjału ma na celu zbudowanie zrównoważonej kultury cyberbezpieczeństwa. Podniesienie świadomości użytkowników sieci jest niezbędne do zrozumienia i zapobieżenia potencjalnym zagrożeniom. Tworzone przez GCA programy mają na celu edukowanie społeczeństwa, rządów i przemysłu, a w konsekwencji pełne wdrożenie kultury cyberbezpieczeństwa[479].

Ostatnim filarem strategicznym jest współpraca międzynarodowa, ponieważ państwa w żaden sposób nie są w stanie zamknąć wirtualnych granic tak, by uniknąć wszelkich cyberzagrożeń. Cyberbezpieczeństwo przestrzeni wirtualnej nie jest problemem tylko krajowym czy regionalnym. Należy je rozpatrywać w kryteriach międzynarodowych, dlatego też konieczna jest harmonizacja i współpraca zarówno na szczeblu rządowym, ale też w kooperacji z przemysłem, organizacjami międzynarodowymi i pozarządowymi. GCA stara się wykorzystać instrumenty współpracy wielostronnej w celu osiągnięcia globalnej strategii zwiększenia cyberbezpieczeństwa[480].

W ramach ITU działa też Sektor Rozwoju Telekomunikacji (ang. *Telecommunication Development Sector,* TDS), który zajmuje się opracowywaniem projektów istotnych z perspektywy zwalczania cyberprzestępczości. Do poruszonych przez TDS problemów zaliczyć można:

- problemy polityki legislacyjnej wraz z propozycjami możliwych zmian w ustawodawstwach państw członkowskich - *ITU Toolkit for Cybercrime Legislation,*
- analizę społecznych zagrożeń w zakresie przestępczości komputerowej oraz sposobach uświadamiania użytkowników o potencjalnych zagrożeń - *Understanding Cybercrime Guide,*
- opracowania związane z zapobieganiem cyberprzestępczości - *ITU National Cybersecurity/ CIIP, Self - Assessment Tool oraz ITU Botnet Mitigation Toolkit*[481].

[478] Filar strategiczny „struktura organizacyjna" GCA - http://groups.itu.int/cybersecurity-gateway/WorkAreas/OrganizationalStructures.aspx [01.07.2015].
[479] Budowanie potencjału GCA - http://groups.itu.int/cybersecurity-gateway/WorkAreas/CapacityBuilding.aspx [01.07.2015].
[480] Filar strategiczny „współpraca międzynarodowa" GCA - http://groups.itu.int/cybersecurity-gateway/WorkAreas/InternationalCooperation.aspx [01.07.2015].
[481] M. Siwicki, *Cyberprzestępczość* …, s. 33.

3.1.2. Regulacje wypracowane w systemach organizacji regionalnych

W niniejszym podrozdziale omówiony zostanie dorobek prawny wypracowany w systemach organizacji regionalnych: Rady Europy oraz Unii Europejskiej. Organizacje te zrzeszające kraje wysoko rozwinięte już w latach dziewięćdziesiątych XX wieku zauważyły naglącą potrzebę wprowadzenia odpowiednich regulacji prawnych odnoszących się do cyberprzestrzeni. Ustanowione przez nich rozwiązania legislacyjne kreują zupełnie nowe i innowacyjne rozwiązania systemowe. Akty prawne i dokumenty organizacji międzynarodowych były nie tylko podstawą do harmonizacji rozwiązań przyjętych w państwach członkowskich organizacji, ale również inspiracją do podjęcia działań legislacyjnych w innych regionach świata.

3.1.2.1. Dorobek Rady Europy

Opublikowany w 1985 roku raport OECD Przestępstwa związane z komputerem: Analiza polityki legislacyjnej spowodował, że Rada Europy rozpoczęła własny program badawczy nad zjawiskiem przestępczości popełnianej przy użyciu systemów komputerowych. W ramach programu powołano 15-osobowy Komitet Ekspertów, który miał za zadanie opracowanie dyrektyw, dzięki którym organy ustawodawcze państw członkowskich mogłyby wprowadzić do krajowych porządków prawnych minimalny katalog cyberprzestępstw, które winny być karane. Wynikiem prac Komitetu Ekspertów było przedstawienie Europejskiemu Komitetowi Problemów Przestępczości w 1989 roku raportu i projektu zalecenia, który został następnie przyjęty jako Zalecenie nr R(89)9[482].

Komitet Ekspertów Rady Europy poszerzył listę przestępstw przedstawionych w raporcie OECD. Cyberprzestępstwa podzielono na dwie listy - minimalną i fakultatywną. Lista minimalna zawierała czyny, które winny były być uznane za przestępstwo we wszystkich państwach członkowskich Rady Europy. Stwierdzono, że przestępstwa te cechują

[482] A. Adamski, *Prawo …*, s. 6.

się znaczną szkodliwością oraz transgranicznym charakterem, wobec czego istnieje potrzeba ich unifikacji. Na liście znalazło się 8 rodzajów nadużyć komputerowych:

- oszustwo związane z wykorzystaniem komputera,
- fałszerstwo komputerowe,
- uszkodzenie danych lub programów komputerowych,
- sabotaż komputerowy,
- uzyskanie nieuprawnionego dostępu do systemu komputerowego,
- podsłuch komputerowy,
- bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych,
- bezprawne kopiowanie topografii półprzewodników[483].

Z kolei, lista fakultatywna zawierała czyny o mniejszym stopniu szkodliwości, niewywołujące znacznych implikacji na poziomie międzynarodowym. W ocenie twórców raportu podejmowanie skoordynowanych działań w walce z tego typu cyberprzestępcami można było pozostawić w gestii państw członkowskich. Na decyzję miał również wpływ fakt, że przedstawiciele państw członkowskich nie byli w stanie osiągnąć konsensusu w zakresie konieczności penalizacji czynów z listy fakultatywnej, stąd też taka decyzja końcowa[484]. Na liście tej znalazły się cztery typy zachowań:

- modyfikowanie danych lub programów komputerowych,
- szpiegostwo komputerowe,
- używanie komputera bez zezwolenia,
- używanie prawnie chronionego programu komputerowego bez upoważnienia[485].

Państwa członkowskie w większości zaimplementowały chociażby część Zalecenia nr R (89)9 wprowadzając standardy penalizacji czynów głównie z listy minimalnej. Działania te, chodź istotne, były jedynie przyczynkiem do dalszych działań Rady Europy w zakresie zwalczania cyberprzestępczości. Znawcy doktryny wysoko ocenili rolę zalecenia nr R (89)9 w zakresie harmonizacji prawa karnego państw członkowskich Rady Europy.

[483] Ibidem, s. 7.
[484] F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 160.
[485] A. Adamski, *Prawo …*, s. 7.

Kolejnym zaleceniem o istotnym znaczeniu prawym było Zalecenie R (95)13 z dnia 11 września 1995 r. w sprawie zagadnień procesowych związanych z technologią informacyjną. Wydanie tego aktu było konsekwencją problemów faktycznych, jakie napotkały państwa członkowskie na płaszczyźnie gromadzenia dowodów elektronicznych w tradycyjnie rozumianym procesie karnym[486].

Komitet Ministrów w 1997 roku w czasie spotkania Delegatów Ministrów powołał nowy komitet o nazwie Komitet Ekspertów w sprawie przestępczości w cyberprzestrzeni (*The Committee of Experts on Crime in Cyber-space*, PC-CY). Komitet rozpoczął w kwietniu 1997 roku prace nad przygotowaniem projektu Konwencji Rady Europy o cyberprzestępczości. Przez 13 lat, do 2000 roku odbywały się konsultacje i spotkania w celu ustalenia ostatecznego kształtu konwencji. Projekt prezentowany był w ponad 150 krajach. Efektem tych prac było przyjęcie w 2001 roku projektu Konwencji RE o cyberprzestępczości[487].

Konwencja o cyberprzestępczości

Najistotniejszym aktem prawnym o charakterze międzynarodowym odnoszącym się do zagadnienia przestępczości popełnianej przy użyciu systemów komputerowych jest Konwencja o cyberprzestępczości (Konwencja lub Konwencja o cyberprzestępczości)[488], zawarta w Budapeszcie 23 listopada 2001 roku. Konwencja weszła w życie 1 lipca 2004 roku, jako pierwsza umowa międzynarodowa, która podjęła temat przestępstw popełnianych przy użyciu sieci komputerowych. Ponadto, Konwencja zawiera Protokół dodatkowy dotyczący kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych - akt ten będzie szerzej omówiony w dalszej części pracy.

Konwencja o cyberprzestępczości została podpisana przez czterdzieści pięć państw członkowskich Rady Europy (tabela 8). Do tej pory jedynie Rosja i San Marino wstrzymały się od przystąpienia do omawianej umowy międzynarodowej.

[486] A. Lach, *Przestępczość komputerowa*, [w:] A. Grzelak (red.), *Europejskie prawo karne*, Warszawa 2012, s. 261-262.
[487] M. Siwicki, *Cyberprzestępczość* …, s. 35.
[488] Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. Dz. U. z 2014 r., poz 1514.

Tabela 8. Liczba państw członkowskich Rady Europy związanych Konwencją o cyberprzestępczości

Lp.	Państwo	Podpisanie	Ratyfikacja	Wejście w życie	Zastrzeżenia	Deklaracje	Władze	Terytorialny zakres stosowania
1.	Albania	23/11/2001	20/6/2002	1/7/2004			X	
2.	Andora	23/4/2013						
3.	Armenia	23/11/2001	12/10/2006	1/2/2007			X	
4.	Austria	23/11/2001	13/6/2012	1/10/2012	X	X	X	
5.	Azerbejdżan	30/6/2008	15/3/2010	1/7/2010	X	X	X	X
6.	Belgia	23/11/2001	20/8/2012	1/12/2012	X	X	X	
7.	Bośnia i Hercegowina	9/2/2005	19/5/2006	1/9/2006			X	
8.	Bułgaria	23/11/2001	7/4/2005	1/8/2005	X	X	X	
9.	Chorwacja	23/11/2001	17/10/2002	1/7/2004			X	
10.	Cypr	23/11/2001	19/1/2005	1/5/2005			X	
11.	Czechy	9/2/2005	22/8/2013	1/12/2013	X	X	X	
12.	Dania	22/4/2003	21/6/2005	1/10/2005	X		X	X
13.	Estonia	23/11/2001	12/5/2003	1/7/2004			X	
14.	Finlandia	23/11/2001	24/5/2007	1/9/2007	X	X	X	
15.	Francja	23/11/2001	10/1/2006	1/5/2006	X	X	X	
16.	Grecja	23/11/2001						
17.	Gruzja	1/4/2008	6/6/2012	1/10/2012		X		
18.	Holandia	23/11/2001	16/11/2006	1/3/2007			X	X
19.	Hiszpania	23/11/2001	3/6/2010	1/10/2010		X	X	
20.	Irlandia	28/2/2002						
21.	Islandia	30/11/2001	29/1/2007	1/5/2007	X		X	
22.	Lichtenstein	17/11/2008	21/1/2016	1/5/2016	X	X	X	

23.	Litwa	23/6/2003	18/3/2004	1/7/2004	X	X	X	
24.	Łotwa	5/5/2004	14/2/2007	1/6/2007	X		X	
25.	Luksemburg	28/1/2003	16/10/2014	1/2/2015			X	
26.	Macedonia	23/11/2001	15/9/2004	1/1/2005			X	
27.	Malta	17/1/2002	12/4/2012	1/8/2012		X		
28.	Monako	2/5/2013						
29.	Mołdawia	23/11/2001	12/5/2009	1/9/2009		X	X	X
30.	Montenegro	7/4/2005	3/3/2010	1/7/2010	X		X	
31.	Niemcy	23/11/2001	9/3/2009	1/7/2009	X	X	X	
32.	Norwegia	23/11/2001	30/6/2006	1/10/2006	X	X	X	
33.	Polska	23/11/2001	20/2/2015	1/6/2015	X		X	
34.	Portugalia	23/11/2001	24/3/2010	1/7/2010		X	X	
35.	Rumunia	23/11/2001	12/5/2004	1/9/2004			X	
36.	Rosja							
37.	San Marino							
38.	Serbia	7/4/2005	14/4/2009	1/8/2009			X	
39.	Słowacja	4/2/2005	8/1/2008	1/5/2008	X	X	X	
40.	Słowenia	24/7/2002	8/9/2004	1/1/2005			X	
41.	Szwajcaria	23/11/2001	21/9/2011	1/1/2012	X	X	X	
42.	Szwecja	23/11/2001						
43.	Turcja	10/11/2010	29/9/2014	1/1/2015				
44.	Ukraina	23/11/2001	10/3/2006	1/7/2006	X		X	
45.	Węgry	23/11/2001	4/12/2003	1/7/2004	X	X	X	
46.	Wielka Brytania	23/11/2001	25/5/2011	1/9/2011	X		X	
47.	Włochy	23/11/2001	5/6/2008	1/10/2008			X	

Źródło: dane z oficjalnej strony internetowej Rady Europy http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=13/08/2015&CL=ENG [20.10.2016].

Polska podpisała konwencję 23 listopada 2001 roku, jednak w wyniku opóźnień prac legislacyjnych jej ratyfikacja i wejście w życie nastąpiło stosunkowo niedawno, czyli 18 października 2014 roku. Ratyfikacja konwencji nie nastąpiła jeszcze w pięciu państwach członkowskich Rady Europy - Andorze, Grecji, Irlandii, Monako i Szwecji.

Konwencja jest wielostronną umową międzynarodową o półotwartym charakterze. W traktacie zawarto klauzulę umożliwiającą przystąpienie do Konwencji państwom trzecim na zaproszenie. Społeczność międzynarodowa zauważyła potrzebę regulacji zagadnienia cyberprzestępczości. Z tych też względów do konwencji o cyberprzestępczości przystąpiły także inne państwa, niebędące państwami członkowskimi Rady Europy, czyli Japonia czy Stany Zjednoczone Ameryki.

Tabela 9. Liczba państw nienależących do Rady Europy związanych Konwencją o cyberprzestępczości

Lp.	Państwo	Podpisanie	Ratyfikacja	Wejście w życie	Zastrzeżenia	Deklaracje	Władze	Terytorialny zakres stosowania
48	Australia		30/11/2012 przystąpienie	1/3/2013	X		X	
49	Izrael		9/6/2016 przystąpienie	1/9/2016	x		x	
50	Japonia	23/11/2001	3/7/2012	1/11/2012	X	X	X	
51	Kanada	23/11/2001	8/7/2015	1/11/2015	X	X	X	
52	Mauritius		15/11/2013 przystąpienie	1/3/2014			X	
53	Panama		5/3/2014 przystąpienie	1/7/2014			X	
54	Republika Dominikany		7/2/2013 przystąpienie	1/6/2013		X	X	
55	RPA	23/11/2001						
56	Sri Lanka		29/5/2015 przystąpienie	1/9/2015	X	X	X	
57	USA	23/11/2001	29/9/2006	1/1/2007	X	X	X	

Źródło: dane z oficjalnej strony internetowej Rady Europy http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=13/08/2015&CL=ENG, [20.10.2016].

Konwencja o cyberprzestępczości jest podpisana na okres bezterminowy z możliwością jej wypowiedzenia w każdym czasie przez skierowanie odpowiedniej noty do Sekretarza Generalnego Rady Europy. Wypowiedzenie umowy jest skuteczne od pierwszego dnia miesiąca następującego po upływie trzymiesięcznego terminu od otrzymania noty.

W ustępie 9 preambuły do umowy międzynarodowej wskazano, że konwencja jest „niezbędna dla powstrzymania działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowemu wykorzystywaniu tych systemów, sieci i danych, poprzez uznanie takiego postępowania za przestępstwo, zgodnie z niniejszą Konwencją, oraz przyjęcia środków, które będą przydatne w skutecznym zwalczaniu takich przestępstw, poprzez ułatwienie ich wykrywania, prowadzenia dochodzenia i ścigania zarówno na szczeblu krajowym, jak i międzynarodowym, oraz poprzez przyjęcie rozwiązań sprzyjających szybkiej i rzetelnej współpracy międzynarodowej". Konwencja o cyberprzestępczości była pierwszą umową międzynarodową, która uregulowała kwestię przestępczości w przestrzeni wirtualnej. Eksperci Rady Europy słusznie zauważyli, iż czyny takie są coraz bardziej popularne, dlatego też konieczna jest międzynarodowa współpraca w celu efektywnego zwalczania, przeciwdziałania zjawisku, w tym przez wymianę doświadczeń oraz unifikację przepisów proceduralnych.

Celem konwencji jest zapewnienie ochrony użytkowników cyberprzestrzeni oraz bezpieczeństwa sieci między innymi przez zwalczanie pornografii dziecięcej oraz treści rasistowskich i ksenofobicznych w Internecie. Omawiana umowa międzynarodowa w znacznym stopniu przyczyniła się do zharmonizowania i ujednolicenia terminologii krajowych, określenia katalogu najpoważniejszych cyberprzestępstw oraz zakreślenia przepisów proceduralnych i jurysdykcyjnych[489].

W rozdziale drugim konwencji o cyberprzestępczości omawiano środki, jakie należy podjąć na szczeblu krajowym. Część I zawiera postanowienia materialnoprawne, penalizujące następujący katalog czynów, podzielonych na cztery kategorie:

[489] R. Tarnogórski, *Konwencja o cyberprzestępczości - międzynarodowa odpowiedź na przestępczość ery informacyjnej*, [w:] M. Madej, M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa Polski*, Warszawa 2009, s. 205-206.

I. Kategoria I - przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów:

1) nielegalny dostęp do systemu informatycznego - rozumiany jako umyślny, bezprawny dostęp do całości lub części systemu informatycznego; stronom konwencji pozostawiono wybór czy wprowadzą do swojego prawa wewnętrznego wymóg, by czyn został uznany za przestępstwo, musi być popełniony przez naruszenie zabezpieczeń z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, ewentualnie za pośrednictwem systemu informatycznego połączonego z innym systemem (art. 2),
2) nielegalne przechwytywanie danych - rozumiane jako, umyślne, bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne; ponownie stronom pozostawiono wybór wprowadzenia nieuczciwego zamiaru lub związku z systemem informatycznym połączonym z innym systemem jako znamiona przestępstwa (art. 3),
3) naruszenie integralności danych - czyli umyślne, bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych (art. 4),
4) naruszenie integralności systemu - rozumiane jako umyślne, bezprawne poważne zakłócenie funkcjonowania systemu informatycznego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych (art. 5),
5) niewłaściwe użycie urządzeń - czyli umyślna i bezprawna produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania programu komputerowego służącego do popełniania przestępstw lub hasła komputerowego, kodu dostępu lub innych danych uprawniających do uzyskania dostępu do systemu informatycznego lub też posiadania tych urządzeń w zamiarze popełnienia przestępstw komputerowych (art. 6).

II. Kategoria II - przestępstwa komputerowe:

6) fałszerstwo komputerowe - umyślne, bezprawne wprowadzenie, dokonywanie zmian, wykasowywanie lub usuwanie danych informatycznych w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub

wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to czy są one możliwe do bezpośredniego odczytania i zrozumiałe; konwencja pozostawia stronom wybór czy do znamion czynu wprowadzić działanie w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze (art. 7),

7) oszustwo komputerowe - czyli umyślne, bezprawne spowodowanie utraty środków finansowych przez inną osobę przez zmianę, wykasowanie lub usunięcie danych informatycznych lub też każdą inną ingerencję w funkcjonowanie systemu komputerowego, jeżeli sprawca działał z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby (art. 8).

III. Kategoria III - przestępstwa ze względu na charakter zawartych informacji:

8) przestępstwa związane z pornografią dziecięcą - artykułem tym spenalizowano produkcję, oferowanie, udostępnianie, rozpowszechnianie lub transmitowanie oraz pozyskiwanie i posiadanie pornografii dziecięcej za pomocą lub w ramach systemu informatycznego (art. 9).

IV. Kategoria IV - przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych:

9) przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych (art. 10) - wynikających z innych międzynarodowych umów międzynarodowych.

Warto podkreślić, że wskazane wyżej przepisy materialnoprawne nie mogą być stosowane bezpośrednio, ponieważ nie są wystarczająco precyzyjne i nie mają charakteru norm samowykonalnych. Podkreśla się jednak, iż przepisy te „mogą być jednak stosowane pośrednio jako wskazówka przy wykładni przepisów prawa krajowego mających dokonać ich transpozycji”[490]. Stanowią one minimalny standard w zakresie penalizacji cyberprzestępstw. Oznacza to, że państwa członkowskie mogą zdecydować się na kryminalizację innych czynów, które w ich ocenie winny podlegać karze.

Artykuł 11 Konwencji stanowi, iż państwa członkowskie winny penalizować nie tylko sprawstwo czynu, lecz również usiłowanie, pomocnictwo oraz podżeganie do jego popełnienia. Kolejne artykuły określają zasady odpowiedzialności osób prawnych (art. 12),

[490] F. Radoniewicz, op. cit., s. 163.

które w czasie opracowywania Konwencji były swoistym *novum*[491] oraz sposoby określenia kar i środków prawnych (art.13). Umowa międzynarodowa nie wskazuje jakie kary i środki karne powinny zostać zastosowane wobec poszczególnych kategorii czynów. Zakres odpowiedzialności został pozostawiony decyzji państw - stron. Zaleca się jednak, by podjęte przez państwa środki prawne były skuteczne, proporcjonalne i zniechęcały do popełnienia czynów, a w przypadku czynów osób prawnych powinny obejmować środki karne, w tym sankcje pieniężne.

W rozdziale drugim części II Konwencji o cyberprzestępczości zawarte zostały przepisy procesowe poruszające kwestię:

- zakresu przepisów procesowych (art. 14),
- niezwłocznego zabezpieczenia przechowywanych danych informatycznych (art. 16),
- niezwłocznego zabezpieczenia i częściowego ujawnienia danych dotyczących ruchu (art. 17),
- nakazu dostarczenia niezbędnych danych i informacji (art. 18),
- przeszukania i zajęcia przechowywanych danych informatycznych (art.19),
- gromadzenia w czasie rzeczywistym danych dotyczących ruchu (art. 20),
- przechowywania danych dotyczących treści (art. 21).

Strony Konwencji postanowiły podjąć międzynarodową współpracę w sprawach karnych w celu ścigania i prowadzenia postępowań związanych z systemami i danymi informatycznymi oraz zbierania dowodów elektronicznych. Przepisy regulujące kwestię ekstradycji, wzajemnej pomocy prawnej, w tym, w zakresie środków tymczasowych i środków śledczych oraz ustanowienia sieci 24/7 wprowadzono, aby osiągnąć te cele. W stosunku do sprawcy występku opisanego w art. 2-11 Konwencji, aby zastosować ekstradycję, konieczne jest występowanie podwójnej karalności czynu w obu zainteresowanych państwach, a przestępstwo winno być zagrożone karą co najmniej jednego roku pozbawienia wolności. Ekstradycja może również nastąpić na mocy innej umowy ekstradycyjnej łączącej państwa, na przykład na mocy Europejskiej konwencji o ekstradycji[492] (art. 24).

[491] Ibidem, s. 162-163.
[492] Europejska konwencja o ekstradycji sporządzona w Paryżu 13 grudnia 1957 r. Dz.U. z 1994 r., Nr. 70, poz. 307.

Istotnym ułatwieniem dla organów sprawiedliwości jest przewidziana w Konwencji pomoc prawna, która obejmuje nie tylko wzajemne udzielanie informacji, pomoc w prowadzeniu czynności śledczych, ale też zabezpieczenie na wniosek jednej ze stron danych przechowywanych w systemie informatycznym znajdującym się na terytorium drugiej strony. Współpraca międzynarodowa dotyczy też udzielania wzajemnej pomocy w stosunku do gromadzenia w czasie rzeczywistym danych dotyczących ruchu i treści oraz ponadgranicznego dostępu do określonej kategorii danych.

Konwencja, w art. 35 nakłada na strony obowiązek ustanowienia punktów kontaktowych 24/7 zapewnić natychmiastową pomoc dla organów sprawiedliwości podejmujących czynności śledcze w odniesieniu do cyberprzestępstw. W realizacji pomocy sieć 24/7, wyposażona w specjalistyczny sprzęt i wyszkolony personel uprawniona jest do:

- zapewnienia doradztwa technicznego,
- zabezpieczenia i ujawniania danych informatycznych,
- gromadzenia dowodów, dostarczania informacji o prawie oraz lokalizowania osób podejrzanych.

Wpływ Konwencji o cyberprzestępczości na unifikację przepisów dotyczących przestępczości komputerowej jest nieoceniony. Jej ogromną zaletą jest możliwość przystąpienia do traktatu państw spoza Rady Europy oraz możliwość stosowania klauzul opcjonalnych[493]. Zgodnie z danymi organizacji *Data Protection and Cybercrime Division*, która działa pod auspicjami Rady Europy, 140 państw z - 193, które są członkami ONZ - wprowadziło do swojego ustawodawstwa krajowego przepisy dotyczące cyberprzestępczości i w 90% wzorowały się na Konwencji o cyberprzestępczości[494].

Podnoszonym w doktrynie problemem jest długotrwały czas ratyfikacji Konwencji. Wielu krajom, w tym Polsce i Niemcom, ratyfikacja zajęła ponad dekadę. Część państw zgłaszało, iż niezasadna jest ratyfikacja całej Konwencji ze względu na jej liczne wady. Z perspektywy czasu postanowienia Konwencji wydają się bardzo ogólne i mało precyzyjne, jednak akt ten stworzył podwaliny ogólnych ram prawnych dotyczących cyberprzestępczości. W doktrynie podnosi się, że Konwencja o cyberprzestępczości nie wskazuje jasno, które

[493] Ibidem, s. 164.
[494] Cooperation against cybercrime: Progress made in 2012 – A brief review of Council of Europe activities, Dokument dostępny online na oficjalnej stronie internetowej Rady Europy http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Docs2013/cyber%20AS%20review2012_flyer_v6.pdf [13.08.2015].

państwo jest właściwe do ścigania przestępstwa, brak jest również definicji miejsca popełnienia przestępstwa, które mogłoby wyjaśnić kompetencje jurysdykcyjne państwa[495]. Skutkiem tych obaw jest niewprowadzanie do krajowych porządków prawnych poszczególnych zapisów prawnych. Na przykład Niemcy postanowiły nie implementować . 2 konwencji, a USA art. 5[496].

Mimo ogromnego wpływu, jaki Konwencja wywarła na harmonizację prawa dotyczącego cyberprzestępczości jej postanowienia w chwili obecnej wydają się być przestrzale i nie do końca odpowiadające nowym technologicznym wyzwaniom. Przedstawiony w Konwencji katalog przestępstw tworzy minimalny standard, jednak zalecane jest, by państwa rozszerzały go o inne cyberprzestępstwa. Długotrwały proces ratyfikacji spowodował częściową dezaktualizację jej postanowień. Wydaje się, że państwa - strony Konwencji przez długi czas nie uważały cyberprzestępczości za realny problem. Dopiero wydarzenia ostatniego dziesięciolecia - cyberataki na Estonię i Gruzję ukazały prawdziwą wagę problemu.

Protokół dodatkowy do Konwencji o cyberprzestępczości dotyczący kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych

Protokół dodatkowy do Konwencji o cyberprzestępczości dotyczący kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych został sporządzony 28 stycznia 2003 roku w Strasburgu. Został przyjęty przez Komitet Ministrów Rady Europy w listopadzie 2002 roku, a w styczniu 2003 roku otwarty do podpisu. Akt prawny wszedł w życie po złożeniu pięciu dokumentów ratyfikacyjnych, co nastąpiło 1 marca 2006 roku. Protokół dodatkowy do tej pory został podpisany przez 42 państwa (w tym przez RPA i Kanadę), z czego 29 zdecydowało się na

[495] J. Kulesza, *Międzynarodowe …*, s. 150.
[496] M. Siwicki, *Cyberprzestępczość* …, s. 36.

jego ratyfikację[497]. Rzeczpospolita Polska podpisała go w 21 lipca 2003 roku, a ratyfikowała razem z Konwencją o cyberprzestępczości.

Powodem sporządzenia protokołu dodatkowego była próba stworzenia jednolitego sytemu prawa międzynarodowego, który mógłby zapewnić odpowiednie środki prawne reagowania na propagandę o charakterze rasistowskim i ksenofobicznym, która jest rozpowszechniania za pomocą przestrzeni cyfrowej. Ma on stanowić równowagę pomiędzy swobodą wyrażania opinii a efektywną walką z atakami o charakterze rasistowskim i ksenofobicznym.

Strony umowy międzynarodowej w art. 1 ust 1 Protokołu dodatkowego uznały za materiały rasistowskie i ksenofobiczne „każdy materiał pisemny, każdy wizerunek lub każde inne wyrażenie myśli lub teorii, które nawołują, popierają lub podżegają do nienawiści, dyskryminacji lub przemocy przeciw jakiejkolwiek osobie lub grupie osób, ze względu na rasę, kolor, pochodzenie narodowe lub etniczne, jak również religię, jeżeli wykorzystywana jest ona jako pretekst dla któregokolwiek z tych czynników[498]". Uznano, że akty o takim charakterze stoją w jawnej sprzeczności z prawami człowieka, a w związku z tym mogą być zagrożeniem dla rządów prawa i demokratycznej stabilności.

Państwa-strony na mocy Protokołu dodatkowego zobowiązały się do penalizacji następującej kategorii czynów:

- rozpowszechniania materiałów o charakterze rasistowskim lub ksenofobicznym w systemie komputerowym - rozumiane jako umyślna i bezprawna dystrybucja lub publiczne udostępnianie materiałów rasistowskich i ksenofobicznych w systemie komputerowym; strony umowy mogą jednak zastrzec, iż nie będą stosować wskazanej wyżej regulacji w swoim prawie krajowym, jeżeli byłoby to sprzeczne z wewnętrznymi przepisami zapewniającymi swobodę wyrażania opinii, bądź jeżeli czyn nawołuje, popiera lub podżega do dyskryminacji, jednakże nie jest ona związana z przemocą lub nienawiścią (art. 3),
- kierowanie gróźb o podłożu rasistowskim lub ksenofobicznym - czyli czyn polegający na grożeniu za pomocą systemu komputerowego popełnieniem poważnego przestępstwa na szkodę określonej osoby lub grupy osób z powodu

[497] Dane z oficjalnej strony Rady Europy: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=&DF=&CL=ENG [17.03.2017].
[498] M. Duda, *Przestępstwa z nienawiści. Studium prawnokarne i kryminologiczne*, s. 115.

jej/ich przynależności do grupy wyodrębnionej ze względu na rasę, kolor, pochodzenie narodowe lub etniczne lub też wyznanie (art. 4),

- publicznego znieważania ze względów rasistowskich lub ksenofobicznych - rozumianego jako publiczna zniewaga popełniona przy użyciu systemu komputerowego przeciwko osobie lub grupie osób z powodu jej przynależności do grupy wyodrębnionej ze względu na rasę, kolor, pochodzenie narodowe lub etniczne lub też wyznanie (art. 5),
- zaprzeczania, poważnego umniejszania znaczenia, akceptacji lub usprawiedliwiania zbrodni ludobójstwa oraz zbrodni przeciwko ludzkości zdefiniowane przez akty prawa międzynarodowego oraz przez wiążące decyzje międzynarodowych sądów karnych (art. 6).

Ponadto, Protokół dodatkowy przewiduje, iż pomocnictwo i podżeganie do popełnienia któregokolwiek z wyżej wymienionych czynów jest również karalne. Czyny o charakterze rasistowskim i ksenofobicznym, niestety, występują coraz częściej w przestrzeni wirtualnej. W ostatnich kilku latach jest widoczna zwiększająca się lawinowo liczba pejoratywnych komentarzy na temat muzułmanów, uchodźców i innych grup społecznych. Negatywne komentarze w cyberprzestrzeni przekładają się na pewną akceptację społeczną, mogącą skutkować eskalacją konfliktu w świecie realnym, wyrażającą się chociażby w napaściach na osoby ciemnoskóre, niszczeniem świątyń czy nawoływaniem do innych zbrodni nienawiści.

Konwencja Rady Europy o ochronie dzieci przed wykorzystaniem seksualnym i niegodziwym traktowaniem w celach seksualnych

Konwencja Rady Europy o ochronie dzieci przed wykorzystaniem seksualnym i niegodziwym traktowaniem w celach seksualnych została sporządzona 25 października 2007 roku w Lanzarote (konwencja z Lanzarote). Akt ten został podpisany przez 47 członków Rady Europy i do tej pory jedynie pięciu z nich (Armenia, Azerbejdżan, Zjednoczone Królestwo, Norwegia oraz Irlandia) nie ratyfikowało jeszcze wskazanej umowy międzynarodowej. Konwencja z Lanzarote weszła w życie 1 lipca 2010 roku po złożeniu dokumentów ratyfikacyjnych przez pięciu sygnatariuszy, w tym trzy państwa członkowskie

Rady Europy[499]. Rzeczpospolita Polska podpisała Konwencję 25 października 2007 roku jednakże jej ratyfikacja nastąpiła dopiero 26 września 2014 roku[500].

Konwencja z Lanzarote została zawarta z uwagi na narastający krajowy i międzynarodowy problem seksualnego wykorzystania i niegodziwego traktowana dzieci między innymi za pomocą technologii informacyjnych i telekomunikacyjnych. Celem traktatu jest podjęcie międzynarodowej i krajowej współpracy w celu zapobiegnięcia zjawisku i ochronie praw dzieci będących ofiarami tego typu przestępstw. Konwencja nakłada na strony obowiązek podjęcia odpowiednich kroków w celu podnoszenia świadomości społeczeństwa i dzieci, odpowiednich służb (wymiar sprawiedliwości, służba zdrowia, edukacja) na temat zagrożeń związanych z seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych małoletnich. Jednym z nałożonych w artykule 13 obowiązków jest uruchomienie specjalnych linii telefonicznych lub internetowych, udzielających osobom dzwoniącym porad przy zachowaniu poufności rozmów i anonimowości dzwoniących.

Rozdział szósty Konwencji z Lanzarote zawiera postanowienia materialnoprawne poruszające między innymi kwestie pornografii dziecięcej pozyskiwanej za pośrednictwem technologii informacyjnych i telekomunikacyjnych (art. 20), rekrutowania dziecka do prostytucji (które może nastąpić za pomocą systemu komputerowego- art. 19) lub udziału w prezentacjach pornograficznych (art. 21) oraz groomingu[*] (art. 23). Państwa-strony Konwencji z Lanzarote zobowiązały się do podjęcia jak najszerszej współpracy międzynarodowej w celu zapobiegania i zwalczania seksualnego wykorzystywania dzieci i niegodziwego traktowania dzieci w celach seksualnych, zapewnienia ochrony i pomocy ofiarom tych przestępstw oraz efektywnego prowadzenia postępowania karnego w tym przedmiocie (art. 38).

Konwencja z Lanzarote zawiera gwarancje ochrony dzieci przed przemocą seksualną zarówno przez normy materialnoprawne (prostytucja, pornografia dziecięca), jak i procesowe (priorytetowe traktowanie, rozpoznanie bez zbędnej zwłoki). W umowach międzynarodowych jest zauważalny pozytywny trend do zwiększenia ochrony karnoprawnej dzieci przez podwyższenie wieku przyzwolenia czy też większej dbałości o pomoc ofiarom

[499] Dane z oficjalnej strony Rady Europy: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=&DF=&CL=ENG [17.03.2017].
[500] Dz.U. 2014, poz. 1623.
[*] Więcej na ten temat w podrozdziale 4.1.4 *Cyberprzestępstwa związane z treścią inforamcji.*

przemocy (na przykład przez pomoc psychologa)[501]. Niestety, cyberprzestrzeń nasila to zjawisko. Dzieci są coraz bardziej narażone na niebezpieczeństwa ze strony pedofili, nakłaniania do prostytucji czy pornografii dziecięcej. Dlatego też pozytywnie należy ocenić zwiększanie międzynarodowej ochrony w tym zakresie, ponieważ tylko ponadnarodowe kroki pozwolą na szeroko zakrojoną i efektywną walkę ze zjawiskiem.

Inne regulacje Rady Europy

Oprócz wskazanych wyżej konwencji, które w sposób bezpośredni odnoszą się do przestępstw popełnianych przy użyciu systemu komputerowego, Rada Europy podejmuje inne inicjatywy pomocne w zwalczaniu cyberprzestępczości. Należy do nich zaliczyć:

1. **Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych**[502] sporządzoną 28 stycznia 1981 roku w Strasburgu, ratyfikowaną przez 50 państw, w tym Polskę[503].

Celem traktatu jest zapewnienie każdej osobie fizycznej poszanowania jej praw i podstawowych wolności, a w szczególności prawa do prywatności w związku z automatycznym przetwarzaniem jej danych osobowych. Cel ten ma być osiągnięty przez zapewnienie odpowiednich procedur bezpieczeństwa gromadzenia i przechowywania danych, również w stosunku do przepływu danych przez granice państwowe.

Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych jest jednym z najstarszych aktów prawnych regulujących tę kwestię. W artykule 2 konwencji za dane osobowe zostały uznane wszelkie informacje dotyczące osoby fizycznej o ustalonej tożsamości albo dającej się zidentyfikować, czyli tak zwane „podmioty danych". Z kolei automatyczne przetwarzanie zostało zdefiniowane jako następujące operacje wykonywane w całości lub części za pomocą metod zautomatyzowanych: rejestrowanie danych, z zastosowaniem do nich operacji logicznych i/albo arytmetycznych, ich

[501] J. Podlewska, O. Trocha, *Ochrona prawna małoletnich - kierunki przemian prawa i postępowania karnego, zagadnienia wybrane*, „Dziecko Krzywdzone" 2012, nr 2(39), s. 148.
[502] Dz. U. z 2003 r., Nr 3, poz. 25.
[503] Informacje na podstawie aktualnych danych zawartych na stronie internetowej Rady Europy https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=atxlX0lJ [17.03.2017].

modyfikowanie, usuwanie, odzyskiwanie lub rozpowszechnianie. Konwencja wprowadza podstawowe zasady ochrony danych osobowych: zgodne z prawem ich pozyskiwanie, gromadzenie dla określonych i usprawiedliwionych celów, niewykorzystywanie danych przeciwko celowi, zgodnie z którym zostały zgromadzone czy też przechowywanie danych tylko przez czas oznaczony, nie dłuższy niż to uzasadnione ze względu na cel, w którym zostały zgromadzone[504].

Artykuł 6 konwencji zakazuje poddawania automatycznemu przetwarzaniu danych osobowych ujawniających pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne oraz danych osobowych dotyczących zdrowia lub życia seksualnego, ale również do danych osobowych dotyczących wyroków karnych skazujących, chyba że prawo krajowe zawiera odpowiednie gwarancje ochrony. Omawiana umowa międzynarodowa nakłada na państwa-strony obowiązek zapewnienia odpowiednich środków bezpieczeństwa w stosunku do danych osobowych zarejestrowanych w zautomatyzowanych zbiorach w celu ich ochrony przed zniszczeniem, przypadkową utratą, a także przed udostępnieniem, zmianą lub rozpowszechnieniem bez zezwolenia. Ponadto, każdej osobie przyznano prawo do ustalenia czy jej dane osobowe znajdują się w automatycznym zbiorze danych, kto nimi administruje, przyznano też prawo do wglądu do własnych danych z możliwością ich sprostowania oraz usunięcia. Dość istotne postanowienia, z punktu widzenia niniejszych rozważań, zostały zawarte w art. 12 konwencji, w którym postanowiono, że z pewnymi wyjątkami, państwa--strony konwencji nie mogą zabronić ani uzależnić od specjalnego zezwolenia, przepływu danych osobowych przez granice na terytorium innych państw pod pretekstem ochrony prywatności[505].

Na podstawie Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych został powołany Komitet Doradczy, który może zgłaszać propozycje mające na celu ułatwienie lub usprawnienie stosowania konwencji, składać wnioski dotyczące nowelizacji oraz wydawać opnie dotyczące stosowania Konwencji. Wskazuje się, że Rada Europy na podstawie omawianej Konwencji wydała liczne rekomendacje dotyczące między innymi autonomicznego przetwarzania danych medycznych, czy też na potrzeby ubezpieczenia społecznego, wykorzystania danych osobowych w projektach i badaniach naukowych. W 1987 roku Komitet Ministrów Rady Europy wydał zalecenie dotyczące ochrony danych osobowych wykorzystywanych przez Policję, w których

[504] G. Michałowska, *Ochrona praw człowieka w Radzie Europy i w Unii Europejskiej*, Warszawa 2007, s. 130.
[505] Konwencja RE o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, art. 6-12.

ogranicza się możliwość zbierania danych osobowych tylko do takich, które są niezbędne do prawidłowego przeprowadzenia postępowania karnego[506].

2. **Komitet do spraw cyberprzestępczości** (ang. *Cybercrime Convention Committee T-CY*)

Członkami komitetu są reprezentanci państw będących stronami Konwencji o cyberprzestępczości. W roli obserwatorów występują przedstawiciele państw, które podpisały lub zostały zaproszone do przystąpienia do Konwencji o cyberprzestępczości oraz przedstawiciele Komisji Unii Afrykańskiej, UE, Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji, Międzynarodowego Związku Telekomunikacyjnego, Interpolu, Europolu, OBWE, UNCOC i Organizacji Państw Amerykańskich. Spotkania konsultacyjne sygnatariuszy Konwencji odbywają się corocznie[507].

Podstawą działania komitetu jest art. 46 Konwencji. Komitet spotyka się w celu skutecznego stosowania i wdrażania Konwencji, w tym identyfikacji problemów powstałych przy jej implementowaniu, ale również wymiany informacji na temat najnowszych zmian legislacyjnych, politycznych, technicznych oraz tych z zakresu zbierania dowodów cyfrowych. Ponadto, Komitet opracowuje i publikuje raporty związane z wdrażaniem i wykonywaniem postanowień konwencji.

3. **Projekt GLACY** (ang. *Global Action on Cybercrime*)

Wspólny projekt Rady Europy realizowany z UE od 1 listopada 2013 roku do 31 października 2016 roku, mający na celu wspieranie krajów na całym świcie w implementacji konwencji o cyberprzestępczości. Szczegółowym celem programu GLACY jest umożliwienie organom wymiaru sprawiedliwości pogłębienia współpracy międzynarodowej w zakresie zwalczania cyberprzestępczości i gromadzenia dowodów elektronicznych. Prace są prowadzone w następujących obszarach: zaangażowania organów rządowych, harmonizacji przepisów, szkolenia kadr organów sprawiedliwości, współpracy międzynarodowej, wymiany informacji i oceny poczynionych postępów[508].

[506] G. Michałowska, *Ochrona* op. cit., s. 131-132.
[507] Dane z oficjalnej strony Rady Europy: http://www.coe.int/t/dghl/coopearation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp [10.08.2015].
[508] Dane z oficjalnej strony internetowej Rady Europy: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/GLACY/GLACY_en.asp [10.08.2015].

4. Project Cybercrime@Octopus

Projekt Rady Europy, który stanowi rozwinięcie projektu *Global Project on Cybercime* i realizowany był od 1 stycznia 2014 roku do 31 grudnia 2016 roku. Opiera się na dobrowolnych składkach, mających na celu pomoc krajom na całym świecie w celu wdrożenia konwencji o cyberprzestępczości, wzmocnienia ochrony danych i ujednolicenia prawa w tym obszarze. Inicjatywa wspiera Komitet do spraw cyberprzestępczości oraz jest ciałem doradczym dla krajów, które są przygotowane do wdrożenia instrumentów prawnych wynikających z Konwencji o cyberprzestępczości[509].

3.1.2.2 Dorobek Unii Europejskiej

Pierwsze próby uregulowania kwestii związanych z cyberprzestrzenią miały miejsce w latach dziewięćdziesiątych XX wieku, jeszcze pod auspicjami Wspólnoty Europejskiej, która zauważyła narastający problem wykorzystania przestrzeni wirtualnej do rozpowszechniania treści zakazanych przez prawo. W kwietniu 1996 roku wezwano Komisję Europejską do opracowania norm prawnych w zakresie przeciwdziałania rozpowszechnianiu nielegalnych i szkodliwych treści w Internecie. W wyniku prac Komisji Europejskiej 16 października 1996 roku przyjęto Komunikat Komisji dla Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno - Społecznego i Regionów na temat nielegalnej i szkodliwej treści w Internecie[510] oraz „Zielony Dokument" dotyczący ochrony małoletnich i poszanowania godności ludzkiej w usługach informacyjnych i audiowizualnych[511]. Dokument zawierał propozycję zmian w celu prewencji rozpowszechniania nielegalnych treści oraz wskazywał na rozbieżności w zakresie penalizacji i definiowania cyberprzestępstw, w szczególności w zakresie przestępstw związanych z pornografią dziecięcą[512].

W kolejnych latach Unia Europejska podejmowała coraz śmielsze kroki w zakresie proponowanych rozwiązań legislacyjnych. Prawodawstwo i dokumenty unijne wprowadziło

[509] Dane z oficjalnej strony internetowej Rady Europy: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/Cybercrime@Octopus_en.asp [10.08.2015].
[510] COM(96) 487.
[511] COM(96) 483 final.
[512] M. Siwicki, *Cyberprzestępczość* …, s. 37-38.

jednolite i holistyczne przepisy regulujące najbardziej istotne problemy prawne pojawiające się w cyberprzestrzeni. Odgórne uregulowania wymuszały na państwach członkowskich podjęcie odpowiednich kroków w celu wprowadzenia stosownych zmian w swoich krajowych porządkach prawnych i zapewnienia chociaż minimalnych standardów ochrony. Sprzyjało to ujednoliceniu rynku oraz stawia Unię Europejską na stanowisku lidera, kreującego nowe innowacyjne rozwiązania prawne. Wiele państw i innych organizacji międzynarodowych. spoza kręgu europejskiego pilnie śledziło regulacje UE, a następnie wzorując się na przyjętych rozwiązaniach wprowadzało zmiany we własnym prawie. W niniejszym rozdziale zostaną opisane normy prawne Unii Europejskiej odnoszące się do przestrzeni wirtualnej orazpodejmowane przez UE działania legislacyjne w celu zapewnienia bezpieczeństwa sieci, zwalczania cyberprzestępczości, ochrony danych osobowych czy kwestii związanych z wirtualnym obrotem gospodarczym.

3.1.2.2.1 Regulacje bezpośrednio odnoszące się do cyberprzestrzeni

Akty prawne dotyczące bezpieczeństwa sieci

Bezpieczeństwo przestrzeni wirtualnej i istniejących w niej sieci stanowi obecnie jedno z największych wyzwań prawnych i technicznych. Zgodnie z ustawodawstwem unijnym wiele krajów zaczęło wprowadzać do swoich porządków prawnych regulacje związane z cyberbezpieczeństwem i ochroną sieci.

Decyzja Parlamentu Europejskiego i Rady 854/2005/WE z 11 maja 2005 r. w sprawie ustanowienia wieloletniego programu wspólnotowego na rzecz promowania bezpieczniejszego korzystania z Internetu i nowych technologii sieciowych[513]

Ustanowiony na lata 2005-2008 program wspólnotowy Bezpieczniejszy Internet Plus miał na celu promowanie bezpiecznego korzystania z Internetu i nowych technologii sieciowych, w szczególności przez najmłodszych użytkowników sieci.

Cel ten miał być osiągnięty przez realizację następujących działań:

1) zwalczanie treści sprzecznych z prawem - przez zapewnienie ogólnoeuropejskiego zasięgu i współpracy oraz zwiększenie efektywności, wymianę informacji, najlepszych praktyk i doświadczeń przez podniesienie świadomości społecznej na temat numerów interwencyjnych; decyzja nakłada na państwa członkowskie i państwa kandydujące obowiązek wprowadzenia numerów alarmowych, tak by mogły być włączone do europejskiej sieci numerów interwencyjnych (załącznik 1 do decyzji, działanie 1),
2) blokowanie treści niechcianych i szkodliwych - przez upowszechnienie informacji na temat działania i skuteczności filtrującego oprogramowania i usług umożliwiających blokowanie treści szkodliwych i niechcianych, w szczególności w trosce o dostępność takich danych dla małoletnich (załącznik 1 do decyzji, działanie 2),
3) promowanie bezpieczniejszego otoczenia - przez spotkania na Forum Bezpieczniejszy Internet, w którym uczestniczyli przedstawiciele przemysłu, organów ścigania, decydentów oraz organizacji użytkowników (na przykład organizacje rodziców, organy ochrony konsumentów, organy ochrony praw autorskich). Forum stanowiło miejsce spotkań, dyskusji, wymiany informacji oraz doświadczeń na poziomie krajowym i europejskim; zachęcano na nim do promowania bezpieczniejszego Internetu przez zachęcanie dostawców usług do sporządzania kodeksów postępowania, informowania użytkowników o bezpiecznym korzystaniu z sieci oraz z możliwości użycia programów filtrujących czy też numerów interwencyjnych, (załącznik 1 do decyzji, działanie 3),
4) podnoszenie poziomu świadomości - przez przeprowadzanie kampanii społecznych, informowanie użytkowników o europejskim oprogramowaniu i usługach filtrujących,

[513] Dz.Urz UE L 149 z 11.06.2005 r.

uruchomienie węzłów koordynacyjnych w celu wymiany europejskich doświadczeń (załącznik 1 do decyzji, działanie 4).

W programie uczestniczyły osoby prawne mające siedzibę w państwach członkowskich UE oraz osoby prawne z siedzibą w państwach kandydujących. W wyniku realizacji programu rozszerzono sieć numerów interwencyjnych o Czechy i Słowenię, sieć ośrodków odpowiedzialnych za podnoszenie świadomości o Cypr, Luksemburg i Łotwę, gdzie sieci takie wcześniej nie istniały. Ustanowiono również Dzień Bezpiecznego Internetu, który zawsze odbywa się w pierwszej połowie lutego. Jest to element ogólnoświatowych wysiłków w zakresie wspierania bezpieczniejszego korzystania z cyberprzestrzeni przez wszystkich użytkowników, a zwłaszcza dzieci i młodzież[514].

Dyrektywa Parlamentu Europejskiego i Rady nr 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów[515]

Nowelizacja dyrektyw nr 2002/22/WE, 2002/58/WE oraz rozporządzenia (WE) nr 2006/2004 stanowiła konsekwencję reformy ram regulacyjnych Unii Europejskiej w dziedzinie sieci i usług łączności elektronicznej, w tym udoskonalenia przepisów o niepełnosprawnych użytkownikach końcowych. Nowela jest zasadniczym krokiem ku stworzeniu jednolitej europejskiej przestrzeni informacyjnej oraz zintegrowanego społeczeństwa informacyjnego. W preambule (pkt. 3) wskazano, że plan ten jest konsekwencją między innymi komunikatu Komisji dla Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 1 czerwca 2005 roku, zatytułowanego i2010 — Europejskie społeczeństwo informacyjne na rzecz wzrostu gospodarczego i zatrudnienia.

[514] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Komunikat dotyczący realizacji wieloletniego wspólnotowego programu wspierania bezpiecznego korzystania z Internetu i nowych technologii sieciowych (Bezpieczny Internet +), COM/2006/0661 końcowy.
[515] Dz.Urz. UE L 337 z 18.12.2009 r.

Omawiana dyrektywa w szerokim zakresie, w artykule 1 ust. 1-15 wprowadza zmiany dyrektywy 2002/22/WE (dyrektywa o usłudze powszechnej). Nowe przepisy regulują dostarczanie sieci i usług łączności elektronicznej dla użytkowników końcowych, w tym osób niepełnosprawnych. Akt zawiera też postanowienia poruszające kwestię praw i obowiązków przedsiębiorstw zajmujących się świadczeniem usług łączności elektronicznej, jakości i dostępności świadczonych usług, formy zawarcia umowy z przedsiębiorstwami zapewniającymi przyłączenie do publicznej sieci łączności, obowiązku przejrzystego informowania o cenach i taryfach oferowanych usług.

W art. 2 do dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej) wprowadzono zmiany w zakresie bezpieczeństwa przetwarzania usług łączności elektronicznej, dopuszczalności użycia automatycznych systemów wywołujących, wdrażania i egzekwowania kar wynikających z nieegzekwowania przepisów omawianej dyrektywy. Ponadto, zapisano nowe przepisy w zakresie obowiązków dostawcy usług w przypadku naruszenia danych osobowych.

Program Sztokholmski - Otwarta i bezpieczna Europa dla Dobra i Ochrony Obywateli[516]

W Programie Sztokholmskim - Otwarta i Bezpieczna Europa dla Dobra i Ochrony Obywateli Rada Europejska ogłosiła w 2010 roku. Był to harmonogram działań Unii Europejskiej w przestrzeni sprawiedliwości, wolności i bezpieczeństwa na lata 2010-2014. Dokument poruszał wiele kwestii. Zostaną omówione jedynie te, które będą miały bezpośredni lub pośredni związek z cyberprzestrzenią.

Jednym z priorytetów programu, wyrażonym w pkt 1.1. było opracowanie strategii bezpieczeństwa wewnętrznego dla obszaru wspólnotowego w celu walki z przestępczością zorganizowaną, terroryzmem i przestępczością transgraniczną oraz zacieśnieniem współpracy w dziedzinie egzekwowania prawa i kooperacji wymiarów sprawiedliwości w sprawach karnych. Poruszone też zostało zagadnienie ochrony praw obywatela w społeczeństwie informacyjnym oraz konieczność ochrony prywatności między innymi w kontekście wymiany danych osobowych (pkt 2.5). Rada Europejska wezwała Radę, Komisję, PE i państwa członkowskie do opracowania i realizacji polityk mających na celu zwiększenie

[516] Dz.Urz. UE C 115 z 04.05.2010 r.

bezpieczeństwa sieci, przepływu informacji, wzmocnienia infrastruktury krytycznej, w szczególności w zakresie technologii informacyjno-komunikacyjnych i usługowo-komunikacyjnych. Program promował też rozwiązania prawne, które miałyby zapewnić bezpieczeństwo sieci oraz szybką reakcję w przypadku wystąpienia ataków cybernetycznych (pkt 4.2.3). Uznano, że dokument ten był ogromnym krokiem naprzód w kierunku zwiększenia bezpieczeństwa wewnętrznego UE między innymi właśnie z powodu zawarcia w nim postanowień odnoszących się do cyberprzestrzeni[517].

Poważna przestępczość transgraniczna stanowi szczególne zagrożenie dla bezpieczeństwa Unii Europejskiej. Priorytetowo należy zatem traktować przestępstwa takie jak terroryzm, handel ludźmi, handel narkotykami, pornografię dziecięcą i cyberprzestępczość. W Strategii Sztokholmskiej w pkt 3.3.1. założono unifikację przepisów karnych w kwestii wymiaru penalizacji, ustanowienia wspólnych definicji i wymiar kar. W ocenie Rady Europejskiej to Europol winien stać się centrum wymiany informacji między organami ścigania, dostawcami usług i platformą dla organów ścigania, przy jednoczesnym zacieśnianiu współpracy z Eurojustem i Interpolem (pkt 4.3.1.). W związku ze znacznym rozwojem cyberprzestępczości w Programie Sztokholmskim zalecono państwom członkowskim jak najszybszą ratyfikację Konwencji Rady Europy o cyberprzestępczości. W ocenie Rady Europejskiej konwencja RE winna być ramą prawną zwalczania cyberprzestępczości o charakterze globalnym. Na poziomie europejskim szczególną rolę przypisuje się Europolowi, który miałby być europejskim centrum walki ze zjawiskiem (pkt. 4.4.4)

Ocena projektu została przeprowadzona w Rezolucji Parlamentu Europejskiego z dnia 2 kwietnia 2014 r. w sprawie śródokresowego przeglądu Programu Sztokholmskiego[518]. Parlament Europejski w pkt 66 wyraził pogląd, że „przestępczość transgraniczna w UE stale rośnie i w związku z tym podkreśla znaczenie dostatecznego finansowania agencji zajmujących się współpracą organów ścigania; uważa, że obecny „krajobraz" różnych instrumentów, kanałów i narzędzi wymiany informacji między europejskimi organami ścigania jest skomplikowany i rozproszony, co prowadzi do nieskutecznego wykorzystywania dostępnych instrumentów oraz nieodpowiedniego nadzoru demokratycznego i nieodpowiedniej rozliczalności na szczeblu UE; wzywa do opracowania zorientowanej na

[517] A. Kańciak, *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 113-114.
[518] 2013/2024(INI).

przyszłość wizji dotyczącej sposobu kształtowania i optymalizowania wymiany danych pomiędzy organami ścigania w UE przy jednoczesnym zagwarantowaniu praw podstawowych, w tym solidnego poziomu ochrony danych; zauważa, że konieczne jest zwiększenie wzajemnego zaufania pomiędzy organami ścigania w celu usprawnienia wymiany informacji".

Wynikiem inicjatyw podjętych w ramach Programu Sztokholmskiego było utworzenie Europejskiego Centrum do spraw Walki z Cyberprzestępczością przy Europolu, zajmującego się budowaniem zdolności operacyjnych i analitycznych na potrzeby dochodzeń i współpracy z partnerami międzynarodowymi. Parlament Europejski w projekcie rezolucji zauważył postępy poczynione przez państwa członkowskie i Komisję dotyczące strategii bezpieczeństwa i polityki UE w zakresie zwalczania przestępczości międzynarodowej, cyberprzestępczości, przestępczości, której popełnienie ułatwia Internet, czyli pornografia dziecięca, pranie brudnych pieniędzy, ataki na systemy infrastruktury krytycznej, finansowanie terroryzmu. Mimo poczynionych kroków niezbędne jest podejmowanie dalszych działań w celu zwalczania bądź chociażby minimalizacji tego typu czynów przestępczych[519].

Część państw członkowskich mimo zaleceń programu sztokholmskiego nie ratyfikowała konwencji RE o cyberprzestępczości. Wobec powyższego Parlament Europejski w 2014 roku w projekcie rezolucji w sprawie śródokresowego przeglądu Programu Sztokholmskiego wezwał Grecję, Irlandię, Luksemburg, Polskę i Szwecję do ratyfikowania wyżej wymienionej umowy międzynarodowej oraz o jak najszybsze wprowadzenie do swoich wewnętrznych systemów prawnych dyrektywy 2013/40/UE z 12 sierpnia 2013 roku dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW. W wyniku rezolucji Polska oraz Luksemburg wypełniły żądanie i ratyfikowały konwencję o cyberprzestępczości.

[519] Projekt rezolucji Parlamentu Europejskiego z dnia 4 marca 2014 r. w sprawie śródokresowego przeglądu programu sztokholmskiego, pkt. 27 i 55.

Rezolucja Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony (2012/2096(INI))[520]

Parlament Europejski w 2012 roku wydał Rezolucję w sprawie bezpieczeństwa cybernetycznego i cyberobrony. PE w pkt A-Z rezolucji wyraził opinię, że cyberprzestrzeń stała się jednym z najsilniejszych i najskuteczniejszych sposobów przekazywania demokratycznych idei oraz do zrzeszania się w celu walki z dyktaturą. Przestrzeń wirtualna jest jednak szczególnie podatna na zagrożenia, co więcej brakuje w niej wspólnych definicji, norm i środków na poziomie nie tylko unijnym, ale również międzynarodowym. Globalny i nieograniczony charakter cyberprzestrzeni wymaga nowych form międzynarodowej współpracy i zarządzania z udziałem wielu zainteresowanych stron.

Rezolucja przewiduje (w pkt Z, ust 1-55) kilka przewidywanych kierunków zmian:

- działania i koordynacja w UE - konieczność przyjęcia globalnego i skoordynowanego podejścia do problemu zagrożeń w cyberprzestrzeni przez opracowanie kompleksowej unijnej strategii bezpieczeństwa cybernetycznego i cyberobrony, możliwość rozważenia stosowania klauzuli solidarności (art. 222 TFUE) w przypadku ataku cybernetycznego przeciwko któremukolwiek z państw członkowskich; wprowadzenie zmian w polityce unijnej winno zmierzać do zapewnienia maksymalnego poziomu ochrony i zachowania swobód cyfrowych,
- szczebel UE - wezwano wszystkie instytucje UE do pilnego opracowania strategii bezpieczeństwa cybernetycznego i planów awaryjnych własnych systemów, analiz ryzyka oraz planów zarządzania kryzysowego w przypadku wystąpienia cyber – incydentu; położono nacisk na rozwijanie działalności CERT'ów, konieczność przeprowadzenia europejskich ćwiczeń w zakresie ochrony infrastruktury krytycznej oraz rozważenia możliwości powołania stanowiska do spraw unijnej koordynacji cybernetycznej,
- Europejska Agencja Obrony - winna zacieśniać współpracę z NATO, krajowymi oraz międzynarodowymi centrami doskonałości oraz Europejskim Centrum do spraw Walki z Cyberprzestępczością,

[520] Dz. U. C 419 z 16.12.2015 r.

- państwa członkowskie wezwano do udoskonalenia bądź uzupełnienia krajowych strategii bezpieczeństwa cybernetycznego i cyberobrony, opracowania procedur zarządzania ryzykiem, utworzenia wojskowych jednostek zajmujących się cyberbezpieczeństwem oraz wyspecjalizowanych sądów, które będą rozstrzygały sprawy karne dotyczące ataków na systemy informatyczne,
- współpraca publiczno - prywatna bezpieczeństwa cybernetycznego nie może się odbywać się bez współpracy z sektorem prywatnym; wzywa się partnerów z sektora prywatnego do tego, by już na etapie projektowania nowych produktów, sprzętów, usług i aplikacji stosowali odpowiednie zabezpieczenia,
- współpraca międzynarodowa - przez zacieśnienie współpracy z państwami trzecimi, oraz aktywną korelację z ONZ, OBW, OECD oraz Bankiem Centralnym; ponadto, wezwano państwa członkowskie, które jeszcze nie przystąpiły do Konwencji o cyberprzestępczości do jej niezwłocznego podpisania,
- współpraca z NATO - potrzeba wymiany doświadczeń, szczególnie w zakresie planowania, technologii, szkoleń w dziedzinie bezpieczeństwa cybernetycznego i obrony,
- współpraca ze Stanami Zjednoczonymi - kontynuacja podjętej w czasie szczytu transatlantyckiego UE - USA w Lizbonie w 2010 roku współpracy, w tym grupy roboczej UE - USA do spraw bezpieczeństwa cybernetycznego oraz cyberprzestępczości.

Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP))[521]

Wydana 12 września 2013 roku rezolucja PE w pkt A-F zwraca uwagę na rosnące wyzwania cybernetyczne, czyli coraz bardziej zaawansowane ataki zagrażające stabilności i dobrobytowi gospodarczemu państw członkowskich. Zagrożenie to jest o tyle realne, że systemy sieciowe i informatyczne w całej UE są ze sobą ściśle powiązane, a naruszenie bezpieczeństwa informacji może wykroczyć poza granice krajowe i zakłócić funkcjonowanie

[521] Dz. U. C 93 z 09.03.2016 r.

rynku wewnętrznego, podważając równocześnie zaufanie konsumentów do jednolitego rynku cyfrowego.

Parlament Europejski wyartykułował (pkt L, ust 1-24) potrzebę poprawy obronności i bezpieczeństwa UE w cyberprzestrzeni między innymi przez zmiany legislacyjne dostosowujące się do szybkich zmian technologicznych. Zmiany prawodawstwa muszą umożliwiać skuteczną identyfikację i ściganie cyberprzestępców, pomoc ich ofiarom oraz winny propagować wiedzę, edukację i rozwój organizacji CERT oraz rozwój wewnętrznego rynku produktów i usług zapewniających bezpieczeństwo cybernetyczne. Parlament Europejski podkreślił potrzebę opracowania strategicznej polityki komunikacji dotyczącej bezpieczeństwa cybernetycznego UE, sytuacji związanych z kryzysem cybernetycznym, przeglądem strategicznym, współpracą publiczno-prywatną oraz ostrzeżeniami, a także zaleceniami dla ogółu społeczeństwa. Bezpieczeństwo cybernetyczne to nie tylko niezakłócone działanie gospodarki i społeczeństwa, ale przede wszystkim ochrona infrastruktury krytycznej. PE rezolucją wezwał państwa członkowskie oraz Komisję do podjęcia działań w celu zwiększenia świadomości cyberzagrożeń obywateli, zapewnienia doradztwa technicznego i informacji prawnych w zakresie zapobiegania cyberprzestępczości. Wezwano kraje członkowskie do stworzenia szybkich, obustronnych systemów wymiany informacji, czyli zespoły CERT, które mogą być użytecznym narzędziem w procesie rozwoju zaufania w kontekście transgranicznym i międzysektorowym.

Odnosząc się do kwestii obrony cybernetycznej uznano (pkt. L, ust 36-48), że zagrożenia i ataki cybernetyczne silnie zagrażają państwom członkowskim, wobec czego powinny one wzmocnić współpracę z Europejską Agencją Obrony oraz współpracę z NATO, w szczególności w zakresie koordynacji w obszarach planowania, technologii, szkoleń i sprzętu zapewniającego bezpieczeństwo cybernetyczne. Wezwano również Komisję i Europejską Służbę Działań Zewnętrznych do utworzenia zespołu do spraw dyplomacji cybernetycznej, który miałby za zadanie prowadzenie dialogu z innymi państwami i organizacjami o podobnych poglądach w zakresie cyberbezpieczeństwa.

Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2016 r. w sprawie wdrażania wspólnej polityki bezpieczeństwa i obrony (na podstawie sprawozdania rocznego Rady dla Parlamentu Europejskiego na temat wspólnej polityki zagranicznej i bezpieczeństwa), (2016/2067(INI))

Nową rezolucję w sprawie wdrażania wspólnej polityki bezpieczeństwa i obrony z 23 listopada 2016 roku przyjęto wobec zalewającej Europę fali kryzysów - ataków ISIS[522], zalewem imigrantów, atakami na Ukrainę. W obliczu nowej sytuacji w regionie, w pkt. 3 uznano, że „UE powinna poszerzyć dialog i współpracę z państwami trzecimi w regionie oraz z organizacjami działającymi na szczeblu regionalnym i niższym od regionalnego; podkreśla się, że UE powinna być przygotowana na radzenie sobie ze strukturalnymi zmianami w międzynarodowej architekturze bezpieczeństwa, na stawienie czoła wyzwaniom obejmującym konflikty między państwami, upadek państw i ataki cybernetyczne oraz na reagowanie w odpowiedzi na skutki zmian klimatycznych w zakresie bezpieczeństwa". W kolejnych punktach (16-40) zaznaczono, że konflikty we współczesnym świecie rozgrywają się również w cyberprzestrzeni, wobec czego do Wspólnej Polityki Bezpieczeństwa i Obrony należy włączyć elementy cyberbezpieczeństwa i cyberobrony. Z tych też względów Parlament Europejski poparł deklarację podpisaną przez UE i NATO w Warszawie, podkreślając potrzebę pogłębiania współpracy i dalszego budowania zdolności w odniesieniu do zagrożeń cybernetycznych i hybrydowych. Oprócz współpracy z innymi organizacjami międzynarodowymi, wezwano Radę do uwzględniania cyberobrony jako integralnej części debat dotyczących obronności.

Parlament Europejski w pkt. 47 stanął na stanowisku, że „z uwagi na swój charakter cyberbezpieczeństwo jest obszarem polityki, w którym najważniejsza jest współpraca i integracja, nie tylko między państwami członkowskimi UE, kluczowymi partnerami i NATO, ale także między różnymi podmiotami w obrębie społeczeństwa, ponieważ odpowiedzialność za tę kwestię nie ma jedynie charakteru wojskowego; apeluje o jaśniejsze wytyczne na temat sposobu wykorzystania zdolności defensywnych i ofensywnych UE oraz kontekstu takiego wykorzystania; przypomina, że Parlament Europejski wielokrotnie wzywał do gruntownej zmiany rozporządzenia UE dotyczącego wywozu produktów podwójnego zastosowania, aby

[522] ISIS - (ang. *Islamic State of Iraq and Syria*) nazywane również Państwem Islamskim , jest to salaficka organizacja terrorystyczna oraz samozwańczy kalifat ogłoszony w 2014 r. na terytorium Syrii i Iraku.

zapobiec dostaniu się w niewłaściwe ręce oprogramowania i innych systemów, które mogą zostać użyte przeciwko cyfrowej infrastrukturze UE i w celu naruszenia praw człowieka; wzywa UE do obrony na forach międzynarodowych, w tym także na forach zarządzania Internetem, ale nie tylko, zasady, zgodnie z którą podstawowa infrastruktura internetowa powinna stanowić strefę neutralną, w którą nie wolno ingerować rządom dążącym do realizacji swoich krajowych interesów". Zaaprobować należy wyrażone powyżej stanowisko Parlamentu Europejskiego. Cyberbezpieczeństwo przestrzeni wirtualnej nie może być tworzone wyłącznie w ramach jednej organizacji międzynarodowej bądź wąskiej grupy państw. Kwestia ta musi być rozstrzygana we współpracy z organizacjami międzynarodowymi, podmiotami prywatnymi oraz na międzynarodowych forach zrzeszających liczną grupę podmiotów zainteresowanych tą kwestią.

3.1.2.2.2 Regulacje pośrednio odnoszące się do cyberprzestrzeni

Akty prawne dotyczące cyberprzestępczości

Cyberprzestępczość jest jedną z pierwszych kwestii, na które zwrócono uwagę w Unii Europejskiej. Zauważyć należy, że nie przyjęto - na wzór Konwencji o cyberprzestępczości - jednego aktu unijnego regulującego problem przestępczości w przestrzeni wirtualnej. Postanowienia Konwencji Rady Europy są jednak w pełni aprobowane przez UE, która przy rozmaitych okazjach podkreśla konieczność ratyfikacji jej postanowień. W rozważaniach niniejszych przytoczyć należy kilka najważniejszych dokumentów Unii Europejskiej mających na celu zwalczanie poszczególnych form cyberprzestępczości.

Decyzja ramowa Rady nr 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi[523]

Niniejsza decyzja miała na celu harmonizację przepisów krajowych w zakresie zwalczania oszustw popełnianych przy pomocy bezgotówkowych środków płatniczych.

[523] Dz. Urz. WE L 149 z 2.06.2001 r.

Decyzja nakładała na państwa członkowskie obowiązek penalizacji przestępstw odnoszących się do instrumentów płatniczych, transakcji finansowych oraz samego systemu zlecania, przyjmowania, rozliczania i dokonywania transakcji płatniczych, również tych popełnianych za pomocą systemu informatycznego.

W art. 3 decyzji ramowej Rady nr 2001/413/WSiSW zobowiązano państwa członkowskie do penalizacji przestępstw polegających na dokonywaniu lub powodowaniu przekazania pieniędzy lub wartości pieniężnych poprzez doprowadzenie innej osoby do bezprawnej utraty własności w celu uzyskania korzyści ekonomicznej przez osobę popełniającą przestępstwo lub osobę trzecią, za pomocą bezprawnego wprowadzania, zmieniania, usunięcia lub ukrycia danych informatycznych, w szczególności danych umożliwiających identyfikację, lub też za pomocą bezprawnego zakłócania działania programu lub systemu informatycznego. Uchwalenie decyzji ramowej było konsekwencją coraz powszechniejszego użycia bezgotówkowych środków płatniczych, często przez nieświadomych zagrożeń użytkowników. Cyberprzestępcy coraz śmielej zaczęli wykorzystywać nowe technologie do dokonywania oszustw internetowych. Decyzja została transponowana do porządków krajowych przepisów karnych dotyczących środków płatniczych, co można uznać za prawidłowy krok w celu poprawy bezpieczeństwa i zwiększenia pewności obrotu bezgotówkowymi środkami płatniczymi.

Decyzja ramowa 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych[524]

Celem wydania niniejszej decyzji ramowej była harmonizacja przepisów karnych państw członkowskich w zakresie zwalczania rasizmu i ksenofobii, tak by zapewniały one skuteczne, proporcjonalne i odstraszające sankcje karne. Nie mniej istotne było też poszerzenie i polepszenie współpracy sądowej w tym przedmiocie. Decyzja w art. 1 nakazywała penalizację szeregu przestępstw popełnianych na tle rasistowskim i ksenofobicznym między innymi publicznego nawoływania do przemocy lub nienawiści skierowanej przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko

[524] Dz.Urz.UE L 328 z 6.12.2008 r., s. 55-58.

członkowi takiej grupy - w tym popełnienie takiego czynu przez publiczne rozpowszechnianie lub rozprowadzanie tekstów, obrazów oraz innych materiałów o takiej treści.

Oprócz standardowych zasad jurysdykcji terytorialnej i personalnej, decyzja przewiduje w art. 9 ust. 2, że państwo członkowskie UE może zastosować swoją jurysdykcję, jeżeli czyn został popełniony w obrębie systemu informacyjnego, a:

a) sprawca popełniając określone w decyzji ramowej czyny, jest fizycznie obecny na terytorium państwa członkowskiego UE, niezależnie od tego, czy czyny te dotyczą materiału zawartego w systemie informacyjnym kontrolowanym z jego terytorium,
b) czyny dotyczą materiału zawartego w systemie informacyjnym kontrolowanym z terytorium państwa członkowskiego UE, niezależnie od tego, czy sprawca, popełniając je, fizycznie jest obecny na jego terytorium.

Decyzja, oprócz karalności sprawstwa, przewidywała w art. 6 odpowiedzialność podżegacza, pomocnika oraz osób prawnych. Kary i środki karne, jakie można zastosować wobec osób prawnych nie musiały ograniczać się jedynie do grzywien i kar pieniężnych, lecz mogły obejmować takie środki, jak: pozbawienie prawa do wsparcia publicznego lub pomocy publicznej, czasowy lub stały zakaz działalności handlowej, nadzór sądowy czy też sądowy nakaz likwidacji.

Zarówno Protokół dodatkowy Konwencji o cyberprzestępczości, jak i omawiana decyzja mają na celu zwalczanie przejawów nienawiści i rasowej ksenofobii wyrażonej za pomocą cyberprzestrzeni. Dylematem jest pozostawienie odpowiedniego poziomu równowagi pomiędzy dwoma wartościami: ochroną przed nienawiścią i wolnością słowa. Decyzja została wydana w czasie, gdy gro państw nie zdecydowało się jeszcze na związanie się Protokołem dodatkowym Konwencji o cyberprzestępczości, wobec czego była odpowiedzią na potrzebę harmonizacji prawa państw członkowskich w przeciwdziałaniu dyskryminacji. Co istotne, w decyzji ramowej 2008/913/WSiSW zawarto określone procedury pomocy ofiarom dyskryminacji.

Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW[525]

Dyrektywa PE i Rady nr 2011/93/WE ma na celu harmonizację przepisów państw członkowskich Unii Europejskiej w zakresie kryminalizacji niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej. Przewiduje penalizację około dwudziestu przestępstw w czterech kategoriach:

- niegodziwego traktowania w celach seksualnych, na przykład podejmowania czynności seksualnych z udziałem dziecka, doprowadzenia małoletniego do bycia świadkiem czynności seksualnych (art. 3),
- wykorzystania seksualnego, na przykład doprowadzanie lub nakłanianie dziecka do udziału w przedstawieniach pornograficznych lub prostytucji dziecięcej, użycie groźby lub przymusu w tym celu, świadome branie udziału w przedstawieniach pornograficznych z udziałem dziecka i inne (art. 4),
- pornografii dziecięcej, na przykład nabywania, posiadania, udostępniania za pomocą technologii informacyjno - komunikacyjnych pornografii dziecięcej, dystrybucja, rozpowszechnianie oraz oferowanie pornografii dziecięcej (art. 5),
- *grooming*, czyli nagabywanie dzieci za pośrednictwem technologii informacyjno - komunikacyjnych w celach seksualnych (art. 6).

Przepisy dyrektywy zobowiązują państwa członkowskie do podjęcia wszelkich możliwych kroków, w wymienionej kategorii poważnych przestępstw seksualnych na szkodę małoletnich, do umożliwienia ścigania przez wystarczający i proporcjonalny do wagi przestępstwa okres liczony od momentu osiągnięcia pełnoletniości przez pokrzywdzonego. W

[525] Dz. Urz. UE L 335 z 17.12.2011 r.

literaturze przedmiotu zwraca się uwagę na przyjętą elastyczną terminologię „wystarczający" czas ma zapewnić skuteczne ściganie i być „proporcjonalnym do danego przestępstwa"[526].

Dyrektywa 2011/93/UE w art. 9 pozostawia państwom członkowskim decyzję w zakresie wymiaru kary za poszczególne przestępstwa, zastrzegając pewne wartości progowe od jednego roku do dziesięciu lat pozbawienia wolności - w zależności od rodzaju popełnionego czynu oraz od tego, czy dziecko osiągnęło wiek przyzwolenia czy nie. Podżeganie do popełnienia wyżej wymienionych przestępstw również zostało uznane za czyn karalny. Omawiany akt prawny wprowadza w art. 9 szereg czynności, które winny być uznane za okoliczności obciążające w prawie krajowym państw członkowskich. Okolicznościami takimi są wcześniejsza recydywa sprawcy za przestępstwo o tym samym charakterze, popełnienie przestępstwa przez członka rodziny lub osobę bliską dziecku, popełnienie przestępstwa przez wiele osób działających wspólnie czy też użycie poważnej przemocy.

Dyrektywa nakłada na państwa obowiązek podjęcia niezbędnych kroków, aby strony internetowe zawierające lub rozpowszechniające pornografię dziecięcą utrzymywane na ich terytorium były szybko usuwane. Państwa winny dążyć do zapewnienia usunięcia takich stron utrzymywanych poza ich terytorium. Przyznaje ona państwom możliwość blokowania dostępu do stron internetowych zawierających pornografię dziecięcą na swoim terytorium, o ile czynności takie będą przeprowadzane opierając się na przejrzystej procedurze i dostarczając odpowiedniej gwarancji i informowania użytkowników sieci o powodzie zablokowania witryny (art. 25).

Dyrektywa wraz z Konwencją z Lanzarote oraz z Konwencją o cyberprzestępczości tworzy ramy prawne ochrony dzieci przed wykorzystywaniem seksualnym, również za pomocą przestrzeni wirtualnej wprowadzając minimalne normy oraz zakres kar. Na szczególną aprobatę zasługuje wprowadzenie ochrony dzieci podczas postępowania przygotowawczego oraz sądowego, w szczególności przez zapewnienie odpowiednich, mniej stresogennych metod przesłuchań małoletnich (w odpowiednich pomieszczeniach przez wyszkolonych specjalistów), dostęp do doradztwa i zastępstwa prawnego. Dziecko, które padło ofiarą przemocy seksualnej winno mieć zapewnioną szeroką ochronę ze strony państwa, a postępowanie karne, oprócz podstawowego celu, jakim jest ukaranie sprawcy,

[526] M. Kulik, *Zmiana przepisów dotyczących przedawnienia wprowadzone ustawą z dnia 20 lutego 2015 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*, „Annales Universitatis Mariae Curie - Skłodowska" 2016, t. 63, s. 64-65.

winno być przeprowadzone w taki sposób, by minimalizować niepotrzebne czynności z udziałem małoletnich. Z tych też względów, standardy zapewnione przez dyrektywę 2011/93/UE zasługują na aprobatę.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE w sprawie ataków na systemy informatyczne i uchylającą decyzję ramową Rady 2005/222/WSiSW[527]

Dyrektywa, mimo że ma częściowo charakter uchylający, zachowuje znaczną część poprzednich regulacji, wprowadzając równocześnie dodatkowe przepisy materialnoprawne. Omawiany akt unijny ustanowił minimalne normy dotyczące określania przestępstw i kar w dziedzinie ataków na systemy informatyczne. Drugim z celów jego ustanowienia było ułatwienie zapobiegania takim przestępstwom oraz usprawnienie współpracy pomiędzy organami sprawiedliwości (art. 1).

Maciej Siwicki zalicza do postanowień dyrektywy w sprawie ataków na systemy informatyczne, mających najistotniejsze znaczenie:

a) „penalizację wytwarzania, sprzedaży, dostarczenia w celu używania, przywozu, dystrybucji oraz innych sposobów udostępniania urządzeń, w tym programu komputerowego, zaprojektowanego lub przystosowanego głównie do celu popełniania przestępstw (art. 7);
b) zawiera okoliczności obciążające:
    i. przeprowadzenia ataków z wykorzystaniem narzędzia zaprojektowanego do prowadzenia ataków dotykających znacznej liczby systemów informatycznych lub ataków powodujących znaczne szkody, takie jak zakłócenie usług systemowych, straty finansowe lub utrata danych osobowych (art. 9 ust 3),
    ii. jeśli ataki te popełnione są przez sprawcę ukrywającego swoją prawdziwą tożsamość i narażającego na podejrzenia prawowitego właściciela tożsamości (art. 9 ust 5),
    iii. zostały popełnione w ramach organizacji przestępczej, w rozumieniu decyzji ramowej 2008/841/WSiSW, niezależnie od tego, jaki wymiar kary w niej przewidziano,

[527] Dz.Urz. UE L 218/8 z 14.08.2013 r.

iv. powodują poważne szkody,
v. zostały popełnione przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej;

c) wprowadza nowe przestępstwo 'nielegalnego przechwytywania' (art. 6)"[528].

Dyrektywa wprowadza odpowiedzialność osób prawnych, w tym przez nałożenie na nie kar finansowych (art. 11). Zauważając potrzebę międzypaństwowego koordynowania działań na państwa członkowskie został nałożony obowiązek ustanowienia punktów kontaktowych dostępnych 24/7, dzięki którym możliwa jest szybka wymiana informacji (art. 13).

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE zawiera obszerniejsze postanowienia niż decyzja ramowa Rady 2005/222/WSiSW. Przede wszystkim został wprowadzony szerszy katalog przestępstw, które winne być uznane za cyberprzestępstwo oraz wprowadzono okoliczności obciążające popełnienia przestępstwa (spowodowanie szkody, posłużenie się przez cyberprzestępcę tożsamością innej osoby)[529]. Podkreślenia jest wartym fakt, iż dyrektywa określa jedynie standardy minimalne. Oznacza to, że państwa członkowskie nie mogą wprowadzić mniejszych standardów niż te wyznaczone aktem unijnym. Dozwolone jednak jest rozszerzenie zakresu kryminalizacji na przykład przez wprowadzenie karalności usiłowania czy też kwalifikowanych typów czynów. Nie można wykluczyć również, iż za kilka lat zaistnieje potrzeba wprowadzenia nowych regulacji, odpowiadającym nowym wyzwaniom technologii ICT.

Akty prawne dotyczące danych osobowych

Twórcy i właściciele stron internetowych, aplikacji i programów uzyskali dostęp do ogromnych baz danych swoich użytkowników. Już w latach dziewięćdziesiątych XX wieku UE podjęła pierwsze kroki w celu uregulowania i ochrony baz danych. Z upływem lat okazało się, że przepisy te są już niewystarczające i nie odpowiadają współczesnym standardom. Unia Europejska podjęła się wprowadzenia nowych przepisów, które zapewnią należytą ochronę internautów.

[528] M. Siwicki, *Cyberprzestępczość*…, s. 42-43.
[529] F. Radonewicz, op. cit., s. 258.

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnych przepływie takich danych[530]

Rozporządzenie 45/2001 zostało ustanowione w celu zapewnienia osobom fizycznym ochrony w zakresie przetwarzania ich danych osobowych przez instytucje i organy wspólnotowe oraz zapewnienia spójności przepisów i procedur w tym przedmiocie. Rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez osoby fizyczne w ramach działalności osobistej lub domowej, w ramach działalności nieobjętej zakresem prawa UE, przez organy, jednostki organizacyjne i organizacji Unii Europejskiej oraz przez zewnętrzne działania państw członkowskich oraz tych, dotyczących wspólnej polityki zagranicznej i bezpieczeństwa[531]. Aktem tym powołany został Europejski Inspektor Ochrony Danych, który ma monitorować wykonywanie przepisów ochrony danych przez organy i instytucje UE. Wprowadzenie tego niezależnego organu nadzorczego jest trafnym rozwiązaniem, ponieważ pozwoliło na realną kontrolę przestrzegania prawa.

Rozporządzenie wprowadziło w art. 5-10 normy zapewniające poszanowanie danych osobowych, które pozostają w posiadaniu organów wspólnotowych, również tych przetwarzanych przy użyciu sieci telekomunikacyjnych. Dane muszą być przetwarzane rzetelnie i legalnie, powinny być przeznaczone do określonych, jednoznacznych i legalnych celów, muszą również być prawidłowe i w razie konieczności aktualizowane. Przetwarzanie danych może nastąpić wyłącznie wówczas, jeżeli jest to niezbędne do przeprowadzenia zadania na potrzeby interesu publicznego, a użytkownik udzielił zgody na takie przetwarzanie. Z kolei z zasady jest zakazane przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych oraz danych dotyczących zdrowia i życia seksualnego, jak również danych związanych ze sprawami karnymi.

[530] Dz. Urz. UE L 8 z 12.01.2001.
[531] P. Kowalik, D. Wociór, *Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego*, [w:] A. Balicki, P. Barta, M. Byczkowski i in., *Ochrona danych osobowych w sektorze publicznym*, Warszawa 2016, s. 13.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[532]

Rozporządzenie uchwalone 27 kwietnia 2016 roku wejdzie w życie 24 kwietnia 2018 roku, jednakże już obecnie należy mu poświęcić kilka słów, ponieważ wprowadza ono ogromne zmiany rewolucjonizujące kwestię ochrony danych osobowych w Unii Europejskiej. Rozporządzenie 2016/679 zastępuje obowiązującą przez ponad dwie dekady dyrektywę 95/46/WE, która stanowiła podstawowy unijny akt prawny o ochronie danych osobowych. Dyrektywa z czasem, postępującym rozwojem technologicznym oraz postępującą globalizacją okazała się niewystarczająca w obliczu nowych wyzwań[533].

Rozporządzenie ma zapewnić lepszą ochronę danych osobowych mieszkańców UE oraz modernizację i przystosowanie dotychczasowych regulacji do realiów nowego wirtualnego świata. Unowocześnienie i ujednolicenie przepisów umożliwi przedsiębiorstwom ograniczenie biurokracji przez wprowadzenie koncepcji domyślnej ochrony danych osobowych. Rozporządzenie nr 2016/679 daje (art. 12-23) obywatelom możliwość większej kontroli oraz wzmacnia ich prawa między innymi przez łatwiejszy dostęp do danych (zwiększenie liczby informacji na temat sposobu przetwarzania danych, udostępnienia tych informacji w sposób jasny i przejrzysty), nowe prawo do przenoszenia danych (pomiędzy dostawcami usług), klarowniejsze procedury usunięcia danych („prawo do bycia zapomnianym”[*]) oraz wprowadzenie prawa obywatela do bycia poinformowanym o przeprowadzeniu ataku hackerskiego na bazę danych przechowującą jego dane.

Rozporządzenie nakłada również szereg obowiązków na administratora i podmiot przetwarzający dane osobowe (art. 24-33). Zobowiązano ich do dostosowania swoich rozwiązań do omawianej dyrektywy, uwzględnienia ochrony danych osobowych już na etapie projektowania oraz przyjęcia zasady domyślnej ochrony danych, wprowadzenia obowiązku informowania odpowiednich organów nadzorczych o ataku hackerskim przeprowadzonym na bazę danych. Co istotne, przepisy rozporządzenia będzie stosować się również w odniesieniu

[532] Dz.U. L 119 z 4.5.2016.
[533] E. Bielak- Jomaa, *Źródła prawa ochrony danych osobowych*, [w:] T.A.J. Banyś, E. Bielak - Jomaa, M. Kuba i in., *Prawo ochrony danych osobowych*, Warszawa 2013, s. 48.
[*] Więcej na ten temat w rozdziale 4.4.2. *Cyberprzestrzeń a ochrona danych osobowych*.

do firm spoza Unii Europejskiej, jeśli przedsiębiorstwa te będą oferowały towary i usługi na terytorium państw członkowskich. Rozporządzenie ma szczególne znaczenie w kontekście wielkich firm internetowych takich, jak Facebook czy Google, które mają swoje siedziby w Stanach Zjednoczonych.

Nowe rozporządzenie o danych osobowych nakłada bardziej transparentne przepisy dotyczące sposobu przetwarzania danych oraz informowania o ich retencji (24-33). Trafnym rozwiązaniem jest wprowadzenie obowiązku informowania o wycieku danych osobowych. Szczególnie silnią ochronę postanowiono przyznać osobom fizycznym, równocześnie wprowadzając bardzo restrykcyjne przepisy dla firm. Szczególne kontrowersje budzą przepisy zakładające dotkliwe kary finansowe dla przedsiębiorców, które mogą wynosić nawet 20 milionów euro, a w przypadku przedsiębiorstwa - nawet do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (art. 83 pkt. 5). Ponadto, organy i instytucje UE zostały zobowiązane do podjęcia właściwych kroków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa użycia sieci telekomunikacyjnych oraz poufności przepływu takich danych. Za wcześnie jest wyrokować, jakie będą faktyczne konsekwencje unijnych zmian. Jedno jest pewne. Rozporządzenie nr 2016/679 jest niewątpliwą rewolucją w dziedzinie ochrony danych osobowych.

Akty prawne dotyczące obrotu gospodarczego

W doktrynie niejednokrotnie wskazuje się, że brak jest systematyki istniejących regulacji UE dotyczącej umów elektronicznych. Dotychczasowe dokumenty skupiają się na statusie uczestników (konsument, użytkownik, świadczący usługi telekomunikacyjne), środkach komunikacji (poczta, telefon) lub też przedmiocie (na przykład usługach finansowych, umowach przewozu)[534]. Organy prawodawcze w UE zdają sobie sprawę z potencjału i możliwości cyberprzestrzeni w perspektywie stworzenia silnego, konkurencyjnego rynku. W 2010 roku przyjęto „Strategię 2020”[535] i w jej ramach Agendę Cyfrową, która ma stworzyć jednolity rynek cyfrowy do 2020 roku. Europejski rynek

[534] W. Kilian, *Umowy elektroniczne w prawie międzynarodowym*, [w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003, s. 218.

[535] Komunikat Komisji, *Europa 2020 Straregia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu*, KOM(2010)2020, dokument dostępny w języku polskim na oficalnej stronie internetowej Komisji Eurpejskiej: http://ec.europa.eu/eu2020/pdf/1_PL_ACT_part1_v1.pdf [20.02.2017].

cyfrowy miałby stanowić godnego rywala USA w prymacie w rozwoju społeczeństwa informacyjnego[536].

Dyrektywa Parlamentu Europejskiego i Rady nr 2000/31/WE z dnia 8 czerwca 2000 r., w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[537]

Celem uchwalenia dyrektywy było wzmocnienie bezpieczeństwa prawnego handlu elektronicznego, a tym samym zwiększenie zaufania użytkowników do sieci wirtualnej. Dyrektywa ustanawia stabilne ramy prawne, w którym usługi społeczeństwa informacyjnego podporządkowane są zasadom panującym na rynku wewnętrznym (art. 1 ust. 1). Jednym z celów ustanowienia dyrektywy było wyeliminowanie rozbieżności orzeczniczych w państwach członkowskich.

Dyrektywa ma zastosowanie do usług świadczonych w społeczeństwie informacyjnym między przedsiębiorcami oraz między przedsiębiorcami a odbiorcami końcowymi w zakresie usług świadczonych nieodpłatnie oraz usług *on-line*. Dyrektywę stosuje się głównie do rynku wewnętrznego, w kwestiach takich, jak siedziby usługodawców, informacje handlowe, umowy zawierane drogą elektroniczną, odpowiedzialność pośredników, kodeksów postępowania, pozasądowych dróg rozstrzygania sporów, dochodzenia praw przed sądem oraz współpracy między państwami członkowskimi (art. 1 ust 2). Dyrektywa obejmuje zatem takie sektory działalności człowieka w cyberprzestrzeni, jak prasa internetowa, internetowe bazy danych, elektroniczne usługi finansowe czy rozrywkowe oraz usługi przedstawicieli wolnych zawodów (lekarzy, adwokatów, księgowych) świadczone *on-line*.

Rozdział II dyrektywy o handlu elektronicznym nakłada na państwa członkowskie liczne obowiązki[538]między innymi:

- zabrania nakładania obowiązków, uzyskiwania specjalnych zezwoleń usługodawcom świadczącym usługi społeczeństwa informacyjnego, jeżeli tożsama działalność

[536] P.P. Polański, *Europejskie …*, s. 381.
[537] Dz.Urz. UE L 178 z 17.07.2000 r.
[538] Więcej w: D. Lubasz, *Handel elektroniczny. Bariery prawne*, Warszawa 2013.

nieinternetowa nie wymaga takich środków; obowiązek uzyskania zezwolenia na stworzenie portalu internetowego nałożony przez państwo jest zatem niezgodny z dyrektywą; jednakże, jeżeli działalność portalu jest związana na przykład z usługami finansowymi lub bankowymi, to państwo może uzależnić powstanie witryny od uzyskania odpowiedniego zezwolenia,

- zobowiązuje państwa członkowskie do wprowadzenia legislatury nakazującej usługodawcom umożliwienie łatwego, bezpośredniego i stałego dostępu usługobiorcom oraz odpowiednim władzom do informacji dotyczących ich działalności, czyli imienia, nazwiska, adresu, e-maila, numeru rejestru handlowego, tytułu zawodowego,
- nakłada obowiązki, dotyczące informacji handlowej przesyłanej za pomocą systemu informatycznego; powinny one być wyraźnie rozpoznawalne jako informacje handlowe, mieć jednoznaczny charakter, wzmacniać zaufanie klienta i gwarantować uczciwe praktyki handlowe; dodatkowo państwa członkowskie mają wprowadzić odpowiednie uregulowania zapewniające osobom fizycznym możliwość wyłączenia niechcianej poczty (czyli spamu),
- usunięcia wszelkich ograniczeń zakazujących używania informacji handlowych w stosunku do zawodów regulowanych, o ile jest to zgodne z zasadami wykonywania zawodu, etyką i godnością zawodu,
- usunięcia wszelkich zakazów i ograniczeń dotyczących stosowania umów elektronicznych,
- wprowadzenia zasad odpowiedzialności pośredników, w szczególności dostawców hostingu, w przypadku niezgodnych z prawem lub szkodliwych treści publikowanych na ich serwerze lub w ich sieci.

Szerszego omówienia wymaga kwestia umów zawieranych drogą elektroniczną, który został poruszony w sekcji 3 dyrektywy. Artykuł 9 nakłada na państwa członkowskie obowiązek zapewnienia, by ich system prawny umożliwiał zawieranie umów drogą elektroniczną, w szczególności, by regulacje prawne nie stanowiły przeszkody dla używania umów elektronicznych, ani nie wpływały na ich skuteczność i ważność. Niemniej jednak dozwolono na wyłączenia stosowania umów elektronicznych w niektórych kategoriach spraw takich, jak umowy przenoszące prawa do nieruchomości, umowy dotyczące prawa rodzinnego i spadkowego czy umowy poręczenia.

Postanowienia art. 10 dyrektywy poruszają zagadnienie poszczególnych etapów zawierania umów, które winny być sformułowane w sposób jasny, zrozumiały i jednoznaczny przed złożeniem zamówienia przez usługobiorcę. Ponadto, zamieszczono przepis wprowadzający obowiązek zapewnienia środków technicznych umożliwiających określenie i usunięcie błędów przed złożeniem zamówienia, przekazania ogólnych warunków umów i wskazania kodeksów postępowania. Kolejne postanowienia (art. 11) nakładają obowiązek elektronicznego potwierdzenia zamówienia, które uważa się za przyjęte, gdy strony, do których zamówienie oraz potwierdzenie odbioru jest adresowane, mogą mieć do niech elektroniczny dostęp.

Dyrektywa o handlu elektronicznym wywarła ogromny wpływ na obrót gospodarczy w przestrzeni cyfrowej. Przede wszystkim w znacznym stopniu zunifikowała przepisy w zakresie przejrzystości i wymagań stawianych dostawcom usług, kontaktów drogą elektroniczną czy komunikacji handlowej. Z perspektywy prawa zobowiązań ogromne znaczenie spełniają przepisy stwarzające możliwość identyfikacji i poprawy błędów w transakcjach elektronicznych.

W doktrynie podnosi się, że kontrowersje wzbudza kwestia udostępniania danych osobowych usługobiorców naruszających prawa osób trzecich przez pośredników internetowych. Budzące wątpliwości jest ustalenie zakresu odpowiedzialności dostawców usług hostingu i obciążenia ciężarem dowodu osobę, która została dotknięta bezprawnym działaniem naruszyciela[539]. Wprowadzenie obowiązków informacyjnych usługodawców świadczących usługi społeczeństwa informacyjnego było trafnym rozwiązaniem, jednakże martwi brak mechanizmów sankcyjnych, które egzekwowałyby ich wykonanie[540]. Nie można oprzeć się wrażeniu, że finalny kształt dyrektywy był efektem ogromnego kompromisu. W dyrektywnie o handlu elektronicznym nie zdecydowano się na wprowadzenie procedur zawierania umów elektronicznych, co w konsekwencji spowodowało znaczne rozbieżności w implementacji aktu w różnych krajach członkowskich[541].

Dyrektywa o handlu elektronicznym nie może zostać uznana za kompleksowy akt regulujący e-commerce, ponieważ nie zostały w niej poruszone wszystkie aspekty handlu elektronicznego pominięto podatki, prawo konkurencji, hazardu czy danych osobowych. Zagadnienia te, z różnym efektem, są przedmiotem innych unijnych regulacji.

[539] P.P. Polański, *Europejskie …*, s. 275-276.
[540] D. Lubasz, *Handel …*, s. 221.
[541] Ibidem, s. 284.

Fragmentaryzacja przepisów unijnych powoduje trudności przy transpozycji do prawa krajowego jak i problemy w wykładni.

Dyrektywa 2002/65/WE Parlamentu Europejskiego i Rady z dnia 23 września 2002 r. dotycząca sprzedaży konsumentom usług finansowych na odległość oraz zmieniająca dyrektywę Rady 90/619/EWG oraz dyrektywy 97/7/WE i 98/27/WE[542]

Dyrektywa miała na celu ujednolicenie przepisów krajowych państw członkowskich w zakresie sprzedaży usług finansowych na odległość, rozumianych jak każda umowa dotycząca usług finansowych zawarta pomiędzy dostawcą a konsumentem w ramach zorganizowanej sprzedaży na odległość, czyli za pomocą faksu, telefonu czy właśnie Internetu. Przyznaje ochronę konsumentów między innymi zobowiązując dostawcę do doręczenia przed zawarciem umowy wszystkich niezbędnych informacji, poinformowania o prawie konsumenta do odstąpienia od umowy w przeciągu 14 dni. Ponadto, akt unijny wprowadził (art. 1-9) zakaz stosowania niezgodnych z prawem praktyk sprzedażowych (niedozwolone klauzule umowne) oraz ogranicza niechciany kontakt z przedsiębiorcą (spam). Postanowienia dyrektywy były lepiej przygotowane z punktu widzenia technologicznego niż poprzednie tożsame regulacje, lecz mimo wszystko jej postanowienia są mało klarowne w realiach obrotu elektronicznego.

Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady[543] **(Dyrektywa w sprawie konsumentów)**

Przytoczony akt unijny reguluje sprzedaż konsumencką na odległość w obszarze wszystkich innych niefinansowych towarów i usług. Dyrektywa zwiększa ochronę konsumentów przez harmonizację kluczowych aspektów krajowych regulacji dotyczących umów zawieranych pomiędzy klientami a przedsiębiorcami. Jest to szczególne istotne,

[542] Dz.U. L 271 z 09.10.2002.
[543] Dz. Urz. UE L 304 z 22.11.2011 r.

ponieważ w znaczny sposób ułatwia i ujednolica handel transgraniczny, w szczególności w zakresie umów zawieranych za pośrednictwem sieci wirtualnej. Omawiany akt prawny zastępuje dyrektywę w sprawie sprzedaży na odległość (nr 97/7/WE[544]) oraz dyrektywę o sprzedaży obwoźnej (nr 85/577/EWG[545]). Dyrektywa w sprawie konsumentów „stanowi najważniejszy instrument dotyczący handlu elektronicznego przyjęty na początku trzeciej dekady harmonizacji prawa handlu elektronicznego. Jako następczyni dyrektywy 97/7/WE dotyczącej ochrony konsumenta przy umowach zawieranych na odległość programowo odchodzi ona od idei harmonizacji minimalnej, na której oparta była dyrektywa 97/7/WE na rzecz harmonizacji maksymalnej"[546].

Zgodnie z przepisami dyrektywy nr 2011/83/UE przed zawarciem umowy na przedsiębiorcy ciąży obowiązek dostarczenia konsumentowi pewnych informacji, które stanowią integralną część umowy. Są to informacje na temat: głównych cech i łącznej ceny towarów i usług, danych identyfikujących przedsiębiorcę, warunków płatności, dostawy, reklamacji, czasu trwania umowy czy też funkcjonalności i interoperacyjności treści cyfrowych ze sprzętem komputerowym i oprogramowaniem i innych (art. 5-6). Dyrektywa zapewnia konsumentowi prawo do odstąpienia od umowy, również tej zawartej za pomocą przestrzeni wirtualnej, określa jej skutki oraz obowiązki przedsiębiorcy i konsumenta w przypadku odstąpienia (art. 9-16). Wprowadza wiele nowych postanowień między innymi szersze pojęcie konsumenta (też przedsiębiorca, który zawiera umowę poza zakresem prowadzonej działalności gospodarczej), wprowadza do porządku unijnego konstrukcję umowy o dostarczanie treści cyfrowych oraz rozszerza katalog obowiązków informacyjnych.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS)[547]

Rozporządzenie w sprawie identyfikacji elektronicznej i usług zaufania (rozporządzenie eIDAS) ustanowiło nowy system bezpiecznych interakcji elektronicznych

[544] Dyrektywa nr 97/7/WE Parlamentu Europejskiego i Rady z dnia 20 maja 1997 r. w sprawie ochrony konsumentów w przypadku umów zawieranych na odległość.
[545] Dyrektywa nr 85/577/EWG Rady z dnia 20 grudnia 1985 r. w sprawie ochrony konsumentów w odniesieniu do umów zawartych poza lokalem przedsiębiorstwa.
[546] P.P. Polański, *Europejskie* ..., s. 308-309.
[547] Dz.U. L 257, z 28.8.2014.

zawieranych pomiędzy przedsiębiorcami, osobami fizycznymi i władzami publicznymi. Celem omawianego aktu prawnego jest zwiększenie zaufania do transakcji zawieranych za pomocą cyberprzestrzeni. Akt ten zastąpił również od 1 lipca 2016 roku dyrektywę 1999/93/WE w sprawie wspólnotowych ram prawnych dla podpisów elektronicznych.

Rozporządzenie wprowadza powszechnie rozpoznawalne mechanizmy identyfikacji elektronicznej (iID), które jednoznacznie umożliwiają weryfikację tożsamości użytkowników *on-line*. Zgodnie z art. 3 ust 1. elektroniczna identyfikacja rozumiana jest jako proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną. Omawiany akt prawny wprowadza wiele zmian, dostosowując stan prawny do obecnych potrzeb użytkowników sieci. Wprowadzono między innymi pieczęci elektroniczne[548], doręczenia elektroniczne, zabezpieczenia stron internetowych oraz usługi walidacji i konserwacji pieczęci i podpisów elektronicznych.

Zgodnie z rozdziałem II rozporządzenia (art. 6-9) środki identyfikacji elektronicznej, spełniające wymogi rozporządzenia, zgłoszone Komisji oraz zamieszczone w opublikowanym wykazie, wydane przez państwo członkowskie Unii Europejskiej, muszą być uznane przez pozostałe kraje UE. Program identyfikacji elektronicznej wprowadza trzy poziomy bezpieczeństwa: niski, średni i wysoki. Zasada wzajemnego uznawania środków identyfikacji elektronicznej zacznie obowiązywać od 28 września 2018 roku, a w przypadku podmiotów sektora publicznego zasada wzajemnego uznawania obowiązywać będzie wyłącznie w odniesieniu średniego bądź wysokiego poziomu bezpieczeństwa.

Rozporządzenie przewiduje, iż notyfikowane krajowe systemy identyfikacji elektronicznej muszą być interoperacyjne (art. 12), czyli muszą być neutralne technologicznie, nie mogą dyskryminować żadnych konkretnych rozwiązań technologicznych w zakresie identyfikacji elektronicznej, muszą być zgodne z ogólnymi międzynarodowymi standardami, ułatwiając zasady ochrony prywatności i przetwarzanie danych osobowych zgodnie z dyrektywą 95/46/WE. Ponadto, art. 3 wprowadza się usługi zaufania definiowanego jako świadczone za wynagrodzeniem, a obejmujące:

[548] Więcej o pieczęciach elektronicznych w prawie polskim w: D. Szostek, *Pieczęć elektroniczna i jej możliwość wykorzystania w prawie polskim*, [w:] K. Flaga - Gieruszyńska, J. Gołaczyński, D. Szostek, *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016.

- tworzenie, weryfikację, walidację podpisów elektronicznych, pieczęci elektronicznych lub
- elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami,
- tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych,
- konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

Coraz większa liczba umów internetowych ma charakter transgraniczny. Małe i średnie przedsiębiorstwa coraz częściej oferują swoje usługi w innych państwach członkowskich. Dlatego też pełna harmonizacja w zakresie informacji dla konsumentów i prawa do odstąpienia od umów zawieranych na odległość i umów zawieranych poza lokalem przedsiębiorstwa przyczyni się do wysokiego poziomu ochrony konsumentów i lepszego funkcjonowania rynku wewnętrznego w stosunkach między przedsiębiorstwami a konsumentami.

Akty prawne dotyczące własności intelektualnej

Tak jak w pozostałych przytoczonych przypadkach nie istnieje generalne, jednolite prawo autorskie Unii Europejskiej. Powstały jednak liczne dyrektywy dotyczące szeroko rozumianego prawa autorskiego. Regulują one kwestie: ochrony programów komputerowych[549], prawa najmu i użyczenia oraz niektórych praw pokrewnych prawu autorskiemu w zakresie własności intelektualnej[550], prawa autorskiego i praw pokrewnych dotyczących przekazu satelitarnego i retransmisji kablowej[551], czasu ochrony prawa autorskiego[552], ochrony baz danych[553], prawa autorskiego w społeczeństwie

[549] Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych, Dz. Urz. UE L 265 z 11.10.2011, s. 1.
[550] Dyrektywa Parlamentu Europejskiego i Rady 2006/115/WE z dnia 12 grudnia 2006 r. w sprawie prawa najmu i użyczenia oraz niektórych praw pokrewnych prawu autorskiemu w zakresie własności intelektualnej, Dz. Urz. UE L 376 z 27.12.2006, s. 28.
[551] Dyrektywa Rady nr 93/83/EWG z dnia 27 września 1993 r. w sprawie koordynacji niektórych zasad dotyczących prawa autorskiego oraz praw pokrewnych stosowanych w odniesieniu do przekazu satelitarnego oraz retransmisji drogą kablową, Dz. Urz, WE L 248 z 06.10.1993, s. 15.
[552] Dyrektywa Parlamentu Europejskiego i Rady nr 2011/77/UE z dnia 27 września 2011 r. dotycząca zmiany dyrektywy 2006/116/WE w sprawie czasu ochrony prawa autorskiego i niektórych praw pokrewnych, Dz. Urz. UE L 265 z 10.11.2011,s. 1.

informacyjnym[554], jego egzekwowania[555] czy też znaków towarowych[556]. Skupiając się jednak na przedmiocie pracy szczegółowo omówiono jedynie niektóre z nich - mające największe znaczenie w zakresie własności intelektualnej i obrotu w cyberprzestrzeni.

Dyrektywa Parlamentu Europejskiego i Rady nr 2001/29/WE z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym

Parlament Europejski przyjmując niniejszą dyrektywę planował dostosowanie prawa autorskiego i praw pokrewnych do zmian technologicznych następujących w społeczeństwie informacyjnym, a w szczególności zapewnienie wysokiego poziomu ochrony praw własności intelektualnej. Co istotne, celem dyrektywy było również wdrożenie do prawa unijnego przepisów dwóch międzynarodowych traktatów WIPO: o prawie autorskim oraz o artystycznych wykonaniach i nagraniach. Jak wskazuje Przemysław P. Polański, dyrektywa ta uzupełniła występujące wcześniej prawo unijne dotyczące praw autorskim, a w szczególności dyrektywę 91/250/EWG o ochronie programów komputerowych oraz dyrektywę 96/9/WE o ochronie baz danych[557].

Dyrektywa w art. 2 przyznaje wyłączne prawo do zezwalania lub zabraniania bezpośredniego lub pośredniego, tymczasowego lub stałego zwielokrotniania utworu, przy wykorzystaniu wszelkich środków i w jakiejkolwiek formie, w całości lub częściowo: dla autorów (w odniesieniu do ich utworów), dla artystów wykonawców (w stosunku do utrwaleń ich przedstawień), dla producentów fonogramów (w stosunku do ich fonogramów), dla producentów pierwszych utrwaleń filmu (w stosunku do oryginału i kopii tych filmów) dla organizacji radiowych i telewizyjnych (w stosunku do utrwaleń ich programów). Państwa

[553] Dyrektywa Parlamentu Europejskiego i Rady nr 96/9/WE z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych, Dz. Urz. WE L z 27.03.1996, s. 20.
[554] Dyrektywa Parlamentu Europejskiego i Rady nr 2001/29/WE z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, Dz. Urz. WE L 167 z 22.06.2001, s. 10.
[555] Dyrektywa Parlamentu Europejskiego i Rady nr 2004/48/WE z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej, Dz. Urz. WE L 157 z 30.04.2004, s 45.
[556] Dyrektywa Parlamentu Europejskiego i Rady nr 2008/95/WE z dnia 22 października 2008 r. mająca na celu zbliżenie ustawodawstw państw członkowskich odnoszących się do znaków towarowych, Dz.Urz. UE L. z 08.11.2008, s. 25.
[557] P.P. Polański, *Europejskie …*, s. 282.

członkowie UE zapewniają prawo do zabraniania lub zezwalania na jakiekolwiek publiczne udostępnianie ich utworów (art. 3). Obejmuje to podawanie do publicznej wiadomości utworów w taki sposób, aby osoby postronne miały do nich dostęp w wybranym przez siebie miejscu i czasie. Państwa członkowskie powinny przewidzieć wyłączne prawo udostępniania utworów na wymienionych powyżej polach eksploatacji.

Artykułem 4 zostały przyznane wyłączne prawa do zezwalania lub zabraniania jakiejkolwiek formy publicznego rozpowszechniania swoich utworów lub ich kopii, lecz z pewnymi wyjątkami enumeratywnie wymienionymi w artykule 5. Szczególnie istotne w zakresie niniejszych rozważań jest przyznanie ochrony prawnej przeciw obchodzeniu skutecznych zabezpieczeń technicznych obejmujący utwór lub inny przedmiot objęty ochroną (art. 6). Ochrona ta została rozciągnięta również na akty przygotowawcze takie, jak produkcja, przywóz, rozpowszechnianie, sprzedaż lub świadczenie usług względem utworów o ograniczonym zastosowaniu.

Dyrektywa 2001/29/WE doprowadziła do harmonizacji w kilku podstawowych obszarach, przede wszystkim została rozszerzona ochrona zabezpieczeń utworów oraz praw autora na wszelkie formy cyfrowej reprodukcji i dystrybucji wraz z wprowadzeniem katalogu zawierającego wyjątki od zasady. Dyrektywa w znacznym stopniu harmonizuje przepisy dotyczące publicznego udostępniania i rozpowszechniania utworów. W kolejnych latach unijna ochrona prawnoautorska była systematycznie wzmacniana przez akty prawne poruszające poszczególne problemy na przykład dyrektywa Parlamentu Europejskiego i Rady nr 2004/48/WE w sprawie egzekwowania praw własności intelektualnej[558] i inne opisane w dalszych rozważaniach pracy.

Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych[559]

Parlament Europejski stosunkowo późno, bo dopiero w 2009 roku, zdecydował się uregulować kwestię ochrony prawnej programów komputerowych. Konieczność ochrony prawnej programów komputerowych zaistniała wobec ich powszechnego wykorzystania w

[558] Dz.Urz. UE L 157, s. 45.
[559] Dz.U. L 111 z 5.5.2009, s. 16-22.

niemal każdej gałęzi przemysłu. Stwierdzono, że technologia programów komputerowych może być uznana za jeden z fundamentów rozwoju przemysłowego. Wobec tak znaczącej kwestii zdecydowano się wyjaśnić i usunąć różnice pomiędzy różnymi rodzajami ochrony prawnej dotyczącej programów komputerowych.

Artykuł 2 dyrektywy został poświęcony autorstwu programu komputerowego. Według niego autorem może być osoba fizyczna lub grupa osób, które stworzyły program, a nawet, jeżeli zezwalają na to przepisy krajowe, osoba prawna. Jeżeli program został stworzony przez grupę osób, to autorstwo przypisuje się im wszystkim wspólnie. Jeżeli twórcą programu jest pracownik w ramach wykonywania obowiązków służbowych, to wyłącznie uprawnionym do wykorzystywania praw majątkowych z programu będzie jego pracodawca.

Zgodnie z przyjętą regulacją państwa członkowskie przyznają ochronę prawem autorskim programom komputerowym, które winny być chronione tak, jak dzieła literackie w Konwencji berneńskiej o ochronie dzieł literackich i artystycznych. Beneficjentom ochrony przyznano prawa zastrzeżone (art. 4), czyli wyłączne prawo do wykonywania lub zezwalania na:

- częściowe lub całościowe, trwałe lub czasowe powielanie programu komputerowego jakimikolwiek środkami i w jakiejkolwiek formie. W zakresie, w jakim ładowanie, wyświetlanie, uruchamianie, transmitowanie lub przechowywanie programu komputerowego wymaga takiego powielenia, takie czynności wymagają uzyskania zezwolenia uprawnionego,
- translację, adaptację, porządkowanie i jakiekolwiek inne modyfikacje programu komputerowego i powielenie wyników tych działań bez uszczerbku dla praw osoby, która modyfikuje program,
- jakąkolwiek formę publicznej dystrybucji, włącznie z wypożyczeniem oryginalnego programu komputerowego lub jego kopii.

Dyrektywa w art. 6 przewiduje również regulacje na wypadek dekompilacji programu. Zgoda uprawnionego nie jest wymagana, jeżeli powielanie kodu i translacja jego formy są niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego z innymi programami, pod warunkiem, że są spełnione następujące warunki:

- czynności te są wykonywane przez licencjobiorcę lub inną osobę mającą prawo do używania kopii programu,

- informacje niezbędne do osiągnięcia współdziałania nie były uprzednio łatwo dostępne,
- czynności te są ograniczone do tych części oryginalnego programu, które są niezbędne w celu osiągnięcia interoperacyjności.

Unijne prawo autorskie dotyczące programów komputerowych należy uznać jedynie za częściową regulację, ponieważ objęło podstawowe uprawnienia i ich ograniczenia. Podnosi się często, iż brak jest unifikacji w zakresie obrotu prawami majątkowymi (w tym programów komputerowych). Z tych też względów, przy rozróżnieniu sprzedaży oprogramowania i jego licencjowaniem w prawie europejskim należy uwzględnić, że dotyczy ono wyłącznie interpretacji przesłanek wyczerpania prawa[560]. W prawie Unii Europejskiej odrzucono zasadę patentowej ochrony programów komputerowych oraz modelu *sui generis* zaproponowane przez WIPO[561].

Komunikaty

Jako przykłady inicjatyw podejmowanych przez Unię Europejską można wymienić wiele komunikatów Komisji Europejskiej poruszających problem szeroko rozumianej cyberprzestrzeni:

1. Komunikat Komisji Europejskiej z dnia 26 stycznia 2001 r. tworzenie bezpieczniejszego społeczeństwa informacyjnego poprzez zwiększenie bezpieczeństwa struktur informacyjnych i zwalczanie przestępstw związanych z komputerem poruszał kwestię przestępczości komputerowej oraz konieczności podjęcia działań w celu ochrony integralności, dostępności i niezawodności systemów komputerowych. Uzupełnieniem wspomnianego aktu był komunikat bezpieczeństwo sieci i informacji z 2001 roku, który wyszczególniał problemy związane z bezpieczeństwem sieci oraz wprowadzał propozycję działań w przeciwdziałaniu temu zjawisku. Zaakcentowano w nim potrzebę harmonizacji przepisów materialnoprawnych państw członkowskich[562].

[560] Z. Okoń, *Licencja czy sprzedaż? Wyczerpanie prawa dystrybucji programów komputerowych w prawie* UE, [w:] K. Flaga - Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016, s. 324.
[561] A. Nowicka, *Prawnoautorska ochrona programów komputerowych - regulacja polska i jej unijny wzorzec w świetle orzecznictwa Trybunału Sprawiedliwości*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2015, t. 78, z. 2, s. 105.
[562] M. Siwicki, *Cyberprzestępczość* …, s. 39.

2. Komunikat Komisji z dnia 10 maja 2005 r. Program haski: dziesięć priorytetów na najbliższe pięć lat. Partnerstwo na rzecz odnowy europejskiej w dziedzinie wolności, bezpieczeństwa i sprawiedliwości[563] dotyczył między innymi możliwości wydania zalecenia co do minimalnych standardów pozyskiwania i wymiany elektronicznego materiału dowodowego, prywatności i ochrony danych, zwalczania przestępczości zorganizowanej.
3. Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 31 maja 2006 r. Strategia na rzecz bezpieczeństwa społeczeństwa informacyjnego - Dialog, partnerstwo i przejmowanie inicjatywy[564] dotyczy wyzwań związanych z bezpieczeństwem sieci i systemów informatycznych w UE, współpracy z sektorem prywatnym oraz Europejską Agencją do spraw Bezpieczeństwa Sieci i Informacji. Jako główne wyzwania wskazano ataki na systemy informatyczne, coraz częstsze użycie urządzeń mobilnych oraz wzrost świadomości użytkowników o możliwych zagrożeniach.

4. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22 maja 2007 r. w kierunku ogólnej strategii zwalczania cyberprzestępczości[565] wzywa do zwiększenia współpracy między organami ścigania oraz między państwami członkowskimi, harmonizacji przepisów karnych dotyczących cyberprzestępczości, prowadzenia politycznej i prawnej kooperacji z państwami trzecimi oraz sektorem prywatnym, podnoszenia świadomości, prowadzenia badań i szkoleń. Ponadto, zwalczanie cyberprzestępczości powinno polegać na:
    - „prowadzeniu szczegółowych badań w celu przygotowania specjalnego aktu prawnego UE dotyczącego kradzieży tożsamości,
    - rozwijaniu metod i procedur technicznych służących zwalczaniu oszustw i nielegalnego handlu w Internecie,
    - wzmacnianiu działań w konkretnych dziedzinach, takich jak: zwalczanie nadużyć finansowych w sieciach łączności elektronicznej, w tym szczególności związanych z użyciem bezgotówkowych środków pieniężnych”.[566]

[563] COM(2005)0184.
[564] COM(2006)0251.
[565] COM(2007)0267.
[566] M. Siwicki, *Cyberprzestępczość* …, s. 40.

5. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 30 marca 2009 r. w sprawie ochrony krytycznej infrastruktury informatycznej. Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności[567] dotyczy zagrożeń krytycznych struktur informatycznych, sposobów ich ochrony, wzmocnienia współpracy pomiędzy państwami członkowskimi, państwami trzecimi oraz z sektorem publicznym, zwłaszcza w zakresie partnerstwa publiczno-prywatnego. Stwierdzono, że można ograniczyć ataki cybernetyczne za pomocą środków zapobiegawczych oraz skoordynowanych działań w trakcie kryzysu. Zwalczanie zagrożeń będzie więc łatwiejsze w przypadku opracowania usystematyzowanej wymiany informacji i dobrych praktyk. W tym celu zaproponowano pięć filarów: gotowość na wszystkich szczeblach, zapewnienie mechanizmów wczesnego ostrzegania, wzmocnienie unijnych mechanizmów obronnych dla krytycznej infrastruktury informatycznej, propagowanie priorytetów UE na arenie międzynarodowej oraz wspieranie wdrażania dyrektywy Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej.
6. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 19 maja 2010 r. zatytułowany Europejska agenda cyfrowa[568]. Europejska agenda cyfrowa przedstawiona przez Komisję Europejską jest jednym z siedmiu filarów strategii Europa 2020, ustalającej cele dla wzrostu UE do 2020 roku. Celem agendy jest rozwój jednolitego rynku cyfrowego opartego na szybkim Internecie i interoperacyjnych aplikacjach. W agendzie określono siedem priorytetowych obszarów działania:
    - stworzenie jednolitego rynku cyfrowego przez uproszczenie udostępniania i zarządzania prawami autorskimi, ułatwienie elektronicznych płatności i fakturowania poprzez utworzenie Jednolitego Europejskiego Obszaru Płatniczego (SEPA),
    - poprawę warunków ramowych dla interoperacyjnosci między produktami i usługami technologii informacyjno - komunikacyjnych,

[567] COM(2009)0149.
[568] COM(2010) 245.

- zwiększenie zaufania do Internetu i bezpieczeństwa prowadzonych w nim operacji przez walkę z cyberprzestępczością, pornografią dziecięcą, naruszeniem prywatności i danych osobowych,
- zapewnienie dostępu do szybkiego i bardzo szybkiego Internetu - dostarczanie ogólnodostępnego i szybkiego Internetu powinno nastąpić za pomocą łączy szerokopasmowych,
- wzrost nakładów na badania i rozwój technologii informacyjno - komunikacyjnych,
- rozwój umiejętności wykorzystania technologii cyfrowych i wyłączenia społecznego,
- wykorzystanie technologii informacyjno - komunikacyjnych w celu sprostania wyzwaniom stojącym przed społeczeństwem takimi, jak zmiana klimatu, wzrost kosztów leczenia i starzenie się społeczeństwa.

7. Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 22 listopada 2010 r. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpiecznej Europy na lata 2010-2014[569] określa 5 obszarów priorytetowych:
   - rozbijanie międzynarodowych siatek przestępczych – czyli wykrywanie i rozbijanie przestępczości zorganizowanej oraz ochrona gospodarki przez infiltracją przestępczą między innymi korupcją,
   - zwalczanie terroryzmu - walka z radykalizacją postaw i werbowania terrorystów, odcięcie terrorystów od źródeł finansowania, ochrona transportu morskiego i powietrznego,
   - podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni - budowa zdolności w zakresie egzekwowania prawa i sądownictwa, współpraca pomiędzy sektorem publicznym i prywatnym na rzecz ochrony infrastruktury informatycznej, poprawa skuteczności zapobiegania atakom i zakłóceniom cybernetycznym,
   - poprawa bezpieczeństwa przez zarządzanie granicami - wzmocnienie zarządzanie zewnętrznymi granicami UE, wspólne zarządzenie ryzykiem w odniesieniu do przepływu towarów przez zewnętrzne granice UE,
   - zwiększanie odporności na klęski żywiołowe i katastrofy spowodowane przez człowieka.

[569] COM(2010)0673.

8. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 31 marca 2011 r. w sprawie ochrony krytycznej infrastruktury informatycznej. Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni[570] - mimo sukcesów w zakresie ochrony krytycznej infrastruktury teleinformatycznej konieczna jest dalsza praca nad poprawą bezpieczeństwa cyberprzestrzeni. Wzrost bezpieczeństwa sieci ma nastąpić przez budowę strategicznego partnerstwa międzynarodowego, zwiększenia zaufania do chmur obliczeniowych oraz utworzenia w UE sprawnie funkcjonujących krajowych lub rządowych CERT.
9. Komunikat Komisji do Rady i Parlamentu Europejskiego z dnia 28 marca 2012 r. w sprawie zwalczania przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością[571], komunikatem tym powołano Europejskie Centrum do spraw Walki z Cyberprzestępczością[*].
10. Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 7 lutego 2013 r. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń[572]. Zbudowanie bezpieczeństwa cybernetycznego Unia Europejska postanowiła oprzeć na pięciu strategicznych priorytetach. Są nimi:
    - osiągnięcie odporności na zagrożenia cybernetyczne między innymi przez współpracę sektora publicznego i prywatnego, wymianę informacji o incydentach dotyczących bezpieczeństwa sieci i danych oraz partnerstwo publiczno-prywatne,
    - radykalne ograniczenie cyberprzestępczości przez zalecenie ratyfikacji konwencji RE o cyberprzestępczości, zacieśnienie współpracy organów ścigania państw członkowskich oraz Eurojustu i Europejskiego Centrum do spraw Walki z Cyberprzestępczością,
    - opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i ochrony (WPBiO) przez ocenę wymogów operacyjnych, wspieranie rozwoju unijnych zdolności i technologii oraz opracowanie ram politycznych w zakresie obrony cybernetycznej w UE,

[570] KOM(2011)163.
[571] COM(2012)0140.
[*] Więcej o Europejskim Centrum do spraw Walki z Cyberprzestępczością w podrozdziale 3.1.4.3.
[572] JOIN(2013)01.

- rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego przez stymulację ogólnoeuropejskiego popytu rynkowego na produkty i technologie o wysokim poziomie bezpieczeństwa, opracowywanie norm bezpieczeństwa oraz wspieranie inwestycji w badania, rozwój i innowację,
- ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie wartości europejskich, czyli promowanie cyberprzestrzeni jako obszaru wolności i przestrzegania praw podstawowych,

11. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 11 marca 2014 r. Otwarta i bezpieczna Europa: realizacja założeń[573] ocenia pozytywnie funkcjonowanie Europejskiego Centrum do spraw Walki z Cyberprzestępczością w pierwszym roku działalności i zapowiada dalszy jego rozwój oraz stworzenie rozwiązań na poziomie globalnym zaczynając od utworzenia przez UE i USA światowego sojuszu przeciwko niegodziwemu traktowaniu dzieci w cyberprzestrzeni w celach seksualnych.
12. W komunikacie Komisji do Parlamentu Europejskiego i Rady z dnia 20 czerwca 2014 r. Sprawozdanie końcowe z realizacji strategii bezpieczeństwa wewnętrznego UE w latach 2010-2014[574] jako pozytywną realizację programu w zakresie cyberprzestępczości wskazano wysoką świadomość europejskich użytkowników sieci na temat zagrożeń w cyberprzestrzeni, unifikację prawa karnego państw członkowskich przez przyjęcie dyrektywy dotyczącej ataków na systemy informatyczne, powołanie Europejskiego Centrum do spraw Walki z Cyberprzestępczością przy biurze Europolu oraz zainicjowania sojuszu z USA w sprawie niegodziwego traktowania dzieci w Internecie w celach seksualnych, dzięki któremu państwa dążą do lepszego identyfikowania ofiar, skutecznego ścigania sprawców oraz ograniczenia pornografii dziecięcej w Internecie.

[573] COM(2014)0154.
[574] COM(2014)0365.

Badania i projekty

Oprócz wymienionych powyżej inicjatyw prawnych, Unia Europejska finansuje badania w zakresie ogólno pojętej cyberprzestrzeni. Wśród najważniejszych wymienić można następujące projekty:

1. **FORWARD** - projekt *Managing emerging threats in ICT Infrastructures*, realizowany w latach 2008-2009. Projekt miał na celu wspieranie współpracy i koordynacji badań z dzieciny cyberbezpieczeństwa, ochrony przed cyberzagrożeniami[575].
2. **WOMBAT**[576] - projekt *Worldwide Observatory of Malicious Behaviours and Attack Threats* realizowany był w ramach 7 Programu Ramowego w latach 2008-2010. Celem projektu było podjęcie kroków mających na celu zrozumienie pojawiających się nowych zagrożeń związanych z gospodarką Internetu i jego użytkowników[577].
3. **COMIFIN**[578] - projekt *Communication Middleware for monitoring Financial Critical Infrastructures*, realizowany w latach 2008-2011. Projekt miał na celu wspieranie ciągłości działań podejmowanych w sferze finansów, ochrony krytycznej infrastruktury finansowej zarówno w razie awarii jak i celowych naruszeń[579].
4. **Cybercrime@IPA**[580] - wspólny projekt UE i Rady Europy, realizowany od 1 listopada 2010 roku do 30 kwietnia 2013 roku. Projekt miał na celu wzmocnienie współpracy organów sądowych w zakresie zwalczania cyberprzestępczości w południowo-wschodniej Europie w ramach Konwencji o cyberprzestępczości. Krajami które brały udział w projekcie były: Albania, Bośnia i Hercegowina, Chorwacja, Czarnogóra, Macedonia, Serbia, Turcja i Kosowo[581].
5. **ETCETERA**[582] - projekt *Evaluation of critical and emerging technologies for the elaboration of a security research agenda*, realizowany od września 2011 roku. do listopada 2013 roku. Badania projektu miały na celu przyczynić się do wzrostu

[575] J. Kosiński, *Paradygmaty …*, s. 228.
[576]Projekt WOMBAT: http://www.wombat-project.eu/ [12.06.2015].
[577] J. Kosiński, *Paradygmaty …*, s. 228-229.
[578] Projekt COMIFIN: http://www.tssg.org/projects/comifin/ [12.06.2015].
[579] J. Kosiński, *Paradygmaty …*, s. 229.
[580]Projekt Cybercrime@IPA: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp [12.06.2015].
[581] J. Kosiński, *Paradygmaty …*, s. 229.
[582] Projekt ETCETERA: http://www.etcetera-project.eu/ [12.06.2015].

bezpieczeństwa europejskiego przez rozwój krytycznych i nowych technologii w dziedzinie bezpieczeństwa[583].

6. **BIC**[584] - projekt *Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services*, realizowany od stycznia 2011 roku do grudnia 2013 roku. Celem projektu było poszerzenie współpracy naukowej pomiędzy UE a partnerami z krajów reprezentujących wschodzące gospodarki o wysokim potencjale wzrostu ICT, czyli RPA, Brazylią czy Indiami[585].
7. **NISHA**[586] - *Network for Information Sharing and Alerting* - sieć wymiany informacji i alarmowania. Projekt realizowany był od stycznia 2012 roku do lutego 2014 roku przez czterech partnerów: PTA/CERT - Węgry, FCCN/CERT Portugalia, Uniwersytet w Gelsenkirchen/ Institute for Internet Security oraz NASK/CERT Polska[587].
8. **Cyberterrorism Project**[588] - celem projektu realizowanego w latach 2012-2014 było wyjaśnienie zagadnienia cyberterroryzmu, zagrożeń z nim związanych oraz przeprowadzenie prognoz na temat potencjalnych celów terrorystów[589].
9. **CAPITAL**[590] - projekt *Cybersecurity reaserch Agenda for Privacy and Technology challenges*, realizowany od października 2013 roku do września 2015 roku. Celami projektu jest wybór kluczowych dziedzin społecznych i technologicznych, które są zagrożone naruszeniami cyberbezpieczeństwa i prywatności, następnie określenie, jak ICT[591] może zminimalizować lub zlikwidować całkowicie zagrożenia[592].
10. **ILLBuster**[593] - projekt finansowany przez Komisję Europejską w ramach programu „*Zapobieganie i zwalczanie przestępczości*". Celem programu jest opracowanie zintegrowanego półautomatycznego systemu informacji pomocnego dla wykrywania nielegalnych działań w Internecie, czyli szkodliwych domen internetowych, pornografii dziecięcej, złośliwego oprogramowania. Liderem projektu, który

[583] J. Kosiński, *Paradygmaty …*, s. 229.
[584] Projekt BIC: http://www.bic-trust.eu/ [12.06.2015].
[585] J. Kosiński, *Paradygmaty …*, s. 229-230.
[586] Projekt NISHA: http://nisha-network.eu/ [12.06.2015].
[587] J. Kosiński, *Paradygmaty …*, s. 230.
[588] Cyberterrorism Project: http://www.cyberterrorism-project.org/ [12.06.2015].
[589] J. Kosiński, *Paradygmaty …*, s. 230.
[590] Projekt CAPITAL: http://www.capital-agenda.eu/default.aspx?page=home [12.06.2015].
[591] ICT - ang. *Information and Communication Technologies* -technologie informacyjno - komunikacyjne, rozumiane jako wszelkie media komunikacyjne tj. Internet, sieci bezprzewodowe, sieć komórkowa satelitarna.
[592] Projekt CAPITAL: http://www.capital-agenda.eu/default.aspx?page=home [12.06.2015].
[593] Projekt ILLBuster: http://illbuster-project.eu/ [12.06.2015].

rozpoczął swą działalność w lutym 2014 roku i ma trwać 24 miesiące jest PRA LAB Uniwersytetu w Caglari[594].

11. **SISSDEN[595]** - projekt ma na celu poprawę cyberbezpieczeństwa europejskich instytucji i użytkowników. Sieć oparta zostanie na ogólnoświatowej sieci sond, utworzonych i utrzymywanych przez konsorcjum. Projekt zakłada analizę złośliwego oprogramowania, która będzie następnie wykorzystywana do przeciwdziałania atakom[596].
12. **Siódmy Projekt Ramowy NECOMA** - projekt finansowany przez Projekt Badań i Rozwoju Ministerstwa Spraw Wewnętrznych i Komunikacji Japonii oraz Siódmy Program Ramowy UE. Projekt ma na celu zbieranie danych o zagrożeniach, ich analizę oraz proponowanie nowych mechanizmów obrony[597].

3.1.3. Regulacje organizacji wyspecjalizowanych

3.1.3.1 Dorobek Sojuszu Północnoatlantyckiego

Sojusz Północnoatlantycki (ang. *North Atlantic Treaty Organization* - NATO) dostrzegając liczne zagrożenia, które mogą mieć miejsce w cyberprzestrzeni w 2002 roku na szczycie w Pradze przyjął program ochrony cybernetycznej (ang. *Cyber Defense Program*). Konieczność zapewnienia dodatkowej ochrony dla systemów informacyjnych i komunikacyjnych była również akcentowana w czasie szczytu w Rydze w 2006 roku. Dopiero cyberataki na estońskie instytucje publiczne i prywatne, przeprowadzone w kwietniu i maju 2007 roku, pokazały, że należy rozpocząć w trybie pilnym prace nad opracowaniem polityki cyberbezpieczeństwa Sojuszu. W rezultacie NATO, w styczniu 2008 roku, zatwierdziło pierwszą politykę cyberbezpieczeństwa (ang. *Cyber Defence Policy*). Jest to istotne, ponieważ kolejne cyberataki, które miały miejsce w czasie konfliktu pomiędzy Rosją

[594] J. Kosiński, *Paradygmaty …*, s. 231.
[595] Projekt SISSDEN: https://sissden.eu/ [10.03.2017].
[596] Ibidem.
[597] Dane z oficjalnej strony internetowej Projektu NECOMA: http://www.necoma-project.eu/ [10.03.2017].

i Gruzją ukazały, iż ataki cybernetyczne mogą w przyszłości stać się głównym składnikiem konwencjonalnych działań wojennych[598].

Na szczycie mającym miejsce 19-20 listopada 2010 roku w Lizbonie przyjęto Koncepcję Strategiczną NATO, która ma obowiązywać przez 10 kolejnych lat. NATO przyjęło za cel zwalczanie cyberterroryzmu za pomocą działań militarnych i politycznych. Punkt 12 Koncepcji Strategicznej zwraca uwagę, że „Ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej; mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy eksternistyczne”[599].

Postanowienia Koncepcji Strategicznej stanowią, że NATO będzie rozwijać możliwości zapobiegania, wykrywania, obrony przed atakami cybernetycznymi oraz przywracania zdolności systemów w przypadku nastąpienia ataku, w tym wykorzystując proces planowania Sojuszu na rzecz wzmocnienia i koordynacji narodowych zdolności w dziedzinie obrony cybernetycznej. By osiągnąć ten cel postanowiono włączyć instytucje NATO w scentralizowany system ochrony cybernetycznej oraz zintegrować system monitorowania, ostrzegania i reagowania cybernetycznego NATO z państwami członkowskimi (art. 19).

W trakcie Szczytu, który odbył się w 2014 roku w Walii, stwierdzono, że podstawowym zadaniem cyberobrony NATO jest ochrona własnych sieci oraz współpraca w celu opracowania efektywnych procesów ochrony sieci członków NATO. Podkreślono, że cyberataki mogą zagrażać narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Ponadto, ataki takie mają negatywny wpływ na nowoczesne społeczeństwa informacyjne. Zobowiązano się do dalszego rozwoju zdolności obronnych, ścisłej współpracy

[598] Dane z oficjalnej strony internetowej NATO
: http://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en [01.08.2015].
[599] Dane z oficjalnej strony internetowej Biura Bezpieczeństwa Narodowego RP:
https://www.bbn.gov.pl/pl/wydarzenia/2694,KoncepcjaStrategicznaNATOtlumaczenie.html [25.06.2015].

dwustronnej oraz międzynarodowej w celu zwiększenia zdolności cyberobronnych Sojuszu oraz planowania operacyjnego i awaryjnego[600].

W Warszawie 8-9 lipca 2016 roku odbył się kolejny szczyt NATO. Jeszcze przed odbyciem szczytu Sekretarz Generalny NATO Jens Stoltenberg uznał, że odbędzie się on w kluczowym dla NATO momencie - największego nasilenia euroatlantyckiej obrony od czasów zakończenia zimnej wojny. Podkreślono, iż zagrożenia w cyberprzestrzeni, czyli cyberataki potencjalnie mogą być uznane za naruszenie art. 5 Traktatu Północnoatlantyckiego[601]. Stoltenberg podkreślił, że kluczową częścią strategii przeciwdziałania zagrożeniem hybrydowym jest właśnie cyberbezpieczeństwo[602].

W trakcie warszawskiego szczytu sporządzono deklarację cyberbezpieczeństwa (*Cyber Defence Pledge*). W punktach 1-4 stwierdzono, iż w szybko zmieniającym się krajobrazie cyberzagrożeń NATO musi podjąć odpowiednie kroki w celu ochrony Sojuszu w cyberprzestrzeni w takim samym zakresie, jak w obronie na lądzie, wodzie i w przestrzeni powietrznej. Potwierdzono walijską Politykę Cyberobrony, przyjętą w celu wzmocnienia cyberochrony infrastruktury i krytycznej i sieci krajowych. Szczególną wagę przyznano współpracy Sojuszu z Unią Europejską, ponieważ przyczynia się ona do wzmocnienia odporności regionu euroatlantyckiego. Dokument potwierdza stosowanie prawa międzynarodowego w cyberprzestrzeni, uznaje prace poczynione w innych organizacjach międzynarodowych oraz podkreśla zalety partnerstwa NATO z państwami sprzymierzonymi, środowiskiem akademickimi i przedstawicielami przemysłu. Równocześnie zaakcentowano potrzebę ułatwiania współpracy w zakresie ochrony cybernetycznej, w tym za pośrednictwem międzynarodowych projektów, edukacji, szkoleń, wymiany informacji w celu wspierania krajowych wysiłków obronny cybernetycznej. Dokument zapewnia, iż Sojusz jest

[600] NATO Summit Declaration: dostępne na oficjalnej stronie internetowej NATO: http://www.nato.int/cps/en/natohq/official_texts_112964.htm [27.10.2016].

[601] Art 5 - Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi, to każda z nich, w ramach wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy artykułu 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie jak i w porozumieniu z innymi Stronami, działania, jakie uzna za konieczne, łącznie z użyciem siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego. O każdej takiej zbrojnej napaści i o wszystkich podjętych w jej wyniku środkach zostanie bezzwłocznie powiadomiona Rada Bezpieczeństwa. Środki takie zostaną zaniechane, gdy tylko Rada Bezpieczeństwa podejmie działania konieczne do przywrócenia i utrzymania międzynarodowego pokoju i bezpieczeństwa. Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. z 2000 r., nr 87, poz. 970).

[602] Wystąpienie Sekretarza Generalnego NATO Jensa Stoltenberga z dnia 25 marca 2015 r. http://www.nato.int/cps/en/natohq/opinions_118435.htm?selectedLocale=en [19.01.2016].

cyberświadomy (ang. *cyber aware*), cyberwyszkolony (ang. *cyber trained*), cyberbezpieczny (ang. *cyber secure*) i cyberaktywny (ang. *cyber enabled*)[603].

Sojusz Północnoatlantycki za priorytet uznał wzmocnienie i zwiększenie cyberobrony sieci narodowych oraz cyber - infrastruktury. Założono w pkt. 5, że w ramach długoterminowego wdrażania cyberobrony NATO będzie:

- opracowywać najpełniejszą gamę możliwości, aby bronić infrastruktury i sieci krajowe - oznacza to stosowanie cyberobrony na najwyższym strategicznym poziomie wraz z organizacjami Sojuszu odpowiedzialnymi za obronność,
- przeznaczać odpowiednie środki, na szczeblu krajowym, w celu wzmocnienia zdolności cyberobronnych. NATO uznało, że jest odpowiedzialne za obronę swoich własnych sieci,
- wzmacniać interakcję wśród odpowiednich organów krajowych odpowiedzialnych za cyberobronę w celu pogłębienia współpracy i wymiany najlepszych praktyk,
- pogłębiać analizę problemu cyberzagrożeń, w tym przez wymianę doświadczeń informacji i ocen,
- zwiększać kwalifikację i świadomość zagrożeń wśród wszystkich zainteresowanych stron. Zwiększenie ochrony na poziomie krajowym z minimalnych standardów do najbardziej wyrafinowanych i solidnych metod ochrony cyberprzestrzeni,
- promować cyberedukację, szkolenia, wykorzystywanie sił do zwiększenia świadomości, budowania wiedzy i zaufania w Sojuszu,
- przyśpieszać realizację uzgodnionych cybernetycznych zobowiązań obronnych, w tym w systemach krajowych państw członkowskich NATO.

NATO słusznie zauważyło, że zarówno państwa, jak i podmioty pozapaństwowe mogą używać cyberataków w swoich operacjach militarnych. W świetle ostatnich wydarzeń cyberakatki mogą być uznane za część wojny hybrydowej. NATO i jego sojusznicy uznają, że ochrona cyberprzestrzeni jest podstawowym zadaniem Sojuszu, zbiorowej obrony, zarządzania kryzysowego oraz kooperacyjnego bezpieczeństwa. Uznaje się, że Sojusz musi być przygotowany do obrony swoich sieci oraz winien posiadać narzędzia do działania przeciwko coraz większej ilości cyberzagrożeń skierowanych bezpośrednio przeciwko członkom NATO. W komunikacie z warszawskiego szczytu (*Warsaw Summit Communiqué*)

[603] Cyber Defence Plagde dostępny na oficjalnej stronie NATO: https://nato.usmission.gov/cyber-defense-pledge/ [24.10.2016].

podkreślono, że Sojusz stoi przed szeregiem wyzwań i zagrożeń, które pochodzą zarówno od wschodu jak i południa, od sił państwowych i niepaństwowych, od sił militarnych, organizacji terrorystycznych, a NATO narażone jest na ataki cybernetyczne i hybrydowe. Obok cyberbezpieczeństwa, jako główne zagrożenia zostały wskazane ekspansja agresji Rosji, organizacja ISIS, kryzys migracyjny oraz pogorszająca się sytuacja na Bliskim Wschodzie i w Północnej Afryce[604].

Polityka cyberbezpieczeństwa NATO jest realizowana przez władze polityczne, wojskowe i techniczne oraz poszczególnych członków Sojuszu. Komitet Cyberbezpieczeństwa (ang. *The Cyber Defence Committee*) jest organem podporządkowanym Radzie Północnoatlantyckiej. Na szczeblu roboczym funkcjonuje urząd NATO do spraw Zarządzania Cyberobroną - *The Cyber Defence Management Board* (CDMB). Urząd jest odpowiedzialny za koordynację cyberobrony Sojuszu Północnoatlantyckiego. W jego skład wchodzą przedstawiciele wszystkich głównych organów zainteresowanych cyberbezpieczeństwem, czyli *Allied Command Operations* (ACO), Allied *Command Transformation* (ACT) oraz innych agend NATO[605].

Kolejnym organem NATO jest *Cooperative Cyber Defence Centre of Excellence* (CCD COE) - Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi w Tallinie. Siedziba Centrum jest nieprzypadkowa. W 2007 roku Estonia stała się ofiarą ataków hakerów, którzy zaatakowali serwery i strony rządowe, strony banków, narodowych serwisów internetowych oraz niektórych dostawców usług internetowych i telekomunikacyjnych. Ataki zostały przeprowadzone przez rosyjskich hakerów w odpowiedzi na przeniesienie z centrum miasta pamiętnika upamiętniającego żołnierzy Armii Czerwonej[606]. Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi zostało utworzone 14 maja 2008 roku. Ma ono akredytację NATO w strukturze sił Sojuszu Północnoatlantyckiego jednakże nie wchodzi w skład struktur dowodzenia NATO, stąd finansowanie następuje spoza budżetu Sojuszu[607]. CCD COE zajmuje się badaniami, szkoleniami, konsultacjami oraz prowadzeniem badań i wymianą doświadczeń w zakresie cyberbezpieczeństwa.

---

[604] Tekst Warsaw Summit Communiqué dostępny na oficjalnej stronie NATO: https://nato.usmission.gov/warsaw-summit-communique/ [24.10.2016].

[605] Dane z oficjalnej strony internetowej Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi https://ccdcoe.org/nato.html [26.06.2015].

[606] J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] M. Górka (red.) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa 2004, s. 210.

[607] Ibidem, s 214.

3.1.3.3. Dorobek Europejskiej Agencji Bezpieczeństwa Sieci i Informacji

Europejska Agencja Bezpieczeństwa Sieci i Informacji - ENISA[608] została powołana do życia 15 marca 2004 roku na mocy rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 460/2004[609]. Obecnie podstawą prawną działania Agencji jest rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004[610]. Agencja ma swoją siedzibę w Heraklionie w Grecji.

Celem działania ENISA, wyrażonym w art. 1 jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji w UE zwiększanie poziomu wiedzy oraz promowanie kultury bezpieczeństwa (w tym cyberbezpieczeństwa). Działalność Agencji skupia się na doradztwie i wspieraniu Komisji oraz państw członkowskich w zakresie bezpieczeństwa informacji, sprzętu i oprogramowania, gromadzenia i analizowania danych na temat incydentów i zagrożeń związanych z bezpieczeństwem danych, podnoszenia świadomości i inicjowania współpracy między różnymi podmiotami w dziedzinie bezpieczeństwa informacji, w szczególności poprzez rozwój partnerstw publiczno - prywatnych[611].

Zgodnie z art. 3 rozporządzenia nr 526/2013 Agencja wykonuje następujące zadania:

- wspieranie opracowywania prawa i polityki UE przez pomoc i doradztwo, przygotowywania analiz i strategii,
- wspieranie budowania potencjału przez wspieranie państw członkowskich i instytucji, organizacji i urzędów UE w zakresie bezpieczeństwa informacji i sieci,
- wspieranie współpracy między organami publicznymi i prywatnymi, w tym uniwersytetami i ośrodkami badawczymi w UE oraz zwiększanie świadomości przez promowanie współpracy między zespołami CERT, wymianę najlepszych praktyk,

[608] ENISA - ang. *European Network and Information Security Agency.*
[609] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji. Aktem pranym obecnie regulującym kwestię działalności ENISA jest Rozporządzenie (UE) nr 526/2013 Parlamentu Europejskiego i Rady z 21 maja 2013 r. uchylające rozporządzenie (WE) nr 460/2004.
[610] Dz.Urz. L 165 z 18.06.2013,
[611] Dane z oficjalnej strony internetowej ENISA: https://www.enisa.europa.eu/about-enisa/activities [15.06.2015].

- wspieranie badań naukowych przez ułatwianie tworzenia europejskich i międzynarodowych norm związanych z zarządzeniem ryzykiem, bezpieczeństwem sieci, produktów, systemów i usług elektronicznych,
- współpracę z instytucjami zajmującymi się cyberprzestępczością, ochroną danych osobowych i ochroną prywatności.

ENISA zajmuje sie takimi problemami, jak przechowywanie danych w chmurze, czy też kwestiami związanymi z infrastrukturą krytyczną, zarządzaniem kryzysowym w przypadku wystąpienia cyberincydentów, edukacji w kwestii cyberbezpieczeństwa, ochrony danych czy też stałego monitorowania występujących w sieci incydentów[612].

W 2016 roku ENISA wydała dokument o nazwie Strategia Europejskiej Agencji Bezpieczeństwa Sieci i Informacji na lata 2016-2020 (*ENISA Strategy 2016-2020*). Uznano, że ENISA we współpracy i wsparciu z państwami członkowskimi i instytucjami UE będzie w pierwszej kolejności dążyć do osiągnięcia:

- doświadczenia (ang. *expertise*) - wspieranie Europy w obliczu pojawiających się problemów bezpieczeństwa sieci i informacji, przez zestawianie, analizowanie i udostępnianie informacji i wiedzy na temat kluczowych zagadnień dotyczących bezpieczeństwa sieci i informacji, które mogą potencjalnie wpłynąć na Unię Europejską biorąc pod uwagę szybką ewolucję środowiska cyfrowego,
- polityki (ang. *policy*) - promowanie bezpieczeństwa sieci i informacji, jako priorytet polityki UE przez wspieranie unijnych instytucji i państw członkowskich w opracowywaniu i wdrażaniu polityki i prawa Unii Europejskiej związanej z bezpieczeństwem sieci i informacji,
- potencjału wykonawczego (ang. *capacity*) - modelowanie rozwoju Europy do osiągnięcia najwyższego poziomu bezpieczeństwa sieci przez wspieranie państw członkowskich w budowaniu ich potencjału bezpieczeństwa sieci i informacji,
- społeczności (ang. *community*) wspieranie rozwoju bezpieczeństwa sieci i informacji poprzez intensyfikację współpracy na szczeblu UE między państwami członkowskimi, instytucjami unijnymi oraz stronami zainteresowanymi bezpieczeństwem sieci i informacji w tym, w sektorze prywatnym,

[612] Dane z oficjalnej strony internetowej ENISA: https://www.enisa.europa.eu/topics [29.10.2016].

- rozwoju umiejętności (ang. *enabling*) - wzmocnienie wpływu ENISA przez poprawę zarządzania jego zasobami oraz efektywniejsze angażowanie podmiotów, w tym państw członkowskich i instytucji unijnych, także na poziomie międzynarodowym[613].

Grupa Robocza do spraw Cyberbezpieczeństwa i Cyberprzestępczości

W ramach ENISA funkcjonuje Grupa Robocza do spraw Cyberbezpieczeństwa i Cyberprzestępczości (ang. *EU-US Working Group on Cyber security and Cyber Crime*). Została ona powołana podczas szczytu Unia Europejska - Stany Zjednoczone w Lizbonie w 2010 roku. Zadaniem grupy jest rozwój cyberbezpieczeństwa w szerokim tego słowa znaczeniu oraz zwalczanie przestępczości popełnianej przy użyciu systemów komputerowych. Grupa postawiła sobie również za cel pogłębienie i poszerzenie współpracy wynikającej z Konwencji Rady Europy o cyberprzestępczości. Ma to nastąpić przez nakłonienie państw członkowskich Unii Europejskiej do przystąpienia do Konwencji oraz promowanie standardów w niej zawartych wśród państw spoza regionu. Po pierwszym spotkaniu Grupy w 2011 roku do jej zadań dodano walkę z cyberatakami na wielką skalę, ponieważ Konwencja w okresie jej powstania nie przewidywała rozwoju tego trendu[614].

3.1.3.4. Dorobek Organizacji Współpracy Gospodarczej i Rozwoju

Organizacja Współpracy Gospodarczej i Rozwoju (*Organisation for Economic Co-operation and Development* - OECD) jako jedna z pierwszych zauważyła potrzebę dyskusji i podjęcia prac nad zagadnieniem karalności nadużyć komputerowych. W 1981 roku wraz z rządem Hiszpanii zorganizowano seminarium na temat społecznych zagrożeń związanych z komputeryzacją. W OECD w 1983 roku rozpoczęto badania nad możliwością wprowadzenia norm międzynarodowego prawa karnego w zakresie cyberprzestępczości. Wynikiem prac była publikacja w 1985 roku raportu *Przestępstwa związane z komputerem: Analiza polityki*

[613] ENISA Stategy 2016-2020, Heraklion 2016, s. 9-15.
[614] J. Kosiński, *Paradygmaty* ..., s. 228.

legislacyjnej (ang. *Computer - Related Crime: Analysis of Legal Policy*), w którym przeanalizowano ustawodawstwa poszczególnych państw członkowskich oraz zaproponowano odpowiednie zmiany legislacyjne. Raport zawierał także listę pięciu kategorii czynów popełnianych za pomocą komputera, które powinny być uznane za karane. Zaliczono do nich: oszustwo komputerowe, fałszerstwo komputerowe, uzyskanie nielegalnego dostępu do systemu komputerowego, sabotaż komputerowy oraz nielegalne kopiowanie programów komputerowych[615]. Wskazany raport przyczynił się do dalszych prac Rady Europy w zakresie cyberprzestępczości między innymi do stworzenia Rekomendacji R(89)9. Organizacja systematycznie publikuje raporty i książki związane z tematyką cyberbezpieczeństwa, złośliwego oprogramowania[616]. W 1990 roku utworzono pod auspicjami OECD grupę ekspertów, którzy mieli opracować zalecenia na temat ochrony informacji przetwarzanej elektronicznie. W 2001 roku powołano podobną grupę, która uwzględniając zalecenia z 1990 roku przygotowała opracowanie *Wytyczne OECD dla bezpieczeństwa systemów informatycznych i sieci: w kierunku kultury bezpieczeństwa* (ang. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*). Kolejny raport z 2005 roku poruszał kwestię wpływu spamu na państwa rozwijające się. Raport z 2007 roku omawiał temat zakresu i sposobu kryminalizacji cyberterroryzmu[617].

W ramach OECD utworzono Komitet do spraw Informacji, Informatyki i Polityki Komunikacyjnej (ang. *Commitee for Information, Computer and Communications Policy* - ICCP), który ma za zadanie prowadzenie badań nad przeciwdziałaniem cyberprzestępczości. ICCP systematycznie przygotowuje raporty, wśród których wymienić należy raporty poruszające kwestie wpływu spamu na rozwijające się państwa, kradzieży tożsamości (*Scoping paper on online Identity theft*) czy też wirusów i szkodliwego oprogramowania (*Computer Virusesand Other Malicious Softwere a Threat to the Internet Economy*)[618].

Oprócz systematycznego wydawania raportów OECD organizuje konferencje, szkolenia i warsztaty dotyczące zapobiegania przestępczości komputerowej.

OECD jest również silnie zaangażowana w kwestię technicznych i prawnych aspektów handlu elektronicznego. Mimo, że wydane przez organizację akty nie mają mocy wiążącej to wywierają wpływ na stanowiska członków społeczności międzynarodowej. Problem e-commerce był przedmiotem kilku konferencji OECD między innymi tych

[615] A. Adamski, *Prawo …*, Warszawa 2000, s. 5-6.
[616] J. Kosiński, *Paradygmaty …*, s. 232.
[617] M. Siwicki, *Cyberprzestępczość* …, s. 44-45.
[618] Ibidem, s. 45.

zorganizowanych w Ottawie (1998), Paryżu (1999), Dubaju (2001) czy też konferencji z 2007 roku, mającą miejsce w Turku w Finlandii[619]. Największe znaczenie miało spotkanie w Ottawie w 1998 roku, podczas którego przyjęto wytyczne planu działania OECD w dziedzinie handlu elektronicznego. Plan był inspiracją do kolejnych działań i inicjatyw podejmowanych w tym przedmiocie. Krystyna Kowalik - Bańczyk wskazuje, że plan ten dzielił się na cztery zasadnicze obszary: wzmocnienia zaufania konsumentów i użytkowników, optymalizacji zalet handlu elektronicznego, poprawy infrastruktury informacji dla handlu elektronicznego oraz stworzenia podstawowych zasad rządzących rynkiem numerycznym. W planie szczególną uwagę zwrócono też na konieczność kontynuowania prac w zakresie ochrony życia prywatnego, ochrony konsumentów, sprawdzania tożsamości oraz dostępu do infrastruktury[620].

OECD zajęło również stanowisko w sprawie podpisów elektronicznych wydając następujące wskazówki dotyczące kryptografii (ang. *Guidelines for Cryptography Policy*[621]):

1. „Metody kryptograficzne powinny być godne zaufania, aby zapewniać bezpieczne użytkowanie systemów informacji i komunikacji.
2. Użytkownicy powinni mieć prawo wyboru metody kryptograficznej zgodnie z prawem mającym zastosowanie.
3. Metody kryptograficzne winny być rozwijane w odpowiedzi na potrzeby i żądania osób indywidualnych, przedsiębiorstw i rządów.
4. Standardy techniczne, kryteria i protokoły metod kryptograficznych powinny być rozwijane i udostępniane na poziomie krajowym i międzynarodowym.
5. Podstawowe prawa jednostek do prywatności, włączając w to tajemnicę korespondencji i ochronę danych osobowych, powinny być respektowane w krajowych założeniach polityki kryptograficznej oraz na etapie implementacji i stosowana metod kryptograficznych.
6. Krajowa polityka kryptograficzna może pozwalać na zgodny z prawem dostęp do tekstów zawierających utajnione informacje lub udostępnianie kryptograficznych kluczy dostępu do tych tekstów. Powinno się to jednak odbywać z najwyższym poszanowaniem innych wskazówek z omawianej listy.

[619] K. Kowalik-Bańczyk, op. cit., s. 120.
[620] Ibidem, s. 121.
[621] Dostępne na oficjalnej stronie internetowej OECD: http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm [10.10.2015].

7. Odpowiedzialność jednostek i instytucji oferujących usługi kryptograficzne powinna być jasno sformułowana, niezależnie od tego, czy wynika ona z tekstu prawnego, czy z umowy.
8. Rządy powinny współpracować, by uzyskać koordynację polityk kryptograficznych. Ich wysiłek powinien być ukierunkowany na usuwanie lub nietworzenie nowych ograniczeń handlu, pod hasłem polityki kryptograficznej"[622].

Krystyna Kowalik - Bańczyk stawia tezę, że *soft law* OECD w postaci rekomendacji jest idealnym rozwiązaniem dla regulacji handlu elektronicznego. Państwa będące członkami OECD popierają zasadę niedyskryminacji uregulowań handlu elektronicznego wobec handlu tradycyjnego. Takie same regulacje powinny dotyczyć obu rodzaju handlu - a co za tym idzie, nie ma potrzeby wprowadzania odmiennych przepisów dotyczących e-commerce. Idea autoregulacji zyskuje coraz większą popularność również ze względu na fakt, iż osiągnięcie międzynarodowego konsensusu w tym przedmiocie może być trudne w najbliższy czasie[623]. Mimo, że stanowisko Krystyny Kowalik Bańczyk zostało wyrażone ponad dekadę temu to wciąż pozostaje aktualne. Wpływa na to fakt, iż międzynarodowe porozumienie do dnia dzisiejszego nie zostało osiągnięte i wydaje się, że stan ten będzie się utrzymywał w kolejnych latach.

W 2008 roku w Seulu wydano Deklarację dla Przyszłości Internetowej Ekonomii (ang. *The Seul Declaration for the Future of the Internet Economy*) w trakcie spotkania ministrów krajów członkowskich ustalono, że głównym wyzwaniem w cyberprzestrzeni jest odpowiednia równowaga pomiędzy prawem, polityką, samoregulacją oraz prawami użytkowników związanych między innymi z: prawami własności intelektualnej, zabezpieczeniem infrastruktury informatycznej i odpowiedniej reakcji na zagrożenia w cyberprzestrzeni, ochroną praw jednostek, w szczególności praw mniejszości i grup szczególnie narażonych, promowania bezpiecznego i odpowiedzialnego używania Internetu z poszanowaniem międzynarodowych norm etycznych i społecznych[624].

Głównymi założeniami deklaracji seulskiej było ułatwienie konwergencji sieci cyfrowych, urządzeń, aplikacji i usług przez politykę, która dostosowana jest do elastycznych norm i szybkich zmian zachodzących w cyberprzestrzeni, stymuluje rozwój innowacyjności i

[622] K. Kowalik-Bańczyk, op. cit., s. 157-158.
[623] Ibidem, s. 121.
[624] The Seul Declaration for the Future of the Internet Economy, Seul 2008, s. 5-6.

infrastruktury komunikacyjnej. Ponadto, założono, iż polityka państw winna zapewniać ochronę infrastruktury krytycznej, tożsamości cyfrowej oraz wspierać handel internetowy[625].

W opublikowanym w 2015 roku raporcie OECD Perspektywy w dziedzinie gospodarki cyfrowej 2015 (ang. *OECD Digital Economy Outlook 2015*) podkreślono, że rządy państw członkowskich OECD mają coraz większą świadomość konieczności rozwoju gospodarki cyfrowej opierając się na odpowiedniej strategii, która może przyczynić się do zmniejszenia bezrobocia, nierówności i ubóstwa. Krajowe strategie cyfrowe w swoich zamierzeniach przewidują takie działania, jak: tworzenie przedsiębiorstw, wzrost wydajności, wspieranie zdrowia, edukacji i oświaty. Rządy państw mają coraz większą świadomość konieczności kształtowania polityki dotyczącej cyberprzestrzeni. W dokumencie szczególnie zaakcentowano potrzebę zachowania otwartości cyberprzestrzeni. Uznano, że Internet rozumiany winien być jako otwarta platforma, na której przedsiębiorcy, obywatele i rządy mogą tworzyć aplikacje, serwisy oraz wprowadzać innowacje zmierzające do rozwoju gospodarki cyfrowej. Organizacja Współpracy Gospodarczej i Rozwoju w dokumencie wyraziła obawę, że korzyści płynące z otwartej i zdecentralizowanej struktury cyberprzestrzeni oraz swobodnego transgranicznego przepływu danych mogą zostać zmniejszone. Jako czynniki, które mogłyby doprowadzić do takiej sytuacji wskazane zostały lokalne wymogi dotyczące treści i przechowywania danych, neutralność sieci, powszechna akceptowalność wielojęzycznych nazw domenowych oraz tworzenie sieci alternatywnych[626].

Trudno wymienić wszystkie dokumenty związane z przestrzenią wirtualną, które zostały opublikowane przez OECD. W tym miejscu należy jedynie zaakcentować tematy, które zostały poruszone przez Organizację Współpracy Gospodarczej i Rozwoju. Są to: wirusy komputerowe i szkodliwe oprogramowanie (*Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*), kradzież tożsamości *on-line* (*OECD Policy Guidance on Online Identity Theft*), piractwo komputerowe (*Piracy of Digital Content*), ochrona dzieci w sieci (*OECD Recommendation on the Protection of Children Online*) czy też ochrona krytycznej infrastruktury informatycznej (*Recommendation of the Council on the Protection of Critical Information Infrastructures*). Wszystkie wskazane powyżej dokumenty dostępne są na oficjalnej stronie internetowej Organizacji Współpracy Gospodarczej i Rozwoju.

[625] Ibidem, s. 6-9.
[626] OECD Digital Economy Outlook 2015, Paryż 2015.

3.1.3.5. Dorobek Światowej Organizacji Handlu

W Światowej Organizacji Handlu[627] (ang. *World Trade Organisation* - WTO) dostrzeżono konieczność regulacji handlu elektronicznego już w latach dziewięćdziesiątych XX wieku. W drugiej połowie lat dziewięćdziesiątych zawarto dwa porozumienia, mające szczególną rolę - Podstawowe Porozumienie Telekomunikacyjne (ang. *Basic Telecommunication Agreement* - BTA[628]) oraz Porozumienie o Technologiach Informacyjnych (ang. *Information Technology Agreement*- ITA)[629].

Porozumienie o technologiach informacyjnych początkowo zostało podpisane przez 29 członków singapurskiej konferencji ministerialnej w grudniu 1998 roku. Od tego czasu liczba członków porozumienia wzrosła do 82, które to państwa reprezentują 97% światowego handlu produktami technologii informatycznej. Sektor IT jest najszybciej rozwijającym się działem w handlu światowym, a produkty IT stanowią około 10% eksportu towarów globalnych. Porozumienie ITA obejmuje dużą część produktów sektora IT, czyli komputery, sprzęt telekomunikacyjny, oprogramowanie. W 2012 roku w 15 rocznicę podpisania ITA uznano, iż porozumienie nie odpowiada wymogom współczesnego rynku, wobec czego niektórzy członkowie uznali, iż katalog produktów zawartych w ITA powinien być rozszerzony. Po przeprowadzonych negocjacjach w 2015 roku członkowie zgodzili się na rozszerzenie katalogu ITA o produkty nowej generacji na przykład urządzenia GPS, półprzewodniki oraz sprzęt medyczny[630].

W trakcie drugiej konferencji ministerialnej 29 maja 1998 roku w Genewie państwa członkowskie WTO przyjęły Deklarację o światowym handlu elektronicznym[631], w której ustalono program pracy mający na celu zbadanie kwestii związanych z e-commerce oraz przedstawienie raportu opisującego stan zaawansowania prac już w czasie kolejnej - trzeciej konferencji ministerialnej w Seattle. Za handel elektroniczny w pkt. 1.3 deklaracji uznano dystrybucję, marketing, sprzedaż lub dostawy towarów i świadczenie usług drogą

[627] Porozumienie ustanawiające WTO (Światową Organizację Handlu) zostało opublikowane w Dz.U. z 1995 r. Nr 98, poz. 483.
[628] Porozumienie to ma formę protokołu dołączonego do GATS i oficjalnie nazywa się ją Czwartym Protokołem GATS. Weszła w życie 5 lutego 1998 r.
[629] K. Kowalik-Bańczyk, op. cit., s. 117.
[630] Dane z oficjalnej strony internetowej WTO: https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm [29.10.2016].
[631] Deklaracja o światowym handlu elektronicznym, z dnia 20 września 1998 r. WT/L/274.

elektroniczną. W dokumencie znalazło się postanowienie, że państwa członkowskie nie zamierzają nakładać ceł na transakcje elektroniczne. Postanowienie o zwolnieniu z cła produktów sprzedawanych w Internecie zostało podtrzymane w czasie konferencji w Seattle[632].

Rada Ogólna WTO w 1998 roku przyjęła program pracy nad e-commerce. Prace zostały podzielone pomiędzy Radę do spraw Handlu Usługami, Radę do spraw Handlu Towarami, Radę TRIPs i Komitet do spraw Konkurencji i Rozwoju. W lipcu 1999 roku każdy z wymienionych organów przedstawił Radzie Generalnej raport. Analiza raportów doprowadziła do zidentyfikowania trzech typów transakcji podejmowanych w Internecie:

- transakcje całkowicie dokonywane w Internecie - od wyboru oferty, zakupu aż do wykonania usługi,
- transakcje mieszane - gdzie produkt jest wybierany w przestrzeni wirtualnej, ale jego dostawa następuje środkami tradycyjnymi,
- transakcje dotyczące transportu telekomunikacji, w tym dostarczanie usług internetowych[633].

Opisany wyżej raport potwierdził, że większość transakcji w cyberprzestrzeni to usługi, w związku czym można do nich zastosować Ogólne Porozumienie o Handlu Usługami (GATS) oraz Deklarację Ministerialną dotyczącą handlu produktami technologii informacyjnych (ATI)[634]. W kolejnych latach debatowano nad programem zbudowania ram dla funkcjonowania światowego handlu w XXI wieku[635].

Światowa Organizacja Handlu 11 grudnia 2009 roku w trakcie kolejnej konferencji ministerialnej w Genewie postanowiła zintensyfikować prace nad nowym programem dotyczącym handlu elektronicznego. W czasie następnego spotkania w Genewie w 2011 roku podkreślono, iż przygotowywany plan oprócz przedstawionych propozycji członków musi opierać się również na podstawowych zasadach WTO, w tym na zakazie niedyskryminacji, przewidywalności oraz przejrzystości. Podejmowane działania mają na celu zapewnienie lepszej łączności z Internetem oraz dostępem do wszelkich informacji i technologii

[632] K. Kowalik-Bańczyk, op. cit., s. 118-119.
[633] Ibidem, s. 118.
[634] Ibidem, s. 118-119.
[635] M. Wojtas, *Liberalizacja wymiany handlowej na forum Światowej Organizacji Handlu*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Współczesne problemy ekonomiczne. Globalizacja. Liberalizacja. Etyka" 2013, nr 7, s. 54.

telekomunikacyjnych. Kroki podejmowane przez WTO mają przyczynić się do rozwoju e-commerce ze szczególnym uwzględnieniem krajów rozwijających się. Program bada i ułatwia dostępność do handlu elektronicznego małych i średnich przedsiębiorców, w tym dla małych producentów i dostawców. W trakcie ostatniej konferencji ministerialnej WTO mającej miejsce w grudniu 2013 roku na Bali ustalono, że prace nad nowym programem handlu elektronicznego powinny obejmować, oprócz wyżej wymienionych, również aspekty związane z rozwojem telefonii komórkowych, elektronicznie dostarczanym oprogramowaniem, chmurą obliczeniową, ochroną danych oraz ochroną konsumentów w cyberprzestrzeni[636]. Aktualnie w ramach prac Światowej Organizacji Handlu trwają negocjacje nowego programu, który zostanie prawdopodobnie przyjęty w trakcie konferencji ministerialnej WTO w grudniu 2017 roku.

3.1.4 Regulacje organizacji zwalczających cyberprzestępczość

3.1.4.1.Dorobek INTERPOLu

Historia Interpolu sięga lat dwudziestych XX wieku. Jest to jedna z najbardziej znaczących organizacji pomagających organom ścigania w walce z przestępczością oraz drugą co do wielkości, po ONZ, organizacją międzypaństwową na świecie[637]. W chwili obecnej członkami Interpolu jest 190 państw[638] ze wszystkich kontynentów świata. Głównym celem działalności Interpolu jest wspieranie organów policji kryminalnych na świecie, wymiana informacji oraz oferowanie wsparcia i narzędzi do efektywnego ścigania przestępstw. Kluczową rolę w działalności organizacji zajmuje utworzony w 2002 roku globalny system łączności I-24/7, dzięki któremu Krajowe Biura Interpolu mogą zdalnie

[636] Dane z oficjalnej strony internetowej WTO: https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm [29.10.2016].
[637] B. Hołyst, *Policja na świecie*, Warszawa 2013, s.1168.
[638] Dane z oficjalnej strony Interpolu: http://www.interpol.int/Member-countries/World [08.07.2015].

uzyskać dostęp do baz danych, dzielić się pilnymi informacjami ze wszystkimi członkami Interpolu 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

Interpol jest szczególnie zaangażowany w globalną walkę z cyberprzestępczością. Większość przestępstw popełnianych w cyberprzestrzeni ma charakter ponadnarodowy i transgraniczny, wobec czego Interpol jest naturalnym partnerem dla krajowych organów ścigania. Jerzy Kosiński wskazuje, że „rola Interpolu w zwalczaniu cyberprzestępczości opiera się na prowadzeniu szkoleń, działaniach operacyjnych i działaniach mających zapewniać nadążanie służbom policyjnym za nowymi zagrożeniami. Realizowana jest przez:

- wspieranie wymiany informacji między państwami członkowskimi za pośrednictwem regionalnych grup roboczych i konferencji,
- dostarczanie szkolenia do budowania i utrzymywania standardów zawodowych,
- koordynowania i wspieranie operacyjnych działań międzynarodowych,
- ustanowienie globalnej listy oficerów kontaktowych ds. zwalczania cyberprzestępczości dostępnych przez całą dobę siedem dni w tygodniu[639] (lista zawierała 134 kontakty na koniec 2012 roku),
- pomaganie krajom członkowskim w przypadku aktów cyberprzestępców lub ścigania sprawców cyberprzestępczości przez dostarczanie usług i dostęp do bazy danych,
- rozwijanie strategicznego partnerstwa z innymi organizacjami międzynarodowymi i podmiotami sektora prywatnego,
- identyfikację pojawiających się zagrożeń i udostępnianie tej wiedzy państwom członkowskim,
- zapewnienie dostępu do bezpiecznego portalu internetowego z informacjami operacyjnymi i dokumentami”[640].

W 2014 roku w Singapurze uruchomiono Globalny Zespół Innowacji Interpolu (*Interpol Global Complex for Innovation* - skrót IGCI). Jest to instytucja badawcza, która ma na celu rozwój metod identyfikacji przestępstw i przestępców, prowadzenie innowacyjnych szkoleń, wparcie operacyjne i współpracę pomiędzy członkami. Celem ośrodka jest umożliwienie jednostkom policji na całym świecie zapewnienie narzędzi i zdolności do

[639] Utworzona na podstawie Rezolucji Zgromadzenia Ogólnego Interpolu nr AG-2008-RES-07 Poszerzenie system komunikacji I-24/7 do jednostek cybercime w celu ułatwienia wymiany aktualnych informacji [za:] J. Kosiński, *Paradygmaty …*, s. 221.
[640] J. Kosiński, *Paradygmaty …*, s. 221.

konfrontacji z coraz bardziej pomysłowymi i skomplikowanymi metodami działania cyberprzestępców.

Do głównych celów działalności IGCI należy budowanie potencjału i przeprowadzanie szkoleń, wsparcie operacyjne i śledcze oraz bezpieczeństwo cyfrowe. Cel trzeci realizowany jest przez:

1. „zwiększanie cyberbezpieczeństwa i przeciwdziałania cyberprzestępczości,
2. funkcjonowanie laboratorium kryminalistycznego wspierającego postępowania w sprawach o cyberprzestępstwa,
3. badania protokołów, narzędzi, usług oraz analizy trendów aktów cyberprzestępców,
4. rozwój praktycznych rozwiązań uzyskiwany we współpracy policji, laboratoriów badawczych, akademickich oraz sektorów publicznego i prywatnego,
5. zarządzanie bezpieczeństwem Internetu”[641].

Interpol podejmuje działania nie tylko ściśle związane z cyberprzestępczością *sensu stricte*. Równie istotne są działania Interpolu w odniesieniu do oszustw, które coraz częściej są popełniane za pomocą cyberprzestrzeni. Interpol zalicza do oszustw finansowych popełnionych za pomocą ICT: pranie brudnych pieniędzy, oszustwa związane z kartami płatniczymi, walutami i sfałszowanymi dokumentami oraz oszustwami związanymi z inżynierią społeczną (*phishing*) W ramach Interpolu powołane są komórki zajmujące się przestępstwami przeciwko dzieciom. Przestępcy nie tylko wymieniają się materiałami zawierającymi pornografię dziecięcą, ale również wykorzystują Internet do nawiązania kontaktu z nieletnimi, przez czaty i sieci społecznościowe[642].

Jako jedne z głównych cyber zagrożeń Interpol wymienia tak zwaną Darknet (ciemna sieć). Darknet jest częścią cyberprzestrzeni ukrytą przed normalnymi użytkownikami, nazywana jest również „Deep Web”, czyli głęboką siecią. Darknet jest siecią wykorzystywaną przez przestępców. Poruszają się oni w sieci za pomocą specjalistycznego oprogramowania, ukrywającego ich prawdziwą tożsamość. Darknet jest wykorzystywany do nielegalnych transakcji takich, jak: sprzedaż narkotyków, broni, nielegalny hazard, handel podrobionymi dokumentami tożsamości czy pornografią dziecięcą. Skomplikowane narzędzia szyfrowania i programy mające na celu ukrycie tożsamości posługujących się nimi osób używane do

[641] Ibidem, s. 221-222.
[642] Dane z oficjalnej strony internetowej Interpolu: https://www.interpol.int/en [29.10.2016].

komunikowania się Darknecie stwarza dla organów ścigania szereg wyzwań w identyfikacji i lokalizacji przestępców[643].

Interpol rozumiejąc konieczność gromadzenia dowodów cyfrowych powołał Laboratorium Interpolu do spraw Dowodów Cyfrowych (ang. *Interpol Digital Forensics Laboratorium*). Uznano, że kryminalistyka cyfrowa jest niezbędna do prowadzenia postępowania policyjnego. Możliwość wyodrębnienia dowodów z komputerów, telefonów komórkowych i urządzeń cyfrowych jest kluczem w skutecznym ściganiu przestępców. Laboratorium Interpolu do spraw Dowodów Cyfrowych pomaga krajom w podniesieniu wykrywalności i wykorzystywania dowodów cyfrowych. Oferowane wsparcie polega głównie na analizie złośliwego oprogramowania, pomocy w zbadaniu urządzeń cyfrowych, szkoleniach z najnowszych cyfrowych narzędzi oraz technik kryminalistycznych oraz testowaniu cyfrowych narzędzi diagnostycznych opracowanych przez sektor prywatny, środowiska akademickie czy też krajowe laboratoria badawcze[644].

Interpol wspólnie z Europolem od 2013 roku organizują konferencje dotyczące cyberprzestępczości. Pierwsza konferencja odbyła się w Hadze 24-25 września 2013 roku jako innowacyjna wspólna inicjatywa organizowana na przemian przez Europejskie Centrum do spraw Walki z Cyberprzestępczością w Hadze oraz Globalny Zespół Innowacji Interpolu w Singapurze. Konferencja skupiła menagerów jednostek ds. walki z cyberprzestępczością z całego świata w celu dalszego wzmacniania współpracy. Celem konferencji było wskazanie metod poprawy efektywności w zwalczaniu przestępczości komputerowej, zawężeniu współpracy, koordynacji i badań międzynarodowych. Podkreślono ponadnarodowy charakter cyberprzestępstw, brak granic fizycznych czy wirtualnych i konieczność współpracy policyjnej zarówno w zakresie zapobiegania jak i zwalczania przestępstw. W trakcie konferencji poruszono temat cyberataków, pieniędzy wirtualnych, różnych form cyberprzestępczości, konieczności stworzenia efektywnych przepisów prawnych, zapewniających skuteczne ściganie przestępców[645].

W trakcie konferencji zorganizowanej w 2015 roku w Hadze debatowano nad problemami związanymi z najnowszymi zagrożeniami w cyberprzestrzeni, opracowywaniem

[643] Dane z oficjalnej strony internetowej Interpolu: https://www.interpol.int/Crime-areas/Cybercrime/The-threats [29.10.2016].
[644] Dane z oficjalnej strony internetowej Interpolu: https://www.interpol.int/Crime-areas/Cybercrime/Activities/Digital-forensics [29.10.2016].
[645] Dane z oficjalnej strony internetowej Interpolu: https://www.interpol.int/News-and-media/News/2013/N20130925 [19.10.2016].

metod walki z przestępczością komputerową, opracowywaniem międzynarodowych ram współpracy, cyberbezpieczeństwem, walką z nadużyciami w walutach wirtualnych oraz ewolucją cyberprzestępczości w Afryce[646]. Konkluzją ostatniej, czwartej konferencji, było stwierdzenie, że organy ścigania i firmy z sektora prywatnego muszą znaleźć odpowiednie rozwiązania ograniczające cyberprzestępczość, konieczna jest również pomoc ofiarom cyberprzestępstw oraz wspieranie przez Interpol oraz Europol istniejących regionalnych ośrodków do walki z cyberprzestępczością przez budowanie potencjału i wymianę informacji[647].

3.1.4.2. Dorobek Europolu

Europol, czyli Europejski Urząd Policji (ang. *The European Police Office*) jest policyjną agendą Unii Europejskiej z siedzibą w Hadze. Idea stworzenia tej instytucji powstała podczas tworzenia Traktatu o Unii Europejskiej w Maastricht (art. K.1). Celem działalności Europolu jest zwalczanie międzynarodowej przestępczości zorganizowanej, przemytu narkotyków, materiałów radioaktywnych, prania brudnych pieniędzy, zabójstw, handlu ludzkimi organami, ale również fałszowania pieniędzy czy przestępstw komputerowych[648]. Europol stanowi wsparcie w zakresie egzekwowania prawa oraz punkt wymiany wiedzy specjalistycznej i informacji na temat działalności przestępczej oraz metod ścigania.

Już w 2007 roku został wydany dokument o nazwie *High Tech Crimes Within the EU: Old crimes new tools, new crimes new tools. Threat Assessment 2007. High Tech Crime Centre*[649], w którym zostały wskazane zagrożenia cyberprzestępczością w Unii Europejskiej. Sformułowano w nim następujące rekomendacje:

[646] Dane z oficjalnej strony internetowej Interpolu: https://www.interpol.int/News-and-media/Events/2015/Europol-INTERPOL-Cybercrime-Conference/Europol-INTERPOL-Cybercrime-Conference [19.10.2016].
[647] Dane z oficjalnej strony internetowej Europolu: https://www.europol.europa.eu/content/interpol-europol-cybercrime-conference-closes-multi-stakeholder-cooperation [29.10.2016].
[648] Z. Rau, *Przestępczość zorganizowana w Polsce i jej zwalczanie*, Kraków 2002, s. 91-92.
[649] *High Tech Crimes Within the EU: Old crimes new tools, new crimes new tools. Threat Assessment 2007. High Tech Crime Centre*, dostęp online https://www.enisa.europa.eu/activities/cert/events/files/ENISA_Europol_threat_assessment_2007_Dileone.pdf [08.07.2015].

- konieczna jest większa wymiana informacji i wzmocnienie współpracy pomiędzy państwami członkowskimi w celu efektywnego zwalczania cyberprzestępczości,
- konieczne jest zacieśnienie współpracy z sektorem prywatnym oraz twórcami oprogramowania w celu wymiany informacji,
- istnieje potrzeba edukowania użytkowników Internetu na temat bezpiecznego korzystania z cyberprzestrzeni,
- zaleca się implementację Konwencji o cyberprzestępczości tak, by stała się największą platformą prawną walki z cyberprzestępczością; co więcej, państwa winny systematycznie aktualizować legislację krajową w sposób odpowiedni do zachodzących szybkich zmian technologicznych,
- istnieje potrzeba harmonizacji postępowań sądowych w celu uzyskania wspólnego podejścia co do kwestii dopuszczenia dowodów w sądzie,
- należy zwrócić uwagę na problem szyfrowania używanego przez przestępców w celu ukrycia dowodów ich przestępczego działania,
- konieczne jest rozwiązanie problemu użycia VoIP[650] w kontekście monitorowania i przechwytywaniem szyfrowanej komunikacji,
- należy zwrócić szczególną uwagę na ochronę infrastruktury krytycznej, która często staje się celem ataków hakerów oraz opracowanie europejskiej strategii w tej płaszczyźnie[651].

Europol podjął szereg działań w walce z cyberprzestępczością i nielegalnymi działaniami podejmowanymi w przestrzeni wirtualnej. Kluczowym zagadnieniem jest z pewnością wymiana informacji, doświadczeń, metod działania oraz międzynarodowa współpraca pomiędzy poszczególnymi państwami. W tym celu Europol systematycznie organizuje szkolenia poruszające najważniejsze aktualne problemy w zwalczaniu cyberprzestępczości na przykład dotyczące wykorzystywania dzieci.

[650] VoIP (ang. *Voice over Internet Protocol*) - technika umożliwiająca przesyłanie mowy za pomocą łączy internetowych lub oddzielnych sieci wykorzystujących protokół IP, popularnie nazywana „telefonią internetową". Dane przesyłane są przy użyciu protokołu IP, co pozwala wykluczyć niepotrzebne „połączenie ciągłe" i np. wymianę informacji gdy rozmówcy milczą. http://www.komputerswiat.pl/poradniki/internet/isp-i-internet/2010/07/przewodnik-po-telefonii-voip.aspx [08.07.2015].

[651] *High Tech Crimes Within the EU: Old crimes new tools, new crimes new tools. Threat Assessment 2007. High Tech Crime Centre*, s. 54-55, dostęp online: https://www.enisa.europa.eu/activities/cert/events/files/ENISA_Europol_threat_assessment_2007_Dileone.pdf [08.07.2015].

Tabela 10. Liczba przedsięwzięć szkoleniowych dotyczących cyberzagrożeń organizowanych przez Europol w latach 2007-2012

Rok	Ogólna liczba szkoleń organizowanych przez CEPOL w danym roku	Nazwa szkolenia	Kraj lub organizacja inicjująca
2007	82	*Child Abuse in Cyberspace*	Irlandia
		High Tech & Cybercrime	Włochy
		High Tech & Cybercrime	Francja
2008	87	*High Tech & Cybercrime*	Portugalia
2009	87	Konferencja nt. nowych technologii w zwalczaniu cyberprzestępczości w porozumieniu z sektorem prywatnym	Czechy
2010	86	*Child Abuse in Cyberspace*	Europol
		High Tech & Cybercrime	Grecja
2011	91	*Child Abuse in Cyberspace*	Belgia
		High Tech & Cybercrime	Słowenia
2012	122	*Child Abuse in Cyberspace*	Malta
		High Tech & Cyberspace	Hiszpania
		Cyberspace forensic	Łotwa
		Investigating cybercrime	Włochy
		Seminarium internetowe dot. Cyberprzestępczości	CEPOL

Źródło: B. Skłodowski, *Unia Europejska wobec cybernetycznych zagrożeń bezpieczeństwa*, [w:] M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa 2014, s. 198.

Wymienione inicjatywy wskazują na systematyczne rozszerzanie współpracy służb państw członkowskich odpowiedzialnych za zwalczanie cyberprzestępczości. Zalecane jest dalsze zacieśnianie współpracy, prowadzenie szkoleń i wymiana doświadczeń we wskazanym zakresie.

W dokumencie o nazwie *Cybercrime: improving international cooperation*[652] Europol przedstawił czynniki, które uznał za istotne z punktu widzenia transgranicznego, międzynarodowego zwalczania przestępczości zorganizowanej, cyberprzestępczości i terroryzmu. Wskazywał w nim, że podstawą do transgranicznej pomocy prawnej jest szereg konwencji i porozumień, wśród których, w odniesieniu do cyberprzestępczości, najbardziej istotna jest Konwencja o cyberprzestępczości. Dla współpracy transgranicznej najbardziej korzystne jest wzajemne uznawanie procedury karnej, a w szczególności metod pozyskiwania i zabezpieczenia dowodów w taki sposób, by dowody zebrane w sposób zgodny z prawem w jednym państwie mogły posłużyć za dowód popełnienia przestępstwa w innym państwie. Wzajemne uznawanie pozyskanych dowodów ma szczególne znaczenie w stosowanych technikach śledczych. Pozytywnie oceniono harmonizację przepisów na poziomie regionalnym - państw członkowskich Unii Europejskiej[653].

W dokumencie Europolu wskazano rozbieżności prawne, które wymagają standaryzacji w celu przyśpieszenia i ułatwienia procedury wymiany informacji. Przede wszystkim, jako duży problem wskazuje się różnorodną klasyfikację dokumentów, do których dostęp jest ograniczony jako „tajne", „ściśle tajne", oraz funkcjonariuszy, którzy mają dostęp do takich danych. Ponadto, konieczna jest harmonizacja przepisów dotyczących danych osobowych, w tym dokładne określenie, które dane osobowe mogą być udostępniane i komu. Jako przykład podaje się adres IP komputera, który w jednym kraju jest uznany za dane osobowe, w innym zaś systemie prawnym nie podlega pod ochronę takich przepisów, a zatem można go swobodnie udostępniać. Jako wartą rozważenia propozycję wskazano ujednolicenie przepisów dotyczących standardów przetwarzania danych, w szczególności w zakresie cyfrowych standardów kryminalistycznych, a mianowicie, czy dane gromadzone i przetwarzane w jednym kraju mogą być wykorzystane w postępowaniu sądowym w innym państwie[654].

Szczególnie istotne z punktu widzenia walki z cyberprzestępczością jest oczywiście szkolenie społeczeństwa, ale też organów ścigania. Szybki rozwój technologii powoduje, iż szkolenia powinny mieć charakter ciągły, zwłaszcza w zakresie nowych technik kryminalistyki cyfrowej. Konieczne jest stałe aktualizowanie materiałów szkoleniowych, wymiana informacji i najlepszych praktyk. Eksperci Europolu słusznie akcentują, iż dużym

[652] Europol, Cybercrime: improving international cooperation. GCCS2015 - Parallel session 4. Discussion paper, Haga 2015.
[653] Ibidem, s. 2-4.
[654] Ibidem, s. 4-5.

wyzwaniem w efektywnej walce z cyberprzestępczością jest posiadanie odpowiednich narzędzi - specjalistycznego i nowoczesnego sprzętu, laboratoriów cyfrowych zdolnych do przetwarzania dużych ilości danych[655].

3.1.4.3. Dorobek Europejskiego Centrum do spraw Walki z Cyberprzestępczością

Przy Europolu 1 stycznia 2013 roku utworzono Europejskie Centrum do spraw Walki z Cyberprzestępczością (ang. *European Cybercrime Centre* - EC3). Celem jego działalności jest walka z następującymi rodzajami przestępstw:

- cyberprzestępstwa popełnione przez zorganizowane grupy przestępcze w szczególności te przynoszące duże zyski, czyli oszustwa internetowe,
- cyberprzestępstwa wyrządzające poważne szkody ofiarom, czyli przemoc seksualna wobec dzieci w cyberprzestrzeni,
- cyberprzestępstwa (również cyber ataki) przeciwko infrastrukturze krytycznej i systemom informatycznym w Unii Europejskiej[656].

Europejskie Centrum do spraw Walki z Cyberprzestępczością, aby zrealizować wyżej wymienione cele:

- jest centralnym ośrodkiem wymiany informacji karnych i wywiadowczych,
- wspiera państwa członkowskie w przeprowadzanych operacjach i dochodzeniach przez dostarczanie analiz, wiedzy i koordynację działań,
- oferuje szereg produktów do analizy strategicznych umożliwiających świadome podejmowanie decyzji na szczeblu taktycznym i strategicznym w zakresie zwalczania i zapobiegania cyberprzestępczości,
- buduje potencjał i przeprowadza szkolenia, w szczególności dla odpowiednich organów państw członkowskich,
- zapewnia wysoko wyspecjalizowanych specjalistów i ekspertyzy kryminalistyczne, które mogą być wykorzystane w dochodzeniach i operacjach,

[655] Ibidem, s. 5-8.
[656] Dane z oficjalnej strony internetowej Europolu: https://www.europol.europa.eu/ec3 [11.06.2015].

- zapewnia koordynację w wymianie informacji i doświadczeń dotyczących cyberprzestępczości pomiędzy krajowymi organami ścigania a sektorem prywatnym, ośrodkami akademickimi i innymi partnerami niezwiązanymi bezpośrednio z wymiarem sprawiedliwości[657].

EC3 został podzielony na kilka punktów kontaktowych (ang. *Focal Points - FP*) zajmujących się następującymi obszarami działania: *FP Terminal* zapewnia wsparcie organów ścigania w sprawach dotyczących oszustw płatniczych, między innymi we współpracy z sektorem prywatnym i organami tj. Europejski Bank Centralny i banki krajowe. *FP Terminal* dąży do zapewnienia bezpieczeństwa i zaufania klientów w elektronicznych i internetowych transakcjach płatniczych oraz w transakcjach zawieranych przy użyciu kart płatniczych. Jednostka tworzy punkty i raporty analityczne dostarczające dane dotyczące na przykład rachunków bankowych, adresów e-mail oraz numerów telefonów. *FP Cyborg* wspiera państwa członkowskie UE w zakresie zapobiegania i zwalczania różnych form cyberprzestępczości wpływających na systemy sieciowej infrastruktury krytycznej. Szczególny nacisk jest położony na działania zorganizowanych grup przestępczych generujących duże zyski. Punkt kontaktowy pracuje nad szeroką gamą zaawansowanych technologicznie przestępstw takich, jak: hacking, *phishing,* kradzież tożsamości, malawere. *FP Cyborg* zapewnia analizę operacyjną i kryminalistyczną, wsparcie techniczne oraz badania cyfrowe dla państw członkowskich zarówno na miejscu (na przykład przez obecność ekspertów w trakcie przeszukań), jak również bezpośrednio z centrali Europolu. *FP Twins* powołany w celu walki z seksualnym wykorzystywaniem dzieci, zapewnia pomoc w zwalczaniu rozpowszechniania materiałów pedofilskich w Internecie, identyfikacji ofiar i przestępców, cyfrowego śledzenia sprawców, przechwytywaniu przesyłanych i informacji.

Europejskie Centrum do spraw Walki z Cyberprzestępczością łączy wiedzę w zakresie analizy strategicznej, wiedzy kryminalistycznej i policyjnej. Jest doskonałym miejscem transgranicznej i transnarodowej współpracy w zakresie zwalczania cyberprzestępczości, ale również wymiany informacji, edukowania krajowych organów ścigania i punktem współpracy z podmiotami prywatnymi. Uzyskiwana w ten sposób wiedza może pozytywnie wpłynąć na zmiany w zakresie polityki i prawodawca, a co najważniejsze na wzrost bezpieczeństwa dla obywateli i przedsiębiorców w świecie cyfrowym.

[657] Ibidem.

W ramach EC3 od 1 sierpnia 2014 roku powołano wspólną grupę zadaniową do spraw cyberprzestępczości (*EU Joint Cybercrime Action Taskforce* - J-CAT). W jej skład wchodzą specjaliści z Austrii, Francji, Hiszpanii, Holandii, Niemiec, Włoch, Wielkiej Brytanii oraz Australii, Kanady, Kolumbii i Stanów Zjednoczonych. Współpraca grupy polega na wzajemnym przekazywaniu sobie informacji wywiadowczych, które pomocne są w ustalaniu zadań, priorytetów w walce i zwalczaniu cyberprzestępczości[658]. J-CAT składa się z oficerów łącznikowych posiadających specjalistyczne wyszkolenie w dziedzinie cyberprzestępczości i cyberbezpieczeństwa. Pochodzą oni z krajów Unii Europejskiej, organów ścigania spoza UE (między innymi USA reprezentowanej przez trzy agencje: FBI, Secret Service oraz Urząd Imigracyjny i Celny) oraz EC3[659].

Zadaniem J-CET jest aktywne prowadzenie wywiadu, zbieranie informacji i przeprowadzanie skoordynowanych działań przeciwko cyberprzestępczości. Osiągnięcie tego celu ma nastąpić przez koordynację działań, wspólne ustalanie priorytetów, przygotowanie, wszczynanie i prowadzenie dochodzeń transgranicznych. J-CET zajmuje się cyberprzestępstwami takimi, jak: malware, botnety, oszustwa *on-line* (systemy płatności *on-line,* stosowanie inżynierii społecznej), pranie pieniędzy, w tym walut wirtualnych oraz nadużyciami seksualnymi dzieci w cyberprzestrzeni[660].

3.1.5. Inne regulacje

3.1.5.1. Dorobek Grupy G8

Podgrupa High Tech Grupy G8[661] została powołana w 1997 roku w celu zwiększenia kooperacji państw w zakresie zapobiegania, dochodzenia i ścigania przestępstw popełnianych przy użyciu komputerów, systemów informatycznych i nowych technologii. W Waszyngtonie

[658] J. Kosiński, *Paradygmaty …*, s. 222-223.
[659] Dane z oficjalnej strony internetowej Europolu: https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat [30.07.2015].
[660] Ibidem.
[661] Grupę G-8 tworzą: Francja, Japonia, Kanada, Niemcy, Rosja, Stany Zjednoczone, Wielka Brytania i Włochy. Od 1977 roku w spotkaniach przywódców grupy G8 biorą udział przedstawiciele Wspólnoty Europejskiej, a obecnie Unii Europejskiej.

w 1997 roku przyjęto dziesięć zasad wraz z dziesięciopunktowym planem działania (ang. *Ten-Point Action Plan to fight tech crimes*) zawierającym propozycje zwalczania przestępczości komputerowej. Na organizowanych corocznie szczytach Grupa G8 poruszała kwestie przeciwdziałania cyberprzestępczości. W Moskwie w 1999 roku omawiano zagadnienie przestępczości komputerowej, w tym pornografii dziecięcej, w Paryżu w 2000 roku grupa G8 wezwała państwa do uregulowania w krajowych porządkach prawnych kwestii przestępczości komputowej tak by zlikwidować „cyfrowe raje prawne" (ang. *digital havens*). G8 w 2001 roku poruszyło kwestię ścigania i wykrywania cyberprzestępców, w Waszyngtonie w 2004 roku zagadnienie międzynarodowej współpracy w przeciwdziałaniu przestępczości komputerowej, w Moskwie w 2006 roku omawiano zagrożenia związane z cyberterroryzmem, w Monachium w 2007 roku politykę legislacyjną w odniesieniu do używania cyberprzestrzeni przez terrorystów, w Rzymie w 2009 roku cyberbezpieczeństwo i cyberprzestępczość, w Muskoka (Kanada) w 2010 roku przestępczość zorganizowaną i terroryzm w sieci wirtualnej, w Deauville (Francja) w 2011 roku zagadnienia dotyczące danych osobowych, przeciwdziałania przestępczości komputerowej, cyberbezpieczeństwa danych[662].

W kolejnych latach profil działalności instytucji rozszerzył się na kwestie związane z wykorzystaniem Internetu przez terrorystów, ochronę infrastruktury krytycznej oraz teleinformatycznej. Ponadto, w ramach podgrupy High Tech Starszych Specjalistów do spraw Międzynarodowej Przestępczości Zorganizowanej powołano sieć 24/7 (*G8 24/7 High Tech Crime Point of Contact Network*), czyli grupę ekspertów wspomagających śledztwa dotyczące cyberprzestępczości 24 godziny na dobę, 7 dni w tygodniu[663].

3.1.5.2. Dorobek Brytyjskiej Wspólnoty Narodów (*The Commonwealth*)

W ramach Brytyjskiej Wspólnoty Narodów od 2009 roku funkcjonuje *Commonwealth Internet Governance Forum* (CIGF). CIFG w 2011 roku wyszło z inicjatywą utworzenia

[662] M. Siwicki, *Cyberprzestępczość*…, s. 26-28.
[663] J. Kosiński, *Paradygmaty* ..., s. 220.

Comonwealth Cybercrime Initiative, które ma na celu zapewnienie współpracy i koordynacji między państwami członkowskimi opracowania jednolitych ram prawnych w zakresie zwalczania i ścigania cyberprzestępczości[664].

W przyjętym 18 marca 2016 roku Planie Strategicznym Telekomunikacyjnej Organizacji Brytyjskiej Wspólnoty Narodów na lata 2016-2020 jedno z głównych założeń dotyczyło cyberprzestrzeni. Za kluczowe uznano konieczność stworzenia wysokiej jakości, niedrogich łączy szerokopasmowych, zapewnienia bezpieczeństwa cybernetycznego, w tym ochrony dzieci w przestrzeni wirtualnej oraz promowanie stosowania technologii informacyjno - telekomunikacyjnych we wszystkich aspektach gospodarki[665].

3.1.5.3. Dorobek CERT

Komputerowe zespoły reagowania kryzysowego CERT (ang. *Computer Emergency Response Team*) są to zespoły reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego. Zadaniem CERT jest całodobowe nadzorowanie i monitorowanie sieci oraz reagowanie na incydenty. Organizacja została utworzona w 1988 roku po pierwszym zmasowanym ataku złośliwego oprogramowania, czyli komputerowego robaka o nazwie Morris Worm. Pierwszy zespół powstał w Carnegie Mellon University w USA[666].

Inicjatywa ta została podjęta również w Polsce. CERT Polska został założony w 1996 roku i od samego początku działalności był członkiem międzynarodowego forum zrzeszającego zespoły reagujące FIRST (ang. *Forum for Incident Response and Security Teams*). Do głównych zadań CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- współpraca z innymi zespołami CERT,
- współpraca w zakresie krajowych i międzynarodowych projektów dotyczących bezpieczeństwa teleinformatycznego,

[664] Ibidem, s. 233.
[665] Strategic Plan of the Commonwealth Telecommunications Organisation (CTO) for the period 2016 – 2020.
[666] Dane z oficjalnej strony internetowej CERT: http://www.cert.org/ [10.06.2015].

- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników,
- działalność badawcza w przedmiocie metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach,
- coroczne publikowanie Raportu CERT Polska analizującego przypadki incydentów zgłoszonych zespołowi,
- promowanie bezpieczeństwa teleinformatycznego przez działania informacyjno-edukacyjne mające na celu wzrost świadomości użytkowników sieci między innymi przez organizację konferencji i działalność w mediach społecznościowych,
- prowadzenie analiz i testów oraz rozwijanie własnych narzędzi pomocnych w zwiększeniu bezpieczeństwa teleinformatycznego[667].

3.2 Regulacje krajowe cyberprzestrzeni mające wpływ na tworzenie prawa międzynarodowego

Z biegiem lat rządy państw zaczęły dostrzegać realną potrzebę zabezpieczenia swojej przestrzeni wirtualnej. Kolejne zmasowane cyberataki na państwa pokazały, że ochrona cyberprzestrzeni nie jest futurystycznym pomysłem rodem z filmów *science - fiction*, lecz realną potrzebą, zwłaszcza w krajach wysoko rozwiniętych, w których znaczna część gospodarki, transportu, służby zdrowia oraz innych elementów infrastruktury krytycznej oparta jest na systemach informatycznych. Przyczynkiem do poważniejszych rozmów na ten temat był atak w 2007 roku rosyjskich hackerów na estońską cyberprzestrzeń i działające w niej rządowe i prywatne strony internetowe. Estonia jako pierwszy kraj w historii padła ofiarą zmasowanego - motywowanego politycznie - ataku na własną przestrzeń wirtualną.

Po tym incydencie rządy krajów wysoko rozwiniętych zaczęły opracowywać politykę i modele doktryny cyberbezpieczeństwa. Mirosław Lakomy, omawiając problem opracowania nowych strategii bezpieczeństwa w kontekście zupełnie nowej grupy zagrożeń w

[667] Dane z oficjalnej strony CERT Polska: http://www.cert.pl/o-nas [10.08.2015].

cyberprzestrzeni, słusznie wskazał, że kwestie te „stanowią rosnące wyzwanie nie tylko dla poszczególnych państw, ale także dla tradycyjnych sojuszy militarnych, w tym przede wszystkim dla Paktu Północnoatlantyckiego, tak w wymiarze prawnym, politycznym, jak i wojskowym. Wydarzenia z Estonii z 2007 roku udowodniły, iż NATO pozostało bezsilne wobec tych nowych zagrożeń. Problem jest tym istotniejszy, że incydenty tego typu, dzięki swojej zróżnicowanej i stale ewoluującej formie, mogą potencjalnie mieć skutki podobne do osiągalnych przy wykorzystaniu konwencjonalnego uzbrojenia”[668]. Cyberataki mogą mieć najróżniejsze źródła, pochodzić od indywidualnych jednostek, grup hackerskich czy też organizacji przestępczych czy grup terrorystycznych, które swoim działaniem chcą osiągnąć wymierną korzyść majątkową, destabilizować politykę, ekonomię i bezpieczeństwo kraju, uniemożliwić bądź poważnie zakłócić komunikację, czy też w końcu zaatakować najbardziej newralgiczne punkty infrastruktury krytycznej państwa. Doświadczenia ostatnich lat wskazują, iż do narzędzi cybernetycznych coraz chętniej sięgają także państwa. Część ataków z całą pewnością sterowana jest bezpośrednio przez instytucje wojskowe, wywiad czy nie do końca jawne militarne cyberjednostki. Niezwykle trudno jest udowodnić, iż za konkretnym atakiem stało dane państwo. W trakcie szczytu NATO, który odbył się w 2016 roku w Warszawie stwierdzono jednak, że cyberatak może być uznany za naruszenie art. 5 Traktatu Północnoatlantyckiego.

Z tych też względów niniejszy rozdział zostanie poświęcony regulacjom krajowym w cyberprzestrzeni. W szczególności omówione zostaną strategie cyberbezpieczeństwa poszczególnych państw oraz regulacje prawne, które mają istotne znaczenie z punktu omawianego w niniejszej dysertacji problemu. Przeanalizowane zostaną dokumenty państw, które stały się ofiarami cyberataków oraz państw wysokorozwiniętych, w których prawo szybko i sprawnie dostosowuje się do zmian technologicznych. Omówiona ona będzie polityka cyberprzestrzeni wielkich supermocarstw: USA, Rosja i Chiny. Państwa te znajdują na szczycie listy krajów będących zarówno ofiarami, jak i agresorami cyberataków. Ponadto, w rozdziale niniejszym poruszona zostanie pokrótce polityka cyberbezpieczeństwa Rzeczpospolitej Polskiej. Opisane regulacje krajowe tworzą pośredni wpływ na tworzenie się międzynarodowych norm prawnych. Negatywne doświadczenia państw powodują, sprecyzowanie przepisów wewnętrznych, nierzadko wprowadzających innowacyjne rozwiązania. Czerpanie i wzorowanie się na rozwiązaniach przyjętych w innych państwach

[668] M. Lakomy, *Polityka cyberbezpieczeństwa Sojuszu Północnoatlantyckiego*, „Przegląd Zachodni” 2013, nr 4, s. 114.

prowadzi do unifikacji przepisów, przyjęcie pewnych międzynarodowych „reguł postępowania" i standardów, które są stopniowo inkorporowane i akceptowane przez społeczność międzynarodową (bądź zdecydowanie odrzucane jako ingerujące zbytnio w prawa innych państw).

3.2.1 Porządki prawne krajów - ofiar cyberataków

Estonia a cyberprzestrzeń

Republika Estońska jest jednym z najbardziej zaawansowanych technologicznie krajów w Unii Europejskiej. Teza, iż społeczeństwo estońskie jest społeczeństwem informacyjnym nie powinna zatem budzić najmniejszych wątpliwości. W 2005 roku Estonia stała się pierwszym krajem na świecie, w którym wykorzystano Internet do głosowania w wyborach lokalnych. Około 95% operacji bankowych przeprowadzanych jest elektronicznie, studenci otrzymują wyniki egzaminów smsem, a kierowcy mogą płacić telefonem za parking[669]. Tak jak w wielu innych wysoko rozwiniętych krajach, Estonia w dużej mierze jest zależna od niezakłóconego, prawidłowego działania systemów komputerowych i źródeł komunikacji.

Estonia jako pierwszy suwerenny kraj na świecie stał się ofiarą zmasowanego cyberataku. W kwietniu i maju 2007 roku infrastruktura IT państwa została zaatakowana przez rosyjskich hakerów w odpowiedzi na przeniesienie, z centrum Tallina na cmentarz wojskowy, pomnika upamiętniającego żołnierzy Armii Czerwonej. Za pomocą DDoS[670] zostały zaatakowane główne strony rządowe, ale również instytucje komercyjne, banki, szkoły oraz dostawcy Internetu. Cyberatak odznaczał się znacznym stopniem zorganizowania, a przeprowadzone dochodzenie pokazało, że jego źródło miało miejsce w Rosji, choć rosyjski rząd zaprzeczył jakimkolwiek związkom z incydentem.

[669] M. Collier, *Estonia: Cyber Superpower*, „Transitions Online" 2007, nr 12/18, s. 2.
[670] DDoS - ang. *Distributed Denial of Service* - rozproszona odmowa usługi - więcej na ten temat w rozdziale 4.1.

Przez kilkanaście dni państwo było sparaliżowane, fala ataków na infrastrukturę informatyczną nasilała się, atakując strony internetowe parlamentu, Ministerstwa Obrony i Sprawiedliwości, policji, banków i niezależnych gazet. Ataki ustały ostatecznie w maju, jednakże unaoczniły, że małe państwo (jak Estonia) jest zupełnie bezbronne wobec cyberterroryzmu czy też innych form zmasowanej informatycznej napaści. Mimo, że ataki nie spowodowały znacznych szkód materialnych i realnego zagrożenia dla infrastruktury krytycznej efekt psychologiczny był ogromy. Rząd estoński wyciągnął prawidłowe wnioski z omawianego incydentu wprowadzając szereg nowych rozwiązań i uregulowań prawnych w różnych dziedzinach - bezpieczeństwa, bankowości, polityki oraz w innych sektorach. Można zaryzykować stwierdzenie, że atak stał się przyczynkiem do wkroczenia na kolejny - bardziej zaawansowany technologicznie i prawnie etap estońskiej polityki cyberbezpieczeństwa.

Estoński rząd we wrześniu 2014 roku zatwierdził Strategię Cyberbezpieczeństwa na lata 2014 - 2017[671], która stanowi kontynuację Strategii Cyberbezpieczeństwa na lata 2008 - 2013. Na skutek ataków w 2009 roku w Komitecie Bezpieczeństwa Estonii powołano Radę Cyberbezpieczeństwa, która miała odpowiadać za wspieranie różnych agencji na poziomie strategicznym oraz nadzorować realizację strategii bezpieczeństwa. Estońskiemu Centrum Informatycznemu w 2010 roku nadano status agencji rządowej i zmieniono nazwę na Estoński Urząd Systemu Informacji (est. *Riigi Infosüsteemi Amet*, RIA). RIA otrzymał uprawnienia do organizowania ochrony sieci informacyjno - komunikacyjnych, w tym infrastruktury krytycznej państwa. Celem RIA jest również wymiana informacji operacyjnych, identyfikacja problemów i rekomendowanie kierunków poprawy bezpieczeństwa infrastruktury krytycznej kraju. Estońska Agencja Bezpieczeństwa Wewnętrznego postawiła wzmocnić swoje zdolności dochodzeniowe w celu zapobiegania zagrożeniom dla bezpieczeństwa narodowego, w tym cyberataków i szpiegostwa[672].

Bardzo ciekawym i godnym naśladowania rozwiązaniem przyjętym w Estonii jest powołanie Jednostki Estońskiej Ligi Cyberobrony (ang. *Estonian Defence League's Cyber Unit* - EDL CU, est. *Kaitseliidu küberkaitse üksus*). Jest to dobrowolna organizacja zrzeszająca obywateli, mająca na celu ochronę estońskiej cyberprzestrzeni, czyli w założeniu „cyberarmia" czy też „cyberrezerwa". Jednostka składa się ze specjalistów w kluczowych zagadnieniach cyberbezpieczeństwa - głównie informatyków, lecz również prawników,

[671] Dokument dostępny na oficjalnej stronie internetowej Ministerstwa Gospodarki i Komunikacji Republiki Estonii: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf [21.11.16].
[672] Cyber Security Strategy 2014-2020, Ministry of Economic Affairs and Communication 2014, s. 2-3.

ekonomistów. Misją EDL CU jest ochrona infrastruktury krytycznej, wspieranie szerszych celów obrony narodowej, podniesienie poziomu bezpieczeństwa cybernetycznego przez edukację społeczeństwa i szkolenia, stworzenie sieci, która ułatwia partnerstwo publiczno - prywatne i zwiększa gotowość do działania podczas sytuacji kryzysowych. Wiedza ochotników EDL CU jest stosowana w celu poprawy bezpieczeństwa systemów informacyjnych estońskich instytucji państwowych i firm, przez skoordynowanie ćwiczeń, testowanie rozwiązań, szkoleń[673].

W Strategii Cyberbezpieczeństwa Estonii na lata 2014 - 2017 główne zagrożenia bezpieczeństwa cybernetycznego zidentyfikowano jako rosnące uzależnienie od infrastruktury ICT i e-usług przez państwo, gospodarkę i społeczeństwo. Kluczowymi obszarami strategii cyberbezpieczeństwa jest zapewnienie dostępu do podstawowych usług, skuteczniejsze zwalczanie cyberprzestępczości i pogłębianie narodowych zdolności obronnych. Dodatkowe działania wspierające będą obejmować: kształtowanie ram prawnych, promowanie międzynarodowej współpracy i komunikacji, podnoszenie świadomości oraz zapewnienie kształcenia specjalistycznego, jak również rozwój rozwiązań technicznych[674].

W omawianym dokumencie uznano, że strategia cyberbezpieczeństwa Estonii:

- stanowi integralną część bezpieczeństwa narodowego, wspomaga prawidłowe funkcjonowania państwa i społeczeństwa, konkurencyjność gospodarki oraz innowacje,
- gwarantuje poszanowanie podstawowych praw i wolności, a także chroni wolność jednostki, dane osobowe i tożsamość,
- działa opierając się na zasadzie proporcjonalności, przy uwzględnieniu istniejących i potencjalnych zagrożeń i zasobów,
- działa w sposób skoordynowany przez współpracę sektora publiczno, prywatnego oraz trzeciego sektora, z uwzględnieniem wzajemnych powiązań i współzależności pomiędzy istniejącą infrastrukturę i usługami w przestrzeni wirtualnej,
- rozpoczyna się od indywidualnej odpowiedzialności za bezpieczne korzystanie z narzędzi ICT,

[673] Ibidem, s. 3.
[674] Ibidem, s. 6.

- za priorytet uznaje zapewnienie bezpieczeństwa cybernetycznego jest przewidywanie, jak również zapobieganie potencjalnym zagrożeniom i skuteczne reagowanie na zagrożenia, które należy zmaterializować,
- musi być wspomagana przez międzynarodowe trendy badań i rozwoju,
- zapewnia cyberbezpieczeństwo państwa przez międzynarodową współpracę z sojusznikami i partnerami[675].

Estonia w 2003 roku ratyfikowała Konwencję Rady Europy o cyberprzestępczości, wprowadzając do swojego kodeksu karnego przepisy dotyczące takich przestępstw, jak sabotaż komputerowy (§ 206), celowe uszkodzenie połączeń do sieci komputerowej bądź systemu komputerowego (§ 207), rozpowszechnianie wirusów komputerowych (§ 208) czy też niedozwolone uzyskanie dostępu do komputera bądź sieci komputerowej (§ 217)[676]. Nowelizacja estońskiego kodeksu karnego wprowadziła przepis penalizujący cyberataki, jednakże z rozróżnieniem na ataki na infrastrukturę krytyczną (w celu poważnego wpłynięcia bądź zniszczenia ekonomicznej bądź społecznej struktury państwa) oraz na zwykłe przestępstwa komputerowe. Zmiany zaszły również w procedurze karnej, gdzie zmieniono postanowienia dotyczące pozyskiwania dowodów, w tym dowodów cyfrowych[677].

Na uwagę zasługuje ustanowiona w 2009 roku nowa ustawa o zarządzaniu awaryjnym, która stanowi przegląd bieżącej konfiguracji narodowej gotowości i struktury zarządzania awaryjnego, w tym w zakresie związanym z zagrożeniami cybernetycznymi. Ustawa oferuje kompleksowe podejście do problemu zarządzania kryzysowego: reguluje zapobieganie, przygotowanie, reagowanie na sytuacje awaryjne oraz łagodzenie skutków katastrofy. Ustawa nakłada na dostawców usług publicznych i właścicieli infrastruktury obowiązki zapewniające zapobieganie sytuacjom kryzysowym oraz zapewnienie stabilnego poziomu ciągłości usług. Dostawcy usług zostali zobowiązani między innymi do przygotowywania i przedstawiania oceny ryzyka, informowania obywateli o zdarzeniach istotnie wpływających na ciągłość świadczonych usług[678].

Wydarzenia sprzed kilku lat bezpośrednio przyczyniły się do zmiany prawa oraz powołania nowych instytucji mających na celu efektywną walkę z zagrożeniami w cyberprzestrzeni. Szczególną uwagę zwraca się nie tylko na pospolite cyberprzestępstwa, ale

[675] Cyber Security Strategy 2014-2020, Ministry of Economic Affairs and Communication 2014, s. 7.
[676] Estoński Kodeks Karny z dnia 06.06.2001 (RT I 2001, 61, 364). Wejście w życie 01.09.2002.
[677] C. Czosseck, R. Ottis, A. Talihärm, *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*, "International Journal of Cyber Warfare and Terrorism" 2011, t. 1, nr 1, s. 28.
[678] Ibidem s. 28.

również na cyberataki o podłożu politycznym, których celem może stać się najważniejsza infrastruktura. Analiza estońskiego porządku prawnego prowadzi do przekonania, iż władze podejmują właściwe kroki w celu zapewniania bezpiecznego funkcjonowania społeczeństwa obywatelskiego. By spełnić ten warunek musi być ono kompleksowo uregulowane prawnie w kilku dziedzinach. Estońskie ramy prawne dotyczące cyberprzestrzeni angażują prawo karne, regulacje dotyczące zarządzania kryzysowego i prawa konfliktów zbrojnych. Doświadczenia estońskie ukazują, że konieczne jest ustanowienie wspólnych standardów bezpieczeństwa dla wszystkich użytkowników sieci, systemów i firm zarządzających infrastrukturą krytyczną. Nie mniej ważne jest również zwiększenie poziomu świadomości społeczeństwa w zakresie cyberbezpieczeństwa przez edukację i szkolenia. Ciekawym rozwiązaniem jest również powołanie Jednostki Estońskiej Ligi Cyberobrony - cyberarmii, pozostającej w gotowości w przypadku wystąpienia cyberataku. Przyjęcie tego rozwiązania daje możliwość szybkiej reakcji na zagrożenie, stąd też tożsame regulacje, w mogą w niedługim czasie pojawić się w innych krajach.

Gruzja a cyberprzestrzeń

Gruzja, podobnie jak Estonia, stała się ofiarą cyberataku. W sierpniu 2008 roku w sposób pośredni wykorzystano cyberprzestrzeń do prowadzenia działań zbrojnych na Kaukazie. Rosyjscy hakerzy dopuścili się zmasowanego ataku na gruzińskie rządowe i komercyjne strony internetowe. Posłużono się atakami DDoS do zablokowania najważniejszych serwerów, w tym witryn o charakterze informacyjnym[679]. W rezultacie gruziński rząd stanął w obliczu niemalże całkowitego zablokowania dostępu od Internetu. W odpowiedzi rząd podjął niekonwencjonalny krok szukania „cyberschronienia" w Stanach Zjednoczonych i innych krajach. Bez uprzedniego uzyskania zgody rządu USA Gruzja przeniosła swe krytyczne zasoby informatyczne do USA, Estonii i Polski[680]. Mirosław Lakomy komentując gruzińskie wydarzenia stwierdził, że: „Co prawda nie wykorzystano tu Internetu do właściwych działań zbrojnych, jednak cyberataki miały istotne znaczenie dla bieżącej propagandy wojennej. Z tego punktu widzenia sukces rosyjskich hakerów pozwolił

[679] J. Joyner, *Comparing Transatlantic Versions of Cybersecurity,* [w:] D.S. Reveron, *Cyberspace and national security. Threats, Opportunities and Power in a Virtual World*, Waszyngton 2012, s. 161.
[680] S.W. Korns, J.E. Kastenberg, *Georgia's Cyber Left Hook*, "Parameters" 2008 - 2009, Winter Issue, s. 60.

Rosji na osiągnięcie pewnej przewagi politycznej w trakcie konfliktu, blokując jednocześnie możliwość prezentowania stanowiska przez Tbilisi. Istotne znaczenie miał także aspekt psychologiczny, związany z pozbawieniem gruzińskich obywateli dostępu do wielu najważniejszych usług internetowych. Przy czym należy pamiętać, iż Kreml nie podjął działań zmierzających do sparaliżowania infrastruktury krytycznej tego kraju"[681].

Konsekwencją ataku była zmiana gruzińskiej polityki w cyberprzestrzeni. Rząd wydał Strategię Cyberbezpieczeństwa Gruzji na lata 2012 - 2015[682], której celem było dostosowanie ustawodawstwa gruzińskiego do międzynarodowych standardów i nowych zagrożeń w cyberprzestrzeni. Główne zamierzenia Strategii to:

- badania i analizy - badanie doświadczeń i najlepszych praktyk innych państw, badania kryteriów i standardów identyfikacji obiektów krytycznych w systemach informacyjnych, analiza ich odporności na naruszenia,
- nowe normy prawne i regulacyjne - wprowadzenie regulacji prawnych zapewniających bezpieczeństwo informacji, ochronę infrastruktury krytycznej niezbędnej dla zachowania cyberbezpieczeństwa, wprowadzenie podstawy prawnej dla działalności CERT, ratyfikacja Konwencji RE o cyberprzestępczości,
- współpraca między podmiotami rządowymi dla zapewnienia bezpieczeństwa cybernetycznego - rozwój gruzińskiej grupy CERT, utworzenie międzynarodowego punktu kontaktowego 24/7 w sprawie cyberprzestępczości, ustalenie formatu i sposobów współpracy publiczno - prywatnej,
- wzrost świadomości w społeczeństwie i edukacja - w tym szkolenia dla podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej, w celu osiągnięcia lokalnych i międzynarodowych standardów ochrony,
- współpraca międzynarodowa - zacieśnienie współpracy w zakresie cyberbezpieczeństwa z organizacjami międzynarodowymi (OECD, UE, NATO, ITU)[683].

Część z wymienionych wyżej założeń została już spełniona. Gruzja w 2012 roku ratyfikowała Konwencję Rady Europy o cyberprzestępczości, zawęziła współpracę międzynarodową i powołała w swoich strukturach nowe organy mające na celu ochronę gruzińskiej cyberprzestrzeni. Jednym z tych organów jest między innymi CERT oraz Biuro

[681] M. Lakomy, op. cit., s. 148.
[682] Dokument dostępny na oficjalnej stronie internetowej gruzińskiego Biura Cyberbezpieczeństwa, http://csbd.gov.ge/bureau.php?lang=en [25.11.2016].
[683] Strategia Cyberbezpieczeństwa Gruzji na lata 2012 - 2015, s. 5-7.

Cyberbezpieczeństwa powołane przy Ministerstwie Obrony. Głównymi celami Biura Cyberbezpieczeństwa są:

- rozwój wspólnej polityki cyberbezpieczeństwa,
- zapewnienie bezpieczeństwa informacji i systemów technologii komunikacyjnych w sektorze obrony,
- wdrożenie i rozwój bezpieczeństwa komputerowego przez szybkie reagowanie za pomocą punków 24/7 na incydenty komputerowe,
- ochrona infrastruktury ICT w ramach Ministerstwa Obrony Gruzji przed zagrożeniami cybernetycznymi oraz cyberatakami,
- badanie w ramach Ministerstwa Obrony Gruzji istniejącej infrastruktury i praca nad poprawą jego bezpieczeństwa,
- harmonizacja ustawodawstwa gruzińskiego z międzynarodowymi normami prawnymi,
- przygotowanie odpowiednich ram prawnych przez programy takie, jak Polityka Cyberbezpieczeństwa czy Plan Działania na rzecz Rozwoju Cyberbezpieczeństwa,
- udział w programach edukacyjnych i szkoleniach,
- nawiązywanie współpracy na szczeblu krajowym i międzynarodowym,
- przekwalifikowanie personelu wojskowego według współczesnych standardów cyberbezpieczeństwa[684].

Paraliż komunikacyjny po ataku uświadomił gruzińskiemu rządowi konieczność zintensyfikowania działań obronnych w cyberprzestrzeni oraz zmian ustawodawstwa. Dobrym krokiem jest oczywiście ratyfikacja konwencji o cyberprzestępczości i powołanie organizacji zapewniającej stałą, międzynarodową komunikację w przedmiocie cyberbezpieczeństwa, w tym stałych punktów kontaktowych i zespołów CERT. Zgodnie z obowiązującym obecnie Narodowym Planem Bezpieczeństwa Gruzji rząd przyjął za cel opracowanie takiego systemu, który w przypadku cyberataku mógłby zminimalizować jego skutki i umożliwić szybkie odzyskanie sprawności działania sieci[685].

Niezwykle cenna jest wymiana doświadczeń pomiędzy różnymi podmiotami. W trakcie przeprowadzonego w 2015 roku polsko - gruzińskiego szkolenia Cyber Exe Gruzja, Szef Gruzińskich Sił Zbrojnych stwierdził, że: „Na tle dzisiejszych wyzwań hybrydowych,

[684] *Cyber Security Development Action Plan 2016 - 2017*, Ministry of Defence of Georgia Cyber Security Bureau, Tbilisi 2016 s. 31-32.
[685] National Security Concept of Georgia dostępny na oficjalnej stronie internetowej Ministerstwa Spraw Zagranicznych Gruzji: http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx?lang=en-US [22.11.2016].

bezpieczeństwo cyberprzestrzeni staje się ważniejsze niż bezpieczeństwo informacji w ogóle. Jak to mówią, kto jest właścicielem przestrzeni wirtualnej, posiada pole bitwy (...). Chcę podkreślić znaczenie tworzenia rezerw cybernetycznych, takiego podejścia wzajemnej współpracy urzędów cywilnych i wojskowych, które zwiększają zdolności obronne i wzmacniają państwo"[686]. Należy w pełni zgodzić się z tym stwierdzeniem. Ochrona cyberprzestrzeni państwa nie może odbywać się wyłącznie w sferze teoretycznej. Niezbędne jest tworzenie rezerw cybernetycznych, szkolenie sił wojskowych i podmiotów cywilnych oraz nieustanna współpraca międzynarodowa umożliwiająca wymianę najlepszych praktyk oraz informacji o zagrożeniach.

Doświadczenia Estonii i Gruzji wywarły realny wpływ na politykę innych państw. Społeczność międzynarodowa zrozumiała, że cyberprzestrzeń jest obszarem, który może być wykorzystany do ataku na państwo i jego infrastrukturę w konsekwencji doprowadzając do całkowitego paraliżu komunikacyjnego, odcięcia od źródeł dowodzenia i koordynacji. Efektem zmiany postrzegania paradygmatu bezpieczeństwa cyberprzestrzeni było uznanie, że cyberatak może stanowić naruszenie artykułu 5 Traktatu Północnoatlantyckiego.

Polska a cyberprzestrzeń

Polska systematycznie pada ofiarą ataków w cyberprzestrzeni. W październiku 2014 roku doszło do kradzieży danych osobowych z systemu Giełdy Papierów Wartościowych[687], oraz kradzieży i publikacji w Internecie danych z serwerów Ministerstwa Gospodarki[688], rok wcześniej rządowe strony internetowe zostały zaatakowane przez hakerów protestujących przeciwko podpisaniu przez Polskę umowy ACTA[689]. Mimo, że w Polsce nie doświadczyliśmy jeszcze tak zmasowanego ataku, jak to miało miejsce w Gruzji bądź Estonii zasadne wydaje się krótkie opisanie regulacji cyberbezpieczeństwa w naszym kraju.

[686] Dane z oficjalnej strony internetowej Cybsecurity.org, https://www.cybsecurity.org/cyber-exe-gruzja-2015/ [14.12.2016].
[687] Dane z oficjalnej strony internetowej Gazety Prawnej http://biznes.gazetaprawna.pl/artykuly/880266,raport-nik-polska-szeroko-otwarta-na-cyberataki.html [22.11.2016].
[688] Raport Najwyższej Izby Kontroli, Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, s. 21.
[689] Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi (ang. *Anti-Counterfeiting Trade Agreement)* porozumienie wielostronne, mające ustalić międzynarodowe standardy w walce z naruszeniami własności intelektualnej.

Polska jest stroną szeregu umów międzynarodowych związanych z cyberprzestrzenią. Za najważniejszą z całą pewnością należy uznać Konwencję o cyberprzestępczości sporządzoną 23 listopada 2001 roku w Budapeszcie. Mimo, iż RP podpisała konwencję 23 listopada 2001 roku to w wyniku opóźnień legislacyjnych jej ratyfikacja nastąpiła dopiero po kilkunastu latach - 12 września 2014 roku. Konwencja finalnie weszła w życie 19 listopada 2014 roku. Polska jest również związana prawem Unii Europejskiej oraz umowami międzynarodowymi*.

Dostosowanie prawa krajowego do międzynarodowych i europejskich standardów następowało stopniowo. Duża część zmian w polskim porządku karnym wynikała z obowiązku implementacji postanowień Konwencji RE o cyberprzestępczości oraz uregulowań Unii Europejskiej. W konsekwencji w polskim Kodeksie karnym wprowadzono penalizację takich cyberprzestępstw, jak hacking komputerowy (art. 267 § 1 k.k.), nielegalne uzyskanie dostępu do systemu informatycznego (art. 267 § 1 k.k.), sabotaż komputerowy (art. 287 k.k.) oszustwo i fałszerstwo komputerowe (art. 270 § 1 k.k. oraz 287 k.k.) szpiegostwo komputerowe (art. 130 § 2 k.k.) czy też pornografia dziecięca (art. 202 § 3, 4a i 4b k.k.).

Wzrost cyberprzestępczości, ataki cybernetyczne, cyberterroryzm oraz coraz większe znaczenie technologii informacyjno-komunikacyjnych w zarządzaniu państwem spowodowało, że konieczne stało się opracowanie planu ochrony przestrzeni wirtualnej o newralgicznym znaczeniu dla Polski. Dokumentem o szczególnym znaczeniu jest Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016. Uznano w nim, że cyberprzestrzenią jest: cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami, za cyberprzestrzeń RP uznano: cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)[690].

Najwyższa Izba Kontroli (NIK) zbadała stopień zabezpieczenia polskiej cyberprzestrzeni. Wyniki były druzgocące. W dokumencie wydanym 23 czerwca 2015 roku Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP NIK negatywnie ocenił realizację zadań podmiotów państwowych w zakresie ochrony cyberprzestrzeni RP. W trakcie kontroli ustalono, że administracja państwowa nie tylko nie

* Szczegółowo opisano te akty prawne w podrozdziale. 3.2.2.
690 Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016, s. 6.

podjęła niezbędnych działań mających na celu zabezpieczenie polskiej cyberprzestrzeni, ale niejednokrotnie kierownictwo nie było w ogóle świadome zagrożeń. Przede wszystkim uznano, że brak jest spójnej i systemowej koordynacji działań mającej na celu monitorowanie, przeciwdziałanie i minimalizowanie zagrożeń. Jako podstawowe błędy wskazano brak oszacowania ryzyk dla krajowej infrastruktury krytycznej, brak określonej struktury oraz ram prawnych narodowego systemu ochrony przestrzeni wirtualnej oraz procedur reagowania w przypadku wystąpienia sytuacji kryzysowej w cyberprzestrzeni.

W raporcie podkreślono bierność polskich organów: „Działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. Sprowadzały się one do doraźnego, ograniczonego reagowania na bieżące wydarzenia oraz biernego oczekiwania na rozwiązania, które w tym obszarze zaproponuje Unia Europejska. Kluczowym czynnikiem paraliżującym aktywność państwa w tym zakresie był brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych". Jedynie kilka obszarów ochrony cyberprzestrzeni zostało ocenionych pozytywnie - zaliczono do nich edukowanie społeczeństwa przez NASK[691] i Policję o zagrożeniach w cyberprzestrzeni, wysoki poziom zespołów CERT, utworzenie w MON systemu reagowania na incydenty komputerowe oraz wyspecjalizowanej jednostki - Narodowego Centrum Kryptologii.

Wobec tak znacznej krytyki, 22 stycznia 2015 roku Prezydent Rzeczpospolitej Polski podpisał dokument Doktryna cyberbezpieczeństwa Rzeczpospolitej Polskiej, który miał wzmocnić politykę bezpieczeństwa polskiej sieci wirtualnej. Cyberbezpieczeństwo Rzeczpospolitej Polskiej zostało scharakteryzowane jako „proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni"[692]. Główne zagrożenia cyberbezpieczeństwa Rzeczpospolitej Polskiej zidentyfikowano w obszarach takich, jak: cyberprzestępczość, cyberprzemoc, cyberprotesty, ataki na infrastrukturę krytyczną państwa sterowaną za pomocą systemów informatycznych. Uznano też, że podmioty prywatne są najbardziej narażone na kradzież danych, naruszenia integralności i poufności danych oraz dostępności usług. Z kolei

[691] NASK - Naukowa i Akademicka Sieć Komputerowa jest instytutem badawczym podległym Ministerstwu Cyfryzacji.
[692] Doktryna Cyberbezpieczeństwa Rzeczpospolitej Polskiej 2015, wydana przez Biuro Bezpieczeństwa Narodowego 22 stycznia 2015 r., s. 7.

sektory finansowy, energetyczny, transportowy, wysokich technologii oraz zdrowia publicznego są najbardziej narażone na ataki[693].

Za obszar podwyższonego ryzyka cyberbezpieczeństwa RP uznano wykorzystanie dla potrzeb bezpieczeństwa narodowego (militarnego, pozamilitarnego, wewnętrznego i zewnętrznego) wysoce zinformatyzowanych systemów technicznych obcej produkcji, w szczególności systemów walki i wsparcia (na przykład zautomatyzowanych systemów dowodzenia i kierowania), bez uzyskania dostępu do kodów źródłowych ich oprogramowania, gwarantujących posiadanie nad nimi informatycznej kontroli. Za źródło ryzyka uznano też integralność i nienaruszalność systemów teleinformatycznych administracji publicznej, nieodpowiednie finansowanie zespołów powołanych do koordynacji reagowania na incydenty komputerowe na poziomie krajowym czy też strukturę własności prywatnych operatorów i dostawców usług teleinformatycznych[694].

Zgodnie z przyjętą doktryną zapewnienie bezpieczeństwa cybernetycznego Rzeczpospolitej Polskiej powinno być realizowane w kilku płaszczyznach: przez sektor publiczny (w wymiarze krajowym i międzynarodowym) sektor prywatny (komercyjny), obywatelski oraz w wymiarze transektorowym. Zadania te można podzielić następująco:

- zadania sektora publicznego w wymiarze krajowym - rozpoznawanie zagrożeń, wymiana informacji, analiza ryzyka, zabezpieczenie kryptologiczne najważniejszych informacji, monitoring i szybkie reagowanie na incydenty w sieci oraz przeciwdziałanie cyberprzestępczości; równie istotny jest również stały audyt środków i mechanizmów cyberbezpieczeństwa, opracowanie procedur reagowania na cyberataki, planów reagowania kryzysowego oraz operacyjnych planów funkcjonowania w czasie zagrożenia i wojny oraz prowadzenie aktywnych działań cyberobrony, czyli obrona własnych zasobów teleinformatycznych,
- zadania sektora publicznego na poziomie międzynarodowym: międzynarodowa współpraca, wymiana informacji, doświadczeń i dobrych praktyk, oddziaływanie za pomocą organizacji międzynarodowych na transnarodowe struktury sektora prywatnego oraz partycypowanie w międzynarodowym reagowaniu na zagrożenia cybernetyczne, w szczególności w strukturach Unii Europejskiej i NATO,

[693] Ibidem, s. 10.
[694] Ibidem, s. 11-12.

- zadania sektora prywatnego: współpraca z sektorem publicznym w przedmiocie wymiany informacji o potencjalnych zagrożeniach dla cyberbezpieczeństwa, przeciwdziałanie zagrożeniem, opracowywanie propozycji zmian prawnych oraz wymiana informacji o zagrożeniach i incydentach,
- zadania sektora obywatelskiego: społeczne inicjatywy wspierające cyberbezpieczeństwo, edukowanie i samokształcenie w zakresie bezpieczeństwa w sieci,
- zadania transsektorowe: koordynacja współpraca sektora publicznego i prywatnego, tworzenie mechanizmów wymiany informacji oraz standardów i dobrych praktyk w zakresie cyberbezpieczeństwa[695].

Ministerstwo Administracji i Cyfryzacji wraz z Agencją Bezpieczeństwa Wewnętrznego wydało dokument Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej, w którym ustanawia trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w Cyberprzestrzeni RP. Poziom pierwszy - poziom koordynacji miałby być realizowany przez ministra do spraw informatyzacji. Drugi poziom reagowania na incydenty komputerowe składałby się z Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz podmiotu mającego na celu cyberobronę w sferze militarnej Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych. Ostatni poziom byłby sferą realizacji, w której administratorzy odpowiadaliby za konkretne systemy i sieci[696].

Na przestrzeni kilku lat różne organizacje rządowe wydały dokumenty mające na celu podział kompetencji i ustalenie polityki ochrony polskiej przestrzeni wirtualnej. Na aprobatę zasługuje powołanie nowych czy też wzmocnienie już istniejących jednostek reagowania na zagrożenia w sieci (na przykład CERT) oraz międzynarodowa wymiana doświadczeń i dobrych praktyk. Nie można jednak oprzeć się wrażeniu, że działania organizacji rządowych są nieskoordynowane. Dokumenty Doktryna Cyberbezpieczeństwa RP oraz Polityka Ochrony Cyberprzestrzeni RP miały zbudować ramy do realizacji polityki cyberbezpieczeństwa, tymczasem relacje pomiędzy aktami są luźne i nie do końca jasne. Brak jest jednego holistycznego dokumentu - na wzór rozwiązań krajów zachodnich - stanowiącego strategię cyberbezpieczeństwa naszego kraju. Wydaje się, że nieco bagatelizowane są kwestie obrony w przypadku wystąpienia cyberataku. Budowa cyberbezpieczeństwa kraju, nie może opierać

[695] Ibidem, s. 14-16.
[696] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013, s. 18.

się wyłącznie na rozwiązaniach instytucjonalnych na poziomie rządowym. Konieczne jest zaangażowanie obywateli w cyberobronę kraju, tak jak ma to miejsce chociażby w Estonii. Polska powinna wprowadzić realne mechanizmy ochrony cyberprzestrzeni RP, podjąć skoordynowane działania systemowe, ustanowić precyzyjne struktury zarządzania krajowym systemem ochrony cyberprzestrzeni wskazać jedną instytucję, która w przypadku cyberataku koordynowałaby działania służb. Równie istotne jest podjęcie współpracy podmiotów prywatnych i państwowych (między innymi w formie partnerstwa publiczno-prawnego) w celu zapewnienia odpowiedniego finansowania, wprowadzenia innowacyjnych technologicznie programów i działań mających na celu zapewnienie cyberbezpieczeństwa kraju.

3.2.2 Porządki prawne cybermocarstw

Stany Zjednoczone a cyberprzestrzeń

Stany Zjednoczone w maju 2011 roku przedstawiły swoją wizję międzynarodowej cyberprzestrzeni. Dokument o nazwie Międzynarodowa Strategia Cyberbezpieczeństwa. Dobrobyt, Bezpieczeństwo i Otwartość w Sieciowym Świecie (ang. *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*) podzielono na trzy części: budowanie polityki cyberprzestrzeni, przyszłość cyberprzestrzeni oraz priorytety polityki. Pierwsza część została uznana za fundament międzynarodowej polityki USA. Stany Zjednoczone w dokumencie zapowiedziały, że będą prowadzić politykę międzynarodową przestrzeni cyfrowej, która umożliwi kolejne innowacje, stymulację gospodarki i poprawę jakość życia w USA oraz w innych krajach. Mimo znacznych korzyści cyberprzestrzeni w aspekcie indywidualnym (walka z wykluczeniem społecznym), społecznym (szybsza reakcja służb ratunkowych, lepsza wymiana informacji), biznesowym (rozwój rynków zbytu) czy też rządowym (nowy globalny rynek idei, przepływ informacji) uznano, że przed USA stoją trzy podstawowe wyzwania w przestrzeni wirtualnej. Pierwsze z nich to podstawowe wolności, które powinny również podlegać ochronie w cyberprzestrzeni - zdolność poszukiwania, otrzymywania i przekazywania informacji za pośrednictwem dowolnego medium i bez

względu na granice państwowe. Podkreślono jednak, że wolność słowa i przepływu informacji nie powinna mieć charakteru bezwzględnego, konieczne ograniczenia muszą być jednak ściśle regulowane i dotyczyć najistotniejszych kwestii, czyli pornografii dziecięcej czy terroryzmu. Drugim wyzwaniem jest ochrona prywatności - w tym danych osobowych, w taki sposób by uchronić przed nieuprawnionym ich ujawnieniem, kradzieżą czy oszustwem. Trzecim wyzwaniem jest kwestia swobodnego przepływu informacji. W ocenie USA państwa nie powinny ograniczać swobodnego przepływu informacji w imię ochrony własnych sieci. Cyberprzestrzeń winna zostać przestrzenią otwartą i innowacyjną a najlepsze rozwiązania powinny być dynamiczne, szeroko akceptowalne oraz wyłącznie minimalnie wpływać na sieć[697].

Przyszłość cyberprzestrzeni ma opierać się na ogólnej dostępności, bezpieczeństwie i łatwości komunikacji. Firmy prywatne, w tym te opracowujące systemy i programy komputerowe, będą we współpracy z rządami szybko reagowały na zagrożenia w sieci i wspólnie opracowywały rozwiązania. Również w przypadku transgranicznego popełnienia przestępstwa organy ścigania powinny pogłębiać współpracę w celu wymiany informacji i danych oraz szybkiego i sprawnego zbierania dowodów, również tych cyfrowych[698]. Postanowienia te wydają się uzasadnione, ponieważ właśnie w Stanach Zjednoczonych mają siedziby najwięksi giganci branży IT - Google, Apple, Microsoft, Facebook i inni. Z jednej strony firmy te współpracują z organami sprawiedliwości - z drugiej protestują przeciwko odgórnym narzucaniem daleko idących zobowiązań. Przytoczyć tu trzeba chociażby sprawę Apple, która została wezwane przez FBI do ujawnienia kodu umożliwiającego odkodowanie iPhone'a należącego do Syeda Rizwana Farooka, który 2 grudnia 2015 roku zastrzelił w kalifornijskim San Bernardino 14 osób, a wiele innych ranił[699]. FBI finalnie wycofała pozew jednakże sprawa wywołała głośną dyskusję w z zakresie ochrony danych osobowych przechowywanych w telefonach komórkowych oraz możliwości ingerencji władz w oprogramowanie opracowane przez firmy prywatne.

Zgodnie z Międzynarodową Strategią Cyberbezpieczeństwa Stany Zjednoczone wspierają otwartą, interoperacyjną, bezpieczną i niezawodną infrastrukturę informacyjno -

[697] Międzynarodowa Strategia Cyberbezpieczeństwa. Dobrobyt, Bezpieczeństwo i Otwartość w Sieciowym Świecie, Akt wydany przez Prezydenta Stanów Zjednoczonych Ameryki, Waszyngton 2011, s. 3-5. Dokument dostępny online na oficjalnej stronie internetowej Białego Domu: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [10.10.2016].
[698] Ibidem, s. 7-9.
[699] Dane z serwisu Newsweek Polska http://www.newsweek.pl/nauka/iphone-kontra-fbi,artykuly,382922,1.html [10.10.2016].

komunikacyjną, która wspomaga międzynarodowy handel, wzmacnia bezpieczeństwo międzynarodowe, a także swobodną ekspresję i innowację. Charakter wolnościowy cyberprzestrzeni może być realizowany przez obniżenie ceny komputerów osobistych i dostępu do sieci, większą liczbę aplikacji i oprogramowania *open source* zachęcającego użytkowników do współdziałania i wymiany idei oraz rozwijania gospodarki cyfrowej. Podkreśla się, że reagowanie na incydenty w cyberprzestrzeni wymaga wzmocnienia współpracy i udostępnienia informacji technicznych z sektorem prywatnym i społecznością międzynarodową. Dokument akcentuje, że do przestrzeni wirtualnej powinny być odpowiednio stosowane powszechnie akceptowalne normy prawa międzynarodowego, czyli: przestrzeganie podstawowych wolności, prawo własności, ochrona prywatności, ochrona przed przestępstwami i prawo obrony koniecznej przewidziane między innymi w Karcie ONZ[700].

Polityka USA dotycząca cyberprzestrzeni wyrażona w Międzynarodowej Strategii Cyberbezpieczeństwa zakłada:

- promowanie międzynarodowych standardów, innowacji otwartych rynków - ochrona własności intelektualnej, włączając w to tajemnice handlowe, utrzymanie środowiska wolnego handlu nastawionego na nowe technologie i innowacje,
- ochrona własnych sieci przez zwiększenie ich bezpieczeństwa, niezawodności i elastyczności - promowanie współpracy w ramach społeczności międzynarodowej, ochrona infrastruktury krytycznej, zarządzanie kryzysowe, minimalizacja skutków ataków, odpowiedni dobór dostawców sprzętu hi-tech,
- współpraca w zakresie prawodawstwa - pełna współpraca w zakresie wypracowania międzynarodowej polityki dotyczącej cyberprzestępczości, harmonizacja prawa za pomocą implementacji Konwencji o cyberprzestępczości, uniemożliwienie terrorystom wykorzystania Internetu do zbierania funduszy, rekrutowania, komunikacji i ataków,
- wojskowe przygotowanie do wyzwań XXI wieku - rozpoznanie i dostosowanie potrzeb armii przez dostęp do niezawodnych i bezpiecznych sieci, budowanie i wzmacnianie istniejących sojuszy militarnych w kwestii potencjalnych zagrożeń w cyberprzestrzeni, współpraca z partnerami międzynarodowymi w celu budowania wspólnego cyberbezpieczeństwa,

[700] Międzynarodowa Strategia Cyberbezpieczeństwa, op. cit., s. 7-11.

- zarządzanie cyberprzestrzenią - promowanie otwartości i innowacyjności w cyberprzestrzeni, zachowanie globalnego bezpieczeństwa i stabilności sieci, włączając w to System Nazw Domenowych, promowanie otwartej dyskusji nad kwestią zarządzania Internetem z wieloma, zainteresowanymi podmiotami,
- rozwój międzynarodowy - zapewnienie bezpieczeństwa, dobrobytu, promowanie korzyści płynących z technologii sieciowych, zapewnianie wiedzy i szkoleń mających na celu budowanie potencjału technicznego i cyberbezpieczeństwa, międzynarodowa wymiana dobrych praktyk, zwalczanie cyberprzestępczości, w tym przez szkolenia organów ścigania, techników, prawników i ustawodawców,
- wolność Internetu - wspieranie podstawowych wolności i prywatności - wspieranie podmiotów społeczeństwa obywatelskiego oraz organizacji pozarządowych w osiągnięciu niezależnej, niezawodnej platformy wymiany myśli, poglądów, wypowiedzi i stowarzyszania się, zachęcanie do współpracy międzynarodowej na rzecz skutecznej ochrony prywatności danych handlowych.[701]

Wydana w 2015 roku Narodowa Strategia Bezpieczeństwa (ang. *National Security Strategy*) wskazuje zasady i priorytety amerykańskiej polityki oraz działania podejmowane w celu budowania amerykańskiej potęgi oraz zwiększania jej światowych wpływów. Strategia podkreśla wiodącą rolę USA w porządku międzynarodowym, zakładając współpracę z najważniejszymi europejskimi partnerami i organizacjami międzynarodowymi. Głównym celem w opisanym dokumencie jest bezpieczeństwo USA i jej partnerów, wzrost gospodarczy, szacunek dla krajowych i międzynarodowych wartości uniwersalnych oraz promowanie pokoju i bezpieczeństwa światowego. W Narodowej Strategii Bezpieczeństwa pokrótce odniesiono się również do wyznań związanych z cyberprzestrzenią. Uznano, że rośnie niebezpieczeństwo cyberataków, w tym ataków na infrastrukturę krytyczną. Zaakcentowano, że współzależność światowej gospodarki rośnie wraz z szybkim tempem zmian technologicznych, a osoby, firmy i państwa są obecnie powiązane ze sobą w nieprecedensowy i niespotykany dotychczas sposób[702].

Co ciekawe, Narodowa Strategia Bezpieczeństwa USA odnosząc się do cyberprzestrzeni, wskazuje, iż jest to przestrzeń wspólna tak jak przestrzeń kosmiczna czy morze otwarte, a zagrożenia w niej występujące są tożsame dla wszystkich narodów.

[701] Ibidem, s. 17-24.
[702] Narodowa Strategia Bezpieczeństwa USA, Akt wydany przez Prezydenta Stanów Zjednoczonych Ameryki, Waszyngton Luty 2015, s. 1-4. Dokument dostępny online na oficjalnej stronie internetowej Białego Domu: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy.pdf [10.10.2016].

Przestrzenie te umożliwiają swobodny przepływ osób, towarów, usług i idei. W omawianym dokumencie uznano je za „tętnice globalnej gospodarki i społeczeństwa obywatelskiego". W USA, w miejscu, w którym narodził się Internet, cyberbezpieczeństwo ma szczególne znaczenie. Dobrobyt i bezpieczeństwo kraju w coraz większym stopniu zależy od otwartego, interoperacyjnego, bezpiecznego i niezawodnego Internetu. Konieczne jest zatem zabezpieczenie sieci federalnych, oraz sieci sektora prywatnego w celu wzmocnienia bezpieczeństwa i odporności infrastruktury krytycznej. Szczególną rolę przypisano Kongresowi, który będzie wprowadzał nowe standardy prawne odpowiadające zmianom technologicznym. Rząd USA zakłada również, iż będzie pomagać innym krajom w opracowaniu odpowiednich przepisów prawnych, które w procesie standaryzacji pomogą przeciwdziałać cyberzagrożeniom. W Narodowej Strategii Bezpieczeństwa podkreśla się, że konieczne jest wprowadzenie międzynarodowych norm regulujących kwestię ochrony własności intelektualnej, wolności wypowiedzi w sieci, ochrony infrastruktury cywilnej, a sama cyberprzestrzeń powinna być zarządzana wspólnie przez państwa i sektor prywatny, włączając w to przedstawicieli internautów, jak i kluczowych interesariuszy[703].

Bardziej szczegółowe uregulowania dotyczące kwestii cyberbezpieczeństwa USA zostały omówione w wydanej w kwietniu 2015 roku Cyberstrategii Departamentu Obrony (ang. *The Departament of Defens Cyber Strategy*). Podkreślono w niej, że mimo, iż Internet został zaprojektowany jako otwarty system wymiany informacji, to obecnie jest konieczne zagwarantowanie bezpieczeństwa cybernetycznego państwa. Podmioty państwowe i niepaństwowe prowadzą operacje w cyberprzestrzeni w celu osiągnięcia różnych celów politycznych, gospodarczych i wojskowych. Kraje mogą próbować uderzyć nie tylko w instytucje rządowe, ale również prywatne, jak to miało miejsce w listopadzie 2014 roku, kiedy prawdopodobnie w odwecie za wydanie satyrycznego filmu o Korei Północnej doszło do cyberataku na Sony Pictures Entertainment, naruszenia informacji handlowych Sony oraz kradzieży tysięcy dokumentów cyfrowych zawierających poufne dane pracowników[704].

Departament Obrony w wydanym przez siebie dokumencie założył, że w przypadku konfliktu potencjalny przeciwnik, aby uzyskać strategiczną przewagę, będzie starał się zaatakować infrastrukturę krytyczną i wojskową. By tego uniknąć, konieczne jest podjęcie

[703] Narodowa Strategia Bezpieczeństwa USA, Akt wydany przez Prezydenta Stanów Zjednoczonych Ameryki, Waszyngton Luty 2015, s. 7-22

[704] Cyberstrategia Departamentu Obrony Stanów Zjednoczonych Ameryki, wydany przez Sekretariat Obrony USA, kwiecień 2015, s. 1-2. Dokument dostępny on-line https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [10.10.2016].

kroków w celu zmniejszenia zagrożeń cybernetycznych - rządy, firmy i organizacje muszą zweryfikować systemy i bazy niezbędne do ochrony, oceny ryzyka w przypadku wystąpienia cyberataków. Departament Obrony USA buduje strategię cyberbezpieczeństwa mającą na celu ochronę interesów narodowych, włączając w to dyplomację, interesy informacyjne, wojskowe, gospodarcze, finansowe i narzędzia ścigania. Ostatnia Strategia Działania w Cyberprzestrzeni Departamentu Obrony (ang. *Department of Defense Strategy for Operating in Cyberspace* - DDSOC) z maja 2011 roku wskazywała kierunki wsparcia interesów narodowych w zakresie cyberprzestrzeni. Nowa strategia wprowadza następujące cele strategiczne i cele dla działań cybernetycznych i misji Departamentu Obrony na lata 2015-2020: budowanie cyberbezpieczeństwa, ochrona sieci, systemów i informacji Departamentu Obrony, ochrona narodu przed szeroko zakrojonymi atakami, opracowanie wsparcia operacyjnego i planów awaryjnych. By zrealizować wyżej wymienione cele cyberbezpieczeństwo musi być budowane razem z rządem federalnym, innymi agencjami rządowymi, międzynarodowymi sojusznikami i partnerami oraz przede wszystkim w porozumieniu z sektorem prywatnym[705].

Cyberstrategia Departamentu Obrony podkreśla ważkość prawidłowej koordynacji zadań i wymiany informacji pomiędzy kluczowymi agencjami (Departamentem Obrony, Departamentem Bezpieczeństwa Wewnętrznego, FBI) i organizacjami międzynarodowymi. Wymiana doświadczeń oraz informowanie o potencjalnych zagrożeniach jest niezbędne do efektywnej walki z incydentami w sieci. Twórcami nowych technologii są w znacznej części instytucje prywatne. Departament Bezpieczeństwa buduje bezpieczeństwo swoich sieci we współpracy z firmami prywatnymi, na przykład z korporacjami lotnictwa cywilnego, w celu opracowania nowych systemów sterowania, które będą obsługiwały krytyczną infrastrukturę zaawansowanych systemów sił powietrznych na całym świecie[706].

W CDO przedstawiono trzy podstawowe cele amerykańskiej cyberstrategii. Po pierwsze, Departament Bezpieczeństwa musi chronić własne sieci, systemy i informacje. Cyberprzestrzeń stała się miejscem działań operacyjnych, wobec czego konieczne jest organizowanie szkoleń oraz odpowiednie wyposażenie amerykańskich sił zbrojnych. Tak jak w czasach zimnej wojny siły zbrojne muszą być również przygotowane do działania w miejscu o ograniczonym dostępnie do cyberprzestrzeni i tym samym źródeł łączności.

[705] Cyberstrategia Departamentu Obrony Stanów Zjednoczonych Ameryki, wydany przez Sekretariat Obrony USA, kwiecień 2015, s. 2-3.
[706] Ibidem, s. 3-4.

Drugim celem jest przygotowanie na ewentualne skutki dużego ataku. Należy zidentyfikować jakie negatywne konsekwencje mogą zaistnieć w zakresie ochrony życia, mienia, ekonomii i polityki zagranicznej USA. Trwają prace nad zorganizowaniem zintegrowanego systemu pomiędzy organami państwowymi i stanowymi, który w przypadku ataku zminimalizowałby jego skutki i zasięg oraz przyśpieszył koordynację działań. Trzecim celem jest wykorzystanie wojskowe cyberprzestrzeni. W DDSOC dopuszcza się ewentualność, że cyberprzestrzeń będzie - za zgodą Prezydenta USA bądź Sekretarza Obrony - wykorzystywana w celu wsparcia operacji wojskowych i planów awaryjnych, między innymi przez niszczenie wrogiej sieci lub infrastruktury wojskowej. Uznano, że siły wojskowe USA mogą używać cyber operacji do zakończenia trwającego konfliktu „na amerykańskich warunkach" (ang. „*United States military might use cyber operations to terminate an ongoing conflict on U.S. terms"*), bądź zakłócać sieci wojskowe przeciwnika, by uniemożliwić mu użycie siły. Dopuszczono, również, razem z innymi agencjami użycie United States Cyber Command (używa się również nazwy USCYBERCOM[707]) w celu usunięcia potencjalnych zagrożeń. Podkreślono jednak, że każda decyzja o przeprowadzeniu operacji w cyberprzestrzeni będzie podejmowana z najwyższą starannością i rozwagą[708].

Departament Obrony wyznaczył sześć celów strategicznych w swoich misjach w cyberprzestrzeni. Należą do nich budowa i utrzymanie sił zdolnych do prowadzenia operacji w przestrzeni wirtualnej, obrona i zabezpieczenie sieci Departamentu Obrony oraz wprowadzenie procedur powodujących minimalizację skutków ataków. Za niezbędne uznano, przygotowanie do obrony USA i jej interesów przed destrukcyjnymi atakami na infrastrukturę krytyczną oraz ataki, o możliwych poważnych konsekwencjach. Ponadto, należy opracować cybernarzędzia, które dadzą możliwość kontrolowania eskalacji konfliktu i kształtowania jego przepływu. Ostatnim celem strategicznym jest budowanie i utrzymywanie silnych międzynarodowych sojuszy i partnerstwa w celu zniechęcenia potencjalnych sprawców oraz zwiększenia bezpieczeństwa międzynarodowego[709].

Warto również przytoczyć kilka aktów prawnych, które realizują powyższe założenia. 18 grudnia 2014 roku uchwalono ustawę o cyberbezpieczeństwie narodowym (ang. *The*

[707] United States Cyber Command (w skrócie USCYBERCOM bądź CYBERCOM) są to siły zbrojne podporządkowane United States Stategic Command. USCYBERCOM powstała w 2009 roku, jest organem, w którym centralizuje się dowództwo operacji podejmowanych w cyberprzestrzeni i synchronizuje się ochronę sieci wojskowych USA.
[708] Cyberstrategia Departamentu Obrony Stanów Zjednoczonych Ameryki, wydany przez Sekretariat Obrony USA, kwiecień 2015, s. 4-6.
[709] Ibidem, s. 13-15.

National Cybersecurity Protection Act of 2014)[710], która zmieniła ustawę o bezpieczeństwie narodowym z 2002 roku (ang. *The Homeland Security Act of 2002*). Ustawa powołuje krajowe centrum do spraw Cyberbezpieczeństwa i Komunikacji, które ma na celu koordynację działań Departamentu Bezpieczeństwa Krajowego USA oraz nadzorowanie ochrony infrastruktury krytycznej, bezpieczeństwa cybernetycznego i programów powiązanych z Departamentem Bezpieczeństwa Krajowego. Centrum będzie odpowiedzialne za stworzenie federalnego systemu, który umożliwi ostrzeganie przed zagrożeniami w cyberprzestrzeni, koordynację w czasie rzeczywistym działań operacyjnych w jednostkach federalnych i stanowych, ułatwienie koordynacji międzysektorowej zagrożeń i incydentów, które mogą mieć wpływ na wiele systemów oraz zapewnienie pomocy technicznej, zarządzanie ryzykiem oraz opracowanie rekomendacji w zakresie narzędzi ochrony. Ustanowiono ponadto procedury nakładające obowiązek informowania Kongresu oraz Prokuratora Generalnego o naruszeniach bezpieczeństwa informacji niejawnych oraz cybeatakach na agencje rządowe[711].

Nie można zapomnieć, że w Stanach Zjednoczonych obowiązuje równolegle prawo federalne, stanowe i miejscowe wzbogacone o system precedensowy. Ciężko zatem mówić o wspólnej, spójnej legislaturze w zakresie prawa cyberprzestrzeni. W prawie federalnym wprowadzono regulacje penalizujące najpoważniejsze cyberprzestępstwa takie, jak: oszustwo internetowe, pornografia dziecięca, sprzedaż przez Internet leków na receptę, których obrót jest kontrolowany, hazard internetowy, piractwo komputerowe czy naruszenia praw własności intelektualnej. W ustawach szczegółowych zostały uregulowane kwestie ochrony prywatności w sieci[712], bezpieczeństwa danych finansowych[713], ochrony praw konsumenta[714], dzielenia się informacjami o zagrożeniach[715] czy też o partnerstwie publiczno - prywatnym w celu poprawy cyberbezpieczeństwa[716].

USA jest kolebką cyberprzestrzeni. W kraju tym mają również siedzibę najwięksi giganci branży komputerowej. Stany Zjednoczone jako światowe mocarstwo próbuje wytaczać drogę dla innych państw. Nie można jednak oprzeć się wrażeniu, że proponowane przez nich zmiany mają głównie na celu zabezpieczenie indywidualnych interesów. Z jednej

[710] The National Cybersecurity Protection Act of 2014, Public Law 113-282.
[711] The National Cybersecurity Protection Act of 2014, Public Law 113-282
[712] Cyber Privacy Fortification Act of 2015. H.R. 104,
[713] Data Security Act of 2015, H.R. 2205.
[714] Consumer Privacy Protection Act of 2015, H.R. 2977.
[715] Cyberthreat Sharing Act of 2015, S. 456.
[716] Cybersecurity Enhancement Act of 2014, P.L. 113-274.

strony USA nawołuje do wzmocnienia współpracy międzynarodowej i zachowania wolnościowego charakteru cyberprzestrzeni z drugiej dopuszcza militarne wykorzystanie przestrzeni wirtualnej do zakończenia konfliktu „na amerykańskich warunkach". USA chciałoby pełnić rolę „światowego policjanta" narzucając pewne rozwiązania. Na aprobatę oczywiście zasługuje część z przyjętych propozycji - współpraca w zakresie prawodawstwa, promowanie otwartości cyberprzestrzeni, współpraca transgraniczna oraz kooperacja z sektorem prywatnym. Zrozumieć również można chęć zaostrzenia przyjętych do tej pory rozwiązań. Stany Zjednoczone są jednym z najczęściej atakowanych w przestrzeni wirtualnej krajów. Zgodnie z ostatnimi doniesieniami prasowymi rosyjscy hakerzy manipulowali w trakcie kampanii wyborczej w czasie wyborów prezydenckich w USA w 2016 roku pomiędzy Hilary Clinton a Donaldem Trumpem, próbując zdyskredytować i obniżyć zaufanie do kandydatki Demokratów[717]. Skutkiem cyberataku było wydalenie 35 rosyjskich dyplomatów oraz zastosowanie innych sankcji. Sytuacja ta ukazuje jak wielką rolę odgrywa obecnie cyberbezpieczeństwo państwa.

Prawo i polityka wewnętrzna USA wywiera realny wpływ nie tylko na kształtowanie się prawa cyberprzestrzeni, ale codzienne życie milionów ludzi. Firmy takie, jak Facebook, Google czy Microsoft podlegają prawu amerykańskiemu - w zakresie prywatności, baz danych, praw własności intelektualnej. USA swoją polityką i wewnętrznym prawodawstwem może promować wolnościowy charakter cyberprzestrzeni bądź przyjąć zgoła odmienne podejście narzucając wyśrubowane obowiązki sektorowi prywatnemu (na przykład obowiązek udostępniana danych czy technologii). USA jako mocarstwo ogromną rolę przykłada do swojego bezpieczeństwa - również w cyberprzestrzeni. Stany Zjednoczone dysponują ogromnym potencjałem militarnym, finansowym, ale również technologicznym i personalnym, który jest w stanie proponować zupełnie nowe, innowacyjne rozwiązania. Część państw może wzorować krajowe rozwiązania na prawie USA, inni wbrew przeciwnie, w obawie przed militarnym mocarstwem będą wprowadzać normy chroniące własną przestrzeń cyfrową przed możliwą inwigilacją ze strony Stanów Zjednoczonych.

[717] Dane z serwisu Newsweek Polska http://www.newsweek.pl/swiat/rosyjscy-hakerzy-ingerowali-w-wybory-w-usa-co-na-to-donald-trump-,artykuly,402729,1.html [10.01.2017].

Rosja a cyberprzestrzeń

Rosja nie jest krajem o wysokim stopniu zaawansowania technologicznego. Jest to jednak państwo, które często pojawia się w doniesieniach prasowych w kontekście cyberataków w cyberprzestrzeni. Federacja Rosyjska została wskazana jako agresor i źródło ataku w sporze z Estonią i Gruzją. Manipulowanie amerykańską kampanią wyboczą odbyło się na tak dużą skalę, że niemal pewne jest, iż akcja zaplanowana została na poziomie rządowym. Z kolei epizod estoński został uznany za pierwszą „cyberwojnę". W trakcie konfliktu z Gruzją cyberataki były skorelowane z rosyjskimi atakami militarnymi. Mimo, że trudno jest przypisać ataki bezpośrednio władzom rosyjskim, nie ulega wątpliwości, iż Rosja dużą wagę przykłada do kwestii swojej cyberobronności i bez wątpienia w sposób jawny bądź niejawny jest bardzo aktywna w przestrzeni wirtualnej. Rosyjskie poglądy na temat charakteru, potencjału i wykorzystania cyberprzestrzeni w istotny sposób różnią się do zachodniego konsensusu. Normy, które zachód uznaje za oczywiste w Rosji są postrzegane jako zagrożenie. Czynnikiem utrudniającym wypracowanie wspólnych norm okazuje się również być brak wspólnego słownictwa oraz wspólnych pojęć odnoszących się do cyberprzestrzeni[718].

W Rosji swobodny przepływ informacji jest w dalszym ciągu dużym problemem dla władzy. Na Kremlu panuje przekonanie, że media powinny być narzędziem władzy w kreowaniu określonego, pozytywnego wizerunku kraju i panującego rządu. Przykładem takiego stanowiska może być zatwierdzony przez Władimira Putnia w sierpniu 2000 roku Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej (ang. *Information Security Doctrine of the Russian Federation*). Plan ten jest podstawowym dokumentem regulującym podejście Rosji do bezpieczeństwa informacji, w tym informacji w cybernetycznej przestrzeni. Dokument jest przeznaczony do „zapewniania konstytucyjnych praw i wolności człowieka i obywatela do swobodnego poszukiwania, uzyskiwania, przekazywania, tworzenia i rozpowszechniania informacji za pomocą bliższych środków prawnych. Dogłębna analiza dokumentu doprowadziła jednak Keir'a Gilesa do stwierdzenia, iż media - zarówno państwowe jak i prywatne są Rosji narzędziem państwa w kształtowaniu opinii publicznej w sposób korzystny dla władz"[719]. Wolnościowy charakter przestrzeni wirtualnej, swobodny

[718] K. Giles, *Russia's Public Stance on Cyberspace Issues*, [w:] C. Chosseck, R. Ottis, K. Ziolkowski (red.), *2012 4th International Conference on Cyber Conflict*, Talin 2012, s. 64.
[719] Ibidem, s. 70.

przepływ informacji oraz swoboda wyrażania poglądów i potencjalna możliwość dotarcia do dużej rzeszy odbiorców jest problematyczna dla władz rosyjskich. Przypomnieć należy, że w późnych latach dziewięćdziesiątych Federalna Służba Bezpieczeństwa Federacji Rosyjskiej nakładała na rosyjskich dostawców sieci obowiązek instalowania oprogramowania bądź udostępniania danych, dzięki którym FSB mogło zapoznać się z treściami udostępnianymi przez rosyjskich internautów. Nickolas K. Gvosdev uważa, iż współczesne obowiązujące akty prawne w gruncie rzeczy mają na celu podobne działanie. Akty prawa krajowego umożliwiają zdalny dostęp z biura FSD do danych sieci, umożliwiających lokalizację telefonu, e-maila czy smsa[720].

Prezydent Federacji Rosyjskiej 10 stycznia 2000 roku dekretem nr 24 zatwierdził Narodowy Plan Bezpieczeństwa Federacji Rosyjskiej (ang. *National Security Concept of the Russian Federation*), który stanowi zbiór poglądów na temat sposobu zabezpieczenia jednostki, społeczeństwa i państwa przed zagrożeniami zewnętrznymi i wewnętrznymi w każdej sferze życia Rosjan. Narodowy Plan Bezpieczeństwa Federacji Rosyjskiej punkt III poświęca omówieniu zagrożeń narodowego bezpieczeństwa państwa - wymieniono w nim szeroki zakres potencjalnych niebezpieczeństw - terroryzm, przestępczość zorganizowana, spadek aktywności inwestycyjnej i innowacji, bezpieczeństwo energetyczne. Uznano, iż następuje osłabienie naukowe, techniczne i technologiczne kraju, ograniczone zostały badania strategiczne w ważnych dziedzinach nauki i technologii oraz następuje odpływ specjalistów i naukowców za granicę. Uznano zatem, że Rosja stoi w obliczu groźby utraty swojej czołowej pozycji w zakresie innowacyjności rozwiązań i technologii, prowadzącej do osłabienia branży rodzimych nowych technologii. Trend ten powoduje uzależnienie się od zagranicznych technologii i rozwiązań, co w konsekwencji może doprowadzić do podważenia rosyjskich zdolności obronnych. W Narodowym Planie Bezpieczeństwa Federacji Rosyjskiej uznano, że państwo stoi przed coraz większym zagrożeniem bezpieczeństwa narodowego w sferze informacyjnej. Stwierdzono, iż wiele krajów dąży do zdominowania cyberprzestrzeni i odsunięcia Rosji od zewnętrznego i wewnętrznego rynku informacyjnego. Jako zagrożenie uznano fakt, że szereg państw opracowuje koncepcję wojen informacyjnych, które przewidują „utworzenie niebezpiecznego wpływu" na sfery informacyjne innych krajów, zakłócają

[720] N. K. Gvosdev, *The Bear Goes Digital. Russia and Its Cyber Capabilities*, [w:] D.S. Reveron (red.), *Cyberspace and national security. Threats, Opportunities and Power in a Virtual World*, Waszyngton 2012, s. 173 - 179.

normalne funkcjonowanie systemów informatycznych i telekomunikacyjnych oraz niezawodność przechowywania zasobów informacyjnych[721].

W punkcie IV Narodowego Planu Bezpieczeństwa Federacji Rosyjskiej wymieniono zadania, które mają na celu zapewnienie bezpieczeństwa narodowego Rosji. W sferze cyberbezpieczeństwa położono nacisk na wzmocnienie organów ścigania, przede wszystkim jednostek przeciwdziałania przestępczości zorganizowanej i terroryzmowi. Głównymi zadaniami w zapewnieniu bezpieczeństwa Federacji Rosyjskiej stała się realizacja konstytucyjnych praw i swobód obywateli Rosji w sferze działań informacyjnych, poprawy i ochrony krajowej infrastruktury informacyjnej oraz integracji Rosji w światową przestrzeń informacyjną i przeciwdziałania zagrożeniom w cyberprzestrzeni[722].

Zatwierdzona w maju 2009 roku Narodowa Strategia Bezpieczeństwa Federacji Rosyjskiej do 2020 roku (ang. *Russia's National Security Strategy to 2020*) wskazuje priorytety strategiczne w polityce krajowej i międzynarodowej. Wśród zagrożeń wymieniono: amerykański plan wdrożenia w Europie systemu ochrony przeciwrakietowej, terroryzm, ekspansję NATO, ale również zagrożenia cybernetyczne w obszarze nowych technologii[723].

Wydaje się, że Rosja nie jest zainteresowana przyjęciem wspólnych międzynarodowych norm dotyczących cyberprzestępczości. Do tej pory Federacja Rosyjska nie przystąpiła do Konwencji Rady Europy o cyberprzestępczości. Do rosyjskiego kodeksu karnego wprowadzono jednak przepisy penalizujące pewne działania w sieci takie, jak: uzyskanie nielegalnego dostępu do komputera (art. 272 k.k.), ingerencja w system komputerowy (art. 273 k.k.), pornografia dziecięca (art. 242 i 242.1 k.k.) czy też przestępstwa związane z naruszeniem praw własności intelektualnej (art. 146 i 147 k.k.). Część przepisów została ujęta w odrębnych aktach prawnych ustawą federalną nr 307-FZ z dnia 10 października 2014 r. wprowadzono zmiany do ustawy o ochronie dzieci przed informacjami szkodliwymi dla ich zdrowia i rozwoju, ustawą federalną nr FZ-152 o ochronie danych osobowych, czy też dekretem prezydenckim nr 31s w sprawie ustanowienia systemu

[721] *National Security Concept of the Russian Federation*, Zatwierdzone dekretem Prezydenta nr 24 z dnia 10 stycznia 2000 r. Dokument w języku angielskim dostępny online: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768 [10.10.2016].
[722] Ibidem.
[723] *Russia's National Security Strategy to 2020*, 12 maja 2009, nr. 537. Dokument w języku angielskim dostępny online: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf [10.10.2016].

państwowego do wykrywania, zapobiegania i eliminowania skutków cyberataków na informacyjne zasoby Federacji Rosyjskiej[724].

W Rosji powołano również centrum reagowania na incydenty w rządowych systemach informatycznych. Instytucja ta nosi nazwę GOV CERT.RU i koordynuje działania w dziedzinie wykrywania, zapobiegania i zwalczania nielegalnej działalności związanej z ingerencją w zasoby sieciowe organów rządowych. Z kolei RU-CERT jest centrum reagowania na incydenty w sieci pozarządowej, i tak jak inne zespoły CERT monitoruje sieć w poszukiwaniu incydentów oraz wpiera rosyjskie i zagraniczne podmioty w zakresie wykrywania, zapobiegania i zwalczania nielegalnej działalności. Oprócz dwóch wymienionych instytucji w Rosji powołano specjalny organ do monitorowania cyber incydentów w sektorze kredytowym i finansowym. Organ o nazwie FinCERT stanowi jedną z procedur zabezpieczeń i ochrony danych Banku Rosji. Omawiany podmiot zbiera dane na temat bezpieczeństwa cybernetycznego spółek finansowych, analizuje je, zapewnia informacje dla firm kredytowych i finansowych o możliwych zagrożeniach bezpieczeństwa informacji oraz zapewnia rekomendacje ma wypadek cyberataków. FinCERT współpracuje również z organami Federalnej Służby Bezpieczeństwa[725].

Wskazane dokumenty w swych założeniach mają głównie chronić państwo w przestrzeni wirtualnej. Nie ulega jednak wątpliwości, iż Rosja była, jest i będzie wykorzystywała cyberataki do realizacji swojej polityki, bądź też jako element prowadzonego przez siebie konfliktu zbrojnego. Uwypuklić należy, że Rosja we współczesnym wirtualnym świecie wydaje się również być podatna na cyberataki. Jest to kraj, który w perspektywie ogólnokrajowej nie ma wystarczających środków finansowych na konieczne inwestycje w technologie informatyczne, które skutecznie uchroniłyby ją przed hakerami z Chin czy USA. Wykorzystuje, więc młode osoby oraz rosyjski nacjonalizm do podbudzania haktywizmu również w celach politycznych. W trakcie konfliktu pomiędzy Rosją i Gruzją w 2008 roku, by zostać „cyfrowym żołnierzem" w „Kremlowskiej armii zero - jedynkowej"[726] wystarczyło jedynie postępować, z ogólnie dostępnymi informacjami zawartymi na blogach w RUTNET'cie. Rosyjskie wojsko i służby bezpieczeństwa poszukują również hakerów, którzy będą pracować dla państwa stopniowo tworząc mniej lub bardziej oficjalną cyberarmię[727].

[724] Danie z oficjalnej strony internetowej ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Russia.pdf [01.12.2016].
[725] Ibidem.
[726] Nawiązanie do komputerowego programowania zero-jedynkowego.
[727] N. K. Gvosdev, op. cit., s. 181-183.

Były ultranacjonalistyczny członek Rosyjskiej Dumy Nikolai Kurjanowicz stwierdził, że w niedalekiej przyszłości wiele konfliktów nie będzie odgrywało się na polu bitwy, lecz raczej w sieci Internet, gdzie walczyć będą cyber - żołnierze, czyli hakerzy. Oznacza to, że mała grupa hakerów jest silniejsza niż wielotysięczna armia obecnych sił zbrojnych[728]. Należy bacznie obserwować kroki podejmowane przez władze rosyjskie w zakresie cyberprzestrzeni. Wydaje się, że Rosja coraz śmielej wykorzystuje przestrzeń wirtualną do realizacji swoich celów. Ataki rosyjskich hakerów następują z ukrycia, lecz nie można oprzeć się wrażeniu, że często są sterowane bezpośrednio z Kremla. Rosyjskie akty prawne w przeciwieństwie do ich zachodnich odpowiedników nie nawołują do zacieśnienia współpracy międzynarodowej czy wymiany doświadczeń. Rosyjska cyberprzestrzeń ma służyć rosyjskim interesom oraz budowaniu militarnej potęgi technologicznej.

Rosyjska polityka dotycząca cyberprzestrzeni w sposób bezpośredni wpływa na kształtowanie się propozycji prawnych państw zachodnich. Potencjalna możliwość uznania cyberataku za zbrojną napaść na członka Sojuszu Północnoatlantyckiego jest tego skutkiem. Sprzeczne interesy supermocarstw powodują, że niezwykle trudno będzie opracować w przyszłości konwencyjne ramy prawne zachowań w cyberprzestrzeni. Rosja uznaje wzmocnienie cyberbezpieczeństwa NATO za wrogi krok w jej kierunku, co prowadzi do intensyfikacji nielegalnych działań w świecie wirtualnym.

Chiny a cyberprzestrzeń

W Chińskiej Republice Ludowej Internet pojawił się po raz pierwszy w 1994 roku. Zaledwie po czterech latach liczba chińskich użytkowników sieci wynosiła dwa miliony[729]. Obecnie zgodnie z danymi Internet Live Stats w 2016 roku w Chińskiej Republice Ludowej około 52 % populacji miało dostęp do sieci - jest to ponad 721 milionów internautów[730]. Jest to naprawdę przytłaczająca liczba, zważywszy na fakt, że dotyczy pojedynczego kraju, w którym zasady posługiwania się cyberprzestrzenią drastycznie odbiegają od zachodnich standardów. Powszechnie wiadomo, że rząd chiński od lat cenzuruje swoim obywatelom

[728] Ibidem, s. 184.
[729] N. Inkster, *China in Cyberspace*, [w:] D.S. Reveron, *Cyberspace and national security. Threats, Opportunities and Power in a Virtual World*, Waszyngton 2012, s. 191.
[730] Dane z oficjalnej strony internetowej Internet Live Stats http://www.internetlivestats.com/internet-users/china/ [01.12.2016].

dostęp do treści zgromadzonych w przestrzeni wirtualnej. Za pomocą ponad sześćdziesięciu różnych aktów prawnych rząd kontroluje ruch i udostępniane w Internecie treści. Jedną z podstawowych metod jest blokowanie treści w znanych wyszukiwarkach internetowych chociażby Yahoo! System automatycznie zablokuje wyniki wyszukiwania przy takich słowach, jak: demokracja, dyktatura, prawa człowieka, ludobójstwo czy antykomunizm. Akcję blokowania treści powszechnie nazywa się „Chińskim Murem Ogniowym" czy „Wielkim Firewallem" - jest to nawiązanie do Wielkiego Muru oraz zabezpieczeń sieciowych, które są nazywane zaporami ogniowymi (ang. *firewall*). Za cenzurowanie sieci jest odpowiedzialne Ministerstwo Przemysłu Informatycznego, ale faktycznie podmiotem decyzyjnym jest Departament Propagandy Chińskiej Partii Komunistycznej[731].

Opracowano katalog rzeczy zakazanych w chińskim Internecie. Sformułowania są tak niejasne i ogólne, iż jako działalność wywrotową można traktować niemal wszystko. Przykładowo niedozwolone jest:

- naruszanie podstawowych zasad wyrażonych w konstytucji,
- zagrażanie bezpieczeństwu narodu, ujawnianie tajemnic państwowych, obalanie reżimu krajowego lub zagrożenie integralności i jedności kraju,
- szkodzenie honorowi i interesom narodu,
- podżeganie do nienawiści bądź rasizmu wobec narodów,
- naruszenie krajowych regulacji dotyczących religii, propagowanie złych kultów i feudalnych przesądów,
- rozpowszechnianie plotek zakłócających porządek społeczny lub zakłócenie stabilności społecznej,
- rozpowszechnianie treści obscenicznych, pornografii, hazardu, przemocy, terroru lub podżeganie do popełnienia przestępstwa,
- obrażanie lub zniesławianie bądź naruszanie praw osób trzecich,
- podżeganie do nielegalnych zgromadzeń, stowarzyszeń, marszy czy spotkań, które zakłócają porządek społeczny,
- prowadzenie działalności w imieniu nielegalnej organizacji cywilnej,
- wszelkie inne treści zabronione przez prawo lub przepisy[732].

[731] *How Censorship Works in China: A Brief Overview*, Human Rights Watch https://www.hrw.org/reports/2006/china0806/3.htm [01.12.2016].
[732] Ibidem.

Praktyka pokazała, że cenzura Internetu nie miała tak naprawdę na celu ograniczenia treści generujących nienawiść czy zakłócających porządek społeczny. W rzeczywistości przepisy te są wykorzystane do cenzurowania opinii stojących w sprzeczności z oficjalnym stanowiskiem rządu, czy zwierających informacje, które chiński rząd uważa za kłopotliwe bądź niewygodne. Chińskie przepisy stoją w jawnej sprzeczności z międzynarodowymi standardami ochrony praw człowieka, wyrażonych chociażby w art. 19 ust. 2 Międzynarodowego Paktu Praw Obywatelskich i Politycznych, który stanowi, że „Każdy człowiek ma prawo do swobodnego wyrażania opinii; prawo to obejmuje swobodę poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób według własnego wyboru"[733]. Zgodnie z prawem międzynarodowym, rządy mają prawo do ograniczania swobodnego przepływu informacji wyłącznie w ściśle określonych przypadkach takich, jak bezpieczeństwo państwa czy moralność publiczna. Decyzja o ograniczeniu treści winna być proporcjonalna oraz zgodna z międzynarodowymi standardami ochrony prawa do informacji. Chiński przykład pokazuje, że cenzura sieci ma na celu jedynie ochronę interesów partii komunistycznej i walkę z przeciwnikami dyktatury.

Władza ustawodawcza Chińskiej Republiki Ludowej 7 listopada 2016 roku przyjęła szeroko krytykowaną w świecie zachodnim ustawę o cyberbezpieczeństwie, która wejdzie w życie w czerwcu 2017 roku. Rząd chiński argumentował, iż jest to rozwiązanie przyjęte wobec rosnących cyberzagrożeń, czyli włamań i terroryzmu[734]. Jednakże, tak naprawdę wspomniany akt prawny jest nowym regresywnym środkiem wzmacniającym cenzurę, nadzór i kontrolę nad chińskim Internetem.

Chińska ustawa o cyberbezpieczeństwie nakłada na szereg firm obowiązek cenzurowania „zakazanych" informacji i ogranicza anonimowość w cyberprzestrzeni przez nałożenie obowiązku podania prawdziwego imienia, nazwiska i danych osobowych, oraz nałożenie na krytycznych operatorów infrastruktury informatycznej obowiązku „zapisywania informacji osobistych i ważnych danych biznesowych w Chinach". Zgodnie z nią na firmy mają obowiązek monitorowania i raportowania dla rządu niezidentyfikowanych „incydentów bezpieczeństwa sieci", jak również zapewnienia nieokreślonej „pomocy technicznej" dla agencji obrony, co stwarza obawy nieuzasadnionego zwiększenia nadzoru nad siecią. Nowa

[733] Dz.U. z 1977 r., Nr 38, poz. 167.
[734] Dane z serwisu The Guardian https://www.theguardian.com/world/2016/nov/07/chinas-new-cybersecurity-law-sparks-fresh-censorship-and-espionage-fears [01.12.2016].

ustawa wprowadza daleko idące mechanizmy kontroli. Do aktu został wprowadzony przepis, który zabrania używania cyberprzestrzeni do „obalenia ustroju socjalistycznego" i „fabrykowania lub rozpowszechniania fałszywych informacji w celu zakłócenia porządku gospodarczego". W trakcie prac nad ustawą wprowadzono przepis, który zakazuje wykorzystania Internetu do „wzbudzenia separatyzmu lub uszkodzenia jedności narodowej", oraz zakazuje zakładania stron internetowych i grup komunikacyjnych, które są wykorzystane do „szerzenia metod przestępczych" lub „innych informacji związanych z nielegalnymi i przestępczymi działaniami". Przepisy te dają dla chińskiego rządu kolejne narzędzia do karania niewinnych osób krytykujących obecny rząd. Ustawa zostanie wykorzystana do walki z ruchami wolnościowymi, pokojowymi aktywistami, którzy będą skazywani na surowe kary więzienia pod zarzutem rzekomego sabotowania Chińskiej Republiki Ludowej. Ustawa z całą pewnością przyczyni się do dalszej autocenzury w mediach społecznościowych i obaw o swobodne wyrażenie swojej opinii w przestrzeni wirtualnej. Nowe regulacje są niejasne, niejednoznaczne i dają dużą możliwość dowolnej interpretacji oraz naruszeń[735].

Chińskie przepisy dotyczące cyberprzestrzeni można uznać za najbardziej obszerne i restrykcyjne na świecie. Co najmniej dwanaście agencji rządowych sprawuje pełną władzę nad chińskim Internetem, w tym wszechmocny Państwowy Urząd Informacji, Ministerstwo Bezpieczeństwa Publicznego i Ministerstwo Przemysłu Informatycznego, odpowiedzialne za licencjonowanie i rejestrację wszystkich dostawców sieci. Ciągle postępujące zmiany legislacyjne rozszerzają cenzurę i kontrolę na nowe technologie telefony komórkowe, nowe formy ekspresji, czyli blogi czy media społecznościowe. Oczywistym jest, że chińskie władze nie są w stanie zapewnić całkowicie szczelnej cenzury, jednakże stworzone ramy prawne mają istotny i bezpośredni wpływ na ilość informacji dostępnych w chińskiej przestrzeni wirtualnej[736].

Należy zwrócić szczególną uwagę na fakt, że działalność władz chińskich nie ogranicza się jedynie do własnego terytorium i znajdującym się w jego granicach osób. Chiński rząd stworzył armię hackerów, którzy mają za zadanie nie tylko chronić chińską cyberprzestrzeń, ale również aktywnie atakować określone podmioty na rozkaz władzy. W 2013 roku Stany Zjednoczone po raz pierwszy bezpośrednio oskarżyły chińskie władze o

[735] Dane z oficjalnej strony internetowej Human Rights Watch https://www.hrw.org/news/2016/11/06/china-abusive-cybersecurity-law-set-be-passed [01.12.2016].
[736] *How Censorship Works in China: A Brief Overview*, Human Rights Watch https://www.hrw.org/reports/2006/china0806/3.htm [01.12.2016].

przeprowadzenie cyberataków na amerykańskie sieci komputerowe[737]. Z kolei w 2015 roku miał miejsce ogromny cyberatak na rządowe amerykańskie rządowe komputery, w trakcie którego doszło do kradzieży poufnych informacji około 21,5 mln osób[738]. Amerykanie podejrzewali, że atak został przeprowadzony na polecenie chińskich władz. Zgodnie z doniesieniami prasowymi chińscy hakerzy działający na zlecenie Pekinu przez ataki zdobywają tajne informacje o amerykańskich programach obronnych, gospodarczych i dyplomatycznych. Szpiegostwo komputerowe nie ogranicza się jedynie do próby zdobycia informacji tajnych, ale również do kradzieży najnowocześniejszych technologii. Jak wynika ze statystyk, od kilku lat najwięcej cyberataków miało swoje źródła właśnie w Chinach[739].

W maju 2015 roku wydano dokument Strategia Militarna Chin, w którym uznano, że to właśnie państwo chińskie jest najczęściej atakowanym krajem na świecie. Zgodnie z poglądem wyrażonym we wskazanym dokumencie światowa rewolucja wojskowa wkroczyła w zupełnie nowy etap - precyzyjnej, inteligentnej, bezzałogowej broni i sprzętu. Cyberprzestrzeń i kosmos stały się strategicznym elementem rozwoju armii, a nowoczesna wojna ewoluuje w kierunku informatyzacji. Chińska władza podkreśla, że światowe mocarstwa aktywnie przystosowują swoje krajowe strategie bezpieczeństwa i politykę obronną do wojny w cyberprzestrzeni. Rewolucyjne zmiany technologii wojskowych i nowa forma wojny ma znaczący wpływ na międzynarodowy krajobraz polityczny i wojskowy, który - w ocenie Pekinu - stanowi poważne wyzwanie dla bezpieczeństwa militarnego Chin. Wobec tak zidentyfikowanych zagrożeń Chiny zdecydowały się na utworzenie i rozwój „cyber - sił zbrojnych" - organizacji, która będzie reagować na cyberzagrożenia, utrzymywać bezpieczeństwo sieci narodowej i stabilność społeczną[740]. Cyberarmia jest zbudowana przez hakerów - informatyków, studentów, graczy internetowych i przestępców, który posiadają odpowiednie umiejętności i zgodzili się pracować z rządem[741]. Nie należy łudzić się, iż cyberarmia ma na celu wyłącznie obronę przed cybeatakami. Jednym z powodów jej powołania jest podejmowanie działań cyberszpiegostwa, pozyskiwanie informacji oraz przeprowadzanie ataków na inne kraje.

[737] Dane z serwisu TVN24 http://www.tvn24.pl/wiadomosci-ze-swiata,2/usa-otwarcie-oskarzyly-chiny-o-cyberataki-pekin-to-nieodpowiedzialne,323843.html [01.12.2016].
[738] Dane z serwisu Newsweek Polska: http://www.newsweek.pl/swiat/potezny-cyberatak-na-usa-hakerzy-z-chin-wykradli-dane-amerykanow,artykuly,366557,1.html [01.12.2016].
[739] Dane ze strony internetowej Statista: https://www.statista.com/statistics/440582/ddos-attack-traffic-by-originating-country/ [01.12.2016].
[740] Dokument Strategia Militarna Chin dostępny w języku angielskim na stronie internetowej: https://news.usni.org/2015/05/26/document-chinas-military-strategy [01.12.2016].
[741] N. Inkster, op. cit., s. 202.

3.2.3 Porządki prawne krajów determinowane postępem technologicznym

Japonia a cyberprzestrzeń

Japonia jest krajem zaawansowanym technologiczne. To właśnie w kraju Kwitnącej Wiśni powstały takie koncerny związane z najnowszymi technologiami, jak Toshiba, Sony, Jujitsu czy Sharp Electronics. Społeczeństwo japońskie zaliczyć należy do społeczeństwa informacyjnego, w którym sprawne działanie cyberprzestrzeni jest niezbędne do niezakłóconego jego funkcjonowania.

W listopadzie 2014 roku japoński parlament wydał Zasadniczy Akt o Cyberbezpieczeństwie[742]. Nowelizacją ustawy z 2016 roku Rządowemu Centrum Cyberbezpieczeństwa oraz Narodowemu Centrum Szybkiego Reagowania na Incydenty w Cyberprzestrzeni przyznano możliwość monitorowania bezpieczeństwa cyberprzestrzeni. W ramach agencji powołano osoby zajmujące się przetwarzaniem informacji, które po zdaniu odpowiedniego ministerialnego egzaminu biorą czynny udział w budowaniu cyberbezpieczeństwa Japonii - uczestniczą w seminariach dotyczących bezpieczeństwa przestrzeni wirtualnej i są obowiązani do zachowania poufności uzyskanych danych.

Pierwsza strategia cyberbezpieczeństwa Japonii została opracowana w 2013 roku. Dwa lata później we wrześniu 2015 roku rząd Japonii przygotował Strategię Cyberbezpieczeństwa uznając cyberprzestrzeń za niezbędny fundament japońskiej działalności społeczno - gospodarczej. W japońskiej Strategii cyberbezpieczeństwa jako podstawową zaletę cyberprzestrzeni uznano swobodę globalnej wymiany idei, myśli i innowacji bez względu na granice państwowe. Stwierdzono, że przestrzeń wirtualna jest podstawą dla działań społeczno gospodarczych w kraju. Wraz z pojawieniem się społeczeństwa informacyjnego, w którym przestrzeń wirtualna i realna są wysoce zintegrowane wszystkie rodzaje obiektów fizycznych i osób stały się połączone ze sobą bez względu na ograniczenia fizyczne. Z tych też względów rząd japoński uznał cyberzagrożenia

[742] Ustawa nr 104 z 2014 r. Akt dostępny na stronie internetowej: http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm [20.11.2016].

za kluczowe wyzwanie bezpieczeństwa narodowego, mogące realnie wpłynąć na ekonomię i codzienne życie milionów Japończyków[743].

W strategia cyberbezpieczeństwa wyznaczono pięć celów strategicznych:

- zapewnienie wolnego przepływu informacji (ang. *Assurance of the Free Flow of Information*) - uznano, że powinno się zachować wolnościowy charakter cyberprzestrzeni. Należy w pełni przestrzegać zasad swobodnego przepływu informacji, ze zwróceniem szczególnej uwagi na ochronę prywatności; niezbędne jest zachowanie zdroworozsądkowej równowagi pomiędzy niezbędnymi prawnymi regulacjami w cyberprzestrzeni a ochroną prywatności i swobodnej wymiany informacji,
- zasady prawa (ang. *The Rule of Law*) - krajowe i międzynarodowe zasady prawa winny być stosowane do cyberprzestrzeni, co więcej, ze względu na możliwość zastosowania wielu porządków prawnych konieczne jest opracowanie w tej kwestii uniwersalnych, międzynarodowych zasad; przestrzeń ta winna opierać się na zasadach wolności, demokracji, pokoju i stabilności dla całej międzynarodowej społeczności. Japonia zobowiązuje się aktywnie angażować się w rozwój i wdrażanie międzynarodowych przepisów i norm w tym zakresie,
- otwartość (ang. *Openness*) - rząd japoński podkreślił, że cyberprzestrzeń nie może zostać ograniczona do wyłącznie do określonej grupy podmiotów; podkreślono wolnościowy i otwarty charakter przestrzeni wirtualnej,
- autonomia (ang. *Authonomy*) pokreślono, że dla zapewniania współistnienia i porządku w cyberprzestrzeni należy uszanować jej autonomię,
- współpraca z różnymi podmiotami (ang. *Collaboration among Multi - stekeholders*) - cyberprzestrzeń jest obszarem wielowymiarowym, dlatego też konieczne jest współdziałanie podmiotów publicznych i prywatnych w celu jej ochrony, a rząd powinien spełniać funkcję koordynatora[744].

Oprócz wyżej wymienionych zasad, rząd postawił sobie kilka celów mających za zadanie poprawę bezpieczeństwa japońskiej cyberprzestrzeni. Prowadzone są prace nad wzmocnieniem zdolności reagowania na zagrożenia, zarówno przez organy ścigania jak i siły zbrojne, wzmocnienia koordynowania wymiany informacji między podmiotami publiczno-

[743] *Cybersecurity strategy September 2015*, dostępny na oficjalnej stronie internetowej japońskiej National Center of Incident Readiness and Stategy for Cybersecurity, http://www.nisc.go.jp/eng/index.html [20.11.2016 r].
[744] *Cybersecurity strategy September 2015*, s. 8-10.

-prawnymi. Nie mniej istotne jest zapewnienie cyberbezpieczeństwa chroniącego najbardziej zaawansowaną technologicznie japońską infrastrukturę (energię jądrową, technologie związane z przestrzenią kosmiczną, zaawansowane wyposażenie sił zbrojnych). Strategia szczególny nacisk kładzie na aktywne przyczynienie się do rozwoju międzynarodowych zasad i norm dotyczących cyberprzestrzeni w organizacjach międzynarodowych w tym, w ONZ. Za szczególnie palące uznano rozwiązanie problemu wykorzystania cyberprzestrzeni przez organizacje terrorystyczne[745].

Zmianą polityki cyberbezpieczeństwa determinuje zmiany prawne. Japonia uchwaliła w 2013 roku nową ustawę o ochronie tajemnic państwowych, która reguluje kwestię ochrony informacji niejawnych. Implementowano nią rygorystyczne praktyki bezpieczeństwa danych uznanych przez rząd japoński za tajemnicę państwową. W 2014 roku ustanowiono ustawę o cyberbezpieczeństwie, która wprowadza ochronę infrastruktury krytycznej oraz konieczność informowania o incydentach w cyberprzestrzeni[746]. Zauważyć należy, że Japonia dość wcześnie dostrzegła potrzebę regulacji praw nowych technologii. W 1999 roku ustanowiono ustawę o nieautoryzowanym dostępie do komputera[747], penalizującą tego typu czyny. Niezależnie jednak od przyjętego ustawodawstwa Japonia w 2011 roku przystąpiła, a rok później ratyfikowała Konwencję Rady Europy o cyberprzestępczości[748].

Kanada a cyberprzestrzeń

W Kanadzie w 2008 roku blisko 60% zeznań podatkowych wypełnianych było *on-line*, a niemal 70% bankowości Kanadyjczycy dokonywali za pomocą przestrzeni wirtualnej[749]. Ponad 90 % kanadyjskich firm używa Internetu, co bardzo korzystnie wpływa na rozwój gospodarki, aplikacji mobilnych i nowych technologii. Również rząd w dużej mierze opiera się na niezakłóconym działaniu przestrzeni wirtualnej. Na ponad 130 rządowych serwisach *on-line* można rozliczyć się z podatków, zawnioskować o kredyt

[745] Ibidem, s. 35-40.
[746] Dane z oficjalnej strony internetowej National Center of Incident Readiness and Stategy for Cybersecurity, http://www.nisc.go.jp/eng/index.html [20.11.2016].
[747] Ustawa nr 128 z 1999 r.
[748] D. Ventre, *Cyberspace in Japan's New Defence Strategy*, [w:] D. Ventre (red.) *Cyber Conflict. Competing National Perspectives*, Londyn, 2012, s. 215-217.
[749] Dane z oficjalnej strony internetowej kanadyjskiego Ministerstwa Bezpieczeństwa https://www.publicsafety.gc.ca/cnt/bt/mnstr-en.aspx [02.12.2016].

studencki czy dokonać czynności związanych z ubezpieczeniem społecznym. Kanadyjski rząd uznaje zatem kwestię cyberbezpieczeństwa za jeden z kluczowych elementów polityki państwa, zwłaszcza, że stosowane przez przestępców metody stają się coraz bardziej wyrafinowane i zaawansowane technologicznie[750].

W Kanadzie za cyberprzestępczość jest uznawane przestępstwo popełnione z udziałem komputera jako przedmiotu przestępstwa (hacking, phishing, spam) bądź jako narzędzie służące do jego popełnienia (hate crimes, pornografia dziecięca, oszustwa komputerowe). Departament Sprawiedliwości, Kanadyjska Królewska Policja Konna, Ministerstwo Spraw Zagranicznych i inne organy współpracują ze sobą w celu zapewnienia cyberbezpieczeństwa państwa. Współpraca podejmowana jest ponadto na poziomie regionalnym, federalnym, ale też międzynarodowym. Rząd Federalny 3 października 2010 roku rozpoczął program kanadyjskiej strategii cyberbezpieczeństwa (ang. *Canada's Cyber Security Strategy*), powołano również Kanadyjskie Centrum Reagowania na Cyber - Incydenty (ang. *Canadian Cyber Incident Response Centre*), które ma monitorować, reagować na zagrożenia oraz koordynować działania służb w przypadku wystąpienia ataku[751].

Rząd kanadyjski głównych źródeł zagrożeń w cyberprzestrzeni dopatruje się w kilku czynnikach: cyberprzestępczości (kradzież tożsamości, pranie brudnych pieniędzy, oszustwa), cyberterroryzmowi czy wykorzystaniu cyberprzestrzeni przez wywiad i służby wojskowe państw obcych. Wobec tak zdefiniowanych zagrożeń cyberbezpieczeństwo Kanady jest budowane na trzech filarach:

- zabezpieczenia systemów rządowych - przez sformułowanie jasnych zadań i obowiązków poszczególnych organów rządowych w dziedzinie cyberbezpieczeństwa, odpowiednie zadania zostały przydzielone Kanadyjskiemu Centrum Reagowania na Cyber - Incydenty (monitoring i reagowanie na incydenty), służbie wywiadu (analiza krajowych i międzynarodowych zagrożeń, w tym zagrożeń dla informatycznej infrastruktury krytycznej), Ministerstwu Spraw Zagranicznych i Handlu (pomoc w opracowaniu międzynarodowego wymiaru bezpieczeństwa cybernetycznego i cyberbezpieczeństwa polityki zagranicznej),
- współpracy w celu zabezpieczenia ważnych systemów cybernetycznych znajdujących się poza rządowym systemem federalnym - przez wzmocnienie współpracy z

[750] Canada's Cyber Security Strategy. For a stronger and more prosperous Canada, Canada 2010, s. 2.
[751] Ibidem, s. 3.

jednostkami samorządu terytorialnego zapewniających szeroki zakres podstawowych usług dostępnych *on-line* (w szczególności poprzez ochronę baz danych, w tym rejestrów publicznych, rejestrów medycznych czy podatkowych). Nie mniej ważne jest zacieśnienie współpracy publiczno-prawnej, zwłaszcza w zakresie ochrony infrastruktury krytycznej,

- pomoc Kanadyjczykom w bezpiecznym poruszaniu się w cyberprzestrzeni - przez edukację i informowanie o cyberzagrożeniach[752].

W 2013 roku dokumencie o nazwie *Action Plan 2010-2015 for Canada's Cyber Security Strategy* podsumowano dotychczasową strategię cyberbezpieczeństwa. Od 2012 roku rządowa infrastruktura IT otrzymała dodatkowe finansowanie zapewniające zwiększenie bezpieczeństwa państwa, podpisano porozumienie z USA o zwiększeniu współpracy w zakresie cyberbezpieczeństwa obu krajów, zintensyfikowano też współpracę z konkretnymi podmiotami krajowymi (Wielką Brytanią, Nową Zelandią i Australią) oraz organizacjami międzynarodowymi (NATO, G8, ONZ) w zakresie wymiany wiedzy i wzmocnienia międzynarodowej współpracy w dziedzinie bezpieczeństwa sieci wirtualnej[753].

Jako jedynie przykład innych aktów prawnych odnoszących się do cyberprzestrzeni można wskazać ustawę antyspamową, która została przyjęta 1 lipca 2014 roku. Zakazuje ona wysyłania handlowych wiadomości elektronicznych bez zgody odbiorcy (w tym na portalach społecznościowych i na telefony komórkowe) oraz instalacji programów komputerowych bez wyraźnej zgody właściciela systemu komputerowego. Ustawa antyspamowa zakazuje również wykorzystania fałszywych lub wprowadzających w błąd oświadczeń internetowych w promocji produktów i usług oraz gromadzenia baz danych przez nielegalny do nich dostęp, bądź wykorzystanie adresów e-mail bez zgody ich właścicieli[754]. 10 marca 2015 roku weszła w życie ustawa o ochronie Kanadyjczyków od przestępstw *on-line* (ang. *The Protecting Canadians from Online Crime Act*)[755]. Aktem zmodernizowano przepisy odnoszące się do dowodów elektronicznych i nowego środowiska cyfrowego, znowelizowano przepisy o ochronie konkurencji i ochronie danych komputerowych w zakresie przechowywania i przekazywania danych finansowych. Ustawa wprowadza przepisy dotyczące wzajemnej pomocy prawnej w sprawach karnych oraz nowe uprawnienia śledcze.

[752] Ibidem, s. 9-13.
[753] *Action Plan 2010-2015 for Canada's Cyber Security Strategy*, Canada 2013, s. 5-9.
[754] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23).
[755] Protecting Canadians from Online Crime Act (S.C. 2014, c. 31).

Kanadyjskie prawo wciąż dostosowuje swoje regulacje do nowych zagrożeń w cyberprzestrzeni. Szczególną uwagę zwraca się na partnerstwo publiczno - prywatne, które w Kanadzie ma długą tradycję. Niezbędna jest koordynacja działań nie tylko na poziomie rządowym czy samorządowym. Duża część danych, infrastruktury i zasobów korzysta bądź jest przechowywana w rękach prywatnych, chociażby w postaci dostawców usług sieciowych. Prawidłowym rozwiązaniem jest nawiązanie ściślejszej współpracy organizacjami międzynarodowymi oraz bezpośrednim sąsiadem - USA i wspólne opracowanie strategii cyberobrony w niezbędnych punktach wspólnych[756]. Technologie informacyjno - komunikacyjne oraz cyfrowe media to jedne z najszybciej rozwijających się sektorów kanadyjskiej gospodarki. Z Kanady pochodzą firmy produkujące oprogramowanie, sprzęt komputerowy (chociażby BlackBerry), ale również aplikację na telefony oraz gry komputerowe. Sprzyjająca polityka i kanadyjskie prawo powodują, iż najwięksi komputerowi giganci otwierają tam centra badawczo - rozwojowe ICT (Ericsson, Alcatel, Microsoft)[757]. Dzięki przyjętym rozwiązaniom i szeroko zakrojonym partnerstwem publiczno - prywatnym branża ICT stanowi motor wzrostu gospodarczego w Kanadzie.

Podsumowanie

Rozwiązania przyjęte przez organizacje i instytucje międzynarodowe oraz poszczególne państwa stanowią próbę zmierzenia się z kwestią regulacji zachowań w cyberprzestrzeni. Wszystkie wyszczególnione wyżej akty prawne i dokumenty łączy jednak wspólny mianownik. Jest nim problem w zakreśleniu kompetencji i uprawnień państw w zakresie regulowania przestrzeni wirtualnej. Szczególnym wyzwaniem jest ustalenie granic jurysdykcji państw, zwłaszcza że część z nich podejmuje kroki w celu znacznego rozszerzenia swojego władztwa jurysdykcyjnego. Spór w zakresie jurysdykcji stawia oczywiście pytanie o prawo właściwe w przypadku popełnienia cyberprzestępstwa, działań terrorystów w przestrzeni wirtualnej czy kwestii związanych z codziennym życiem miliona ludzi - handlem elektronicznym czy granicami wolności słowa.

[756] H. Loiseau, L. Lemay, *Canada's Cyber Security Policy: a Tortuous Path Toward a Cyber Security Strategy*, [w:] D. Ventre (red.), *Cyber Conflict. Competing National Perspectives*, Londyn 2012, s. 3-9.
[757] Dane z serwisu Canada Trade: https://canada.trade.gov.pl/pl/analizy-rynkowe/142788,rynek-ict-w-kanadzie.html [26.03.2017].

Opisane w niniejszym rozdziale organizacje międzynarodowe podejmują próbę regulowania najbardziej newralgicznych kwestii związanych z działalnością człowieka w cyberprzestrzeni. Organizacją o największym zasięgu jest oczywiście ONZ, która działając za pomocą swoich wyspecjalizowanych agencji proponuje rozwiązania w zakresie cyberprzestępczości (UNODC) czy handlu elektronicznego (UNICITRAL). Podmiotem, który może w przyszłości odegrać szczególnie ważną rolę jest Forum Zarządzania Internetem, które jest nowym modelem tworzenia wspólnej polityki na poziomie międzynarodowym. Wprawdzie IGF nie może wydawać decyzji merytorycznych, lecz wydaje się, iż wydawanie rekomendacji w formie modelu *soft law* może sprawdzić się w odniesieniu do przyszłych wyznań związanych z regulacją cyberprzestrzeni.

Szczególną uwagę należy zwrócić na pracę regionalnych organizacji międzynarodowych oraz ich wkład w tworzenie się cyberprawa. Jednym z pierwszych holistycznych aktów prawnych poruszających problem działalności kryminalnej człowieka w cyberprzestrzeni była Konwencji Rady Europy o cyberprzestępczości. Do wskazanej umowy międzynarodowej przystąpiło wiele państw również spoza Rady Europy, a niezliczona liczba państw nowelizowała swoje krajowe kodeksy karne, wprowadzając penalizację cyberprzestępstw właśnie opierając się na wspomnianym traktacie. Konwencja o cyberprzestępczości zawiera jednak głównie przepisy materialnoprawne, nie poruszając zupełnie zagadnienia związanego z pracą dochodzeniowo - śledczą i koniecznej współpracy w zakresie kryminalistyki. Regulacjami o szczególnym znaczeniu są również Protokół dodatkowy do konwencji o cyberprzestępczości dotyczący kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych oraz Konwencja RE o ochronie dzieci przed wykorzystaniem seksualnym i niegodziwym traktowaniem w celach seksualnych.

Z europejskiego punktu widzenia organizacją międzynarodową o największym oddziaływaniu na prawo krajowe oraz europejską unifikację przepisów jest oczywiście Unia Europejska. Bez wątpienia jest liderem w zakresie przyjętych rozwiązań oraz szczegółowości poruszanych kwestii. Inne organizacje międzynarodowe decydują się na uregulowanie jedynie ściśle określonej kwestii takich, jak handel elektroniczny czy cyberprzestępczość. Unia Europejska podejmuje próbę regulacji niemal każdego aspektu prawa cyberprzestrzeni - przestępczości, handlu, własności intelektualnej, danych osobowych, wolności słowa. Dzięki wprowadzonym normom europejski rynek jest najbardziej spójny, a internauci łatwiej dochodzą swoich praw. Tym co negatywnie wpływa na kształt i efektywność unijnego prawa

jest ogromna fragmentaryzacja i różnice w implementacji ustawodawstwa UE do krajowych porządków prawnych. Istnieją obszary, w których widoczna jest potrzeba wprowadzenia jednego holistycznego dokumentu, zamiast kilkunastu szczegółowych aktów prawnych (chociażby w zakresie własności intelektualnej). Również dyrektywa o handlu elektronicznym, wydana kilkanaście lat temu powinna zostać znowelizowana, aby odpowiadać wyzwaniom współczesnego e-commerce.

Cyberprzestrzeń jako przestrzeń globalna, ponadnarodowa i transgraniczna nie ogranicza się wyłącznie do rozwiązań regionalnych. Wyspecjalizowane jednostki takie, jak NATO coraz wyraźniej zaznaczają problem cyber - agresji pomiędzy państwami, które mogą stanowić element wojny hybrydowej. Obawa ta jest realna tak jak nigdy wcześniej. Przytoczone w niniejszym rozdziale przykłady cyberagresji na Estonię i Gruzję wskazują, iż oprócz wojen na lądzie, wodzie i powietrzu w przyszłości pojawią się konflikty również w przestrzeni wirtualnej - paraliżując systemy bądź dezinformując przeciwnika. Dlatego też konieczne jest wprowadzenie polityki cyberbezpieczeństwa w krajowych porządkach prawnych. Nie mniej istotna - chociażby w kontekście nasilającego się terroryzmu oraz walki z Państwem Islamskim - jest konieczność koordynacji i współpracy działań w zakresie walki z cyberprzestępczością i cyberterroryzmem. W organizacjach takich, jak Interpol czy Europol wykształcono wyspecjalizowane jednostki, które mają zapobiec, ścigać i zwalczać najpoważniejsze cyberprzestępstwa, czyli cyberterroryzm, pornografię dziecięcą czy pranie brudnych pieniędzy. Tylko skorelowane międzynarodowe działania mogą przynieść oczekiwany skutek. Cyberprzestępcy stają się coraz bardziej pomysłowi, wykorzystują najnowsze techniki i nierzadko - drogi, specjalistyczny sprzęt. Efektywna walka z przestępczością wirtualna, powinna zacząć się od stałej współpracy, wymiany doświadczeń oraz informowania o zagrożeniach. Niezbędne są również szkolenia dla organów ścigania, organów sprawiedliwości oraz techników kryminalistycznych w zakresie technik i metod prowadzenia postępowania cyfrowego oraz zbierania i wykorzystania w sądzie dowodów cyfrowych. Instytucją, która może w przyszłości mieć szczególne znaczenie jest Europejskie Centrum do spraw Walki z Cyberprzestępczością, które jest powołane do walki z najpoważniejszymi przestępstwami popełnianymi w cyberprzestrzeni z przestępczością zorganizowaną, seksualnym wykorzystywaniem dzieci i pornografią dziecięcą oraz ochroną infrastruktury krytycznej Unii Europejskiej.

Nie należy również pominąć wkładu organizacji wyspecjalizowanych podejmujących kroki legislacyjne w celu zapewnienia bezpieczeństwa sieci (ENISA) oraz standaryzowania i

regulowania rynku telekomunikacyjnego w tym w zakresie ochrony przed cyberprzestępczością (ITU). Odzwierciedleniem wolnościowego charakteru cyberprzestrzeni jest organizowanie Światowego Szczytu Społeczeństwa Informacyjnego o elastycznej formule, wskazującego kierunki działań w zakresie budowy społeczeństwa informacyjnego, powszechnego dostępu do informacji oraz Internetu. OECD za pomocą regulacji typu *soft law* podjęła się wytyczenia kierunku zmian legislacyjnych dotyczących podpisu elektronicznego oraz technicznych i prawnych aspektów handlu elektronicznego.

Analiza wybranych dokumentów prowadzi do wniosku, że istniejące rozwiązania traktatowe są fragmentaryczne, a więc niewystarczające. Przyjęcie umowy międzynarodowej jest procesem długotrwałym, poprzedzonym wieloletnimi konsultacjami w celu wypracowania konsensusu. Cyberprzestrzeń, jako dynamiczny obszar podlegający szybkim zmianom, jest zawsze krok przed normami prawa pozytywnego. Przestrzeń wirtualna nie może być jednak obszarem, w którym brak jest norm czy chociaż minimalnych standardów. Z tych też względów część organizacji międzynarodowych proponuje rozwiązania modelowe, przyjmuje rezolucje i zalecenia, które wskazują kierunki rozwoju prawa cyberprzestrzeni. Wydaje się, że właśnie *soft law* odgrywa ogromną rolę w kształtowaniu się norm przestrzeni cyfrowej. Z jednej strony oddolne, nieformalne tworzenie norm odpowiada wolnościowemu charakterowi cyberprzestrzeni, z drugiej w sposób stosunkowo szybki jest w stanie reagować na nowe wyzwania i dynamicznie zmieniającą się sytuację polityczną i technologiczną w globalnym świecie.

W mojej ocenie szczególnie interesujące okazało się porównanie ustawodawstwa poszczególnych państw - zaczynając od krajów, które stały się ofiarami ataków (Estonii i Gruzji), przez cyberpolitykę supermocarstw: USA, Rosji i Chin, a kończąc na krajach wysoko rozwiniętych, w których zmiany legislacyjne szybko nadążają za zmianami technologicznymi. Międzypaństwowy konflikt wydaje się wyłącznie kwestią czasu. Już w chwili obecnej rządy państw wykorzystują cyberprzestrzeń do realizacji własnych celów takich, jak szpiegostwo, dezinformacja czy manipulacja opinią publiczną. Cyberatak na inne państwo może być uznany za naruszenie art. 5 Traktatu Północnoatlantyckiego. Tymczasem porządki prawne niektórych krajów mimo deklarowanych wartości i wolnościowego charakteru przestrzeni wirtualnej dopuszczają możliwość cyberagresji i rozwiązywania konfliktów „na własnych warunkach", jednostronną próbą usprawiedliwienia ingerencji w przestrzeni wirtualnej obcego państwa. Dlatego też przyjąć należy rozwiązania podobne do przyjętych w Estonii,

gdzie stworzono cyberarmię, złożoną z ochotników, którzy będą bronili cyberprzestrzeń swojego kraju w przypadku wystąpienia ataku.

Rozdział 4

Identyfikacja kluczowych zagadnień przedmiotowych prawnomiędzynarodowej regulacji cyberprzestrzeni

Użytkownicy korzystają z Internetu w celach prywatnych, służbowych, handlowych czy rozrywkowych. Cyberprzestrzeń jest również ogromnym rynkiem usług, które w jednej sekundzie łączą oddalone od siebie o miliony kilometrów podmioty. W ostatnich latach przestrzeń cyfrowa wzbudza ogromne zainteresowanie państw, głównie w kontekście zagrożeń związanych z działalnością przestępczą oraz terrorystyczną. Kraje coraz śmielej - w sposób bardziej lub mniej jawny - wykorzystują przestrzeń wirtualną do realizacji swoich celów politycznych czy gospodarczych. Cyberprzestrzeń jest wykorzystywana zarówno przez państwa, jak i inne podmioty (jednostki - hackerów, zorganizowane grupy przestępcze, terrorystów) do prowadzenia wojny informacyjnej. W przyszłości, realna wydaje się obawa wybuchu cyber wojny - konfliktu, w którym kluczową rolę odgrywać będzie komputer, za pomocą którego prowadzona będzie propaganda, dezinformacja, ale również cybernetyczne ataki na systemy i programy przeciwnika.

Nigdy wcześniej nie mieliśmy do czynienia z obszarem, który z uwagi na swój wirtualny, transgraniczny i transnarodowy charakter skupia w jednym miejscu miliardy rozmaitych podmiotów (państwa, osoby fizyczne i prawne) pochodzących z różnych krajów i porządków prawnych. Powstanie konfliktu jurysdykcyjnego, czy to na poziomie publicznym, prywatnym, karnym, czy cywilnym - wydaje się być tylko kwestią czasu. Przestrzeń wirtualna nie posiada jednego, zunifikowanego i harmonijnego prawa. Prawo cyberprzestrzeni tworzą między innymi akty prawa międzynarodowego, akty stanowione organizacji międzynarodowych oraz prawo krajowe. Należy jednak postawić sobie pytanie, jakie

zagadnienia są szczególnie istotne w kontekście międzynarodowej regulacji cyberprzestrzeni i działań w niej podejmowanych.

W niniejszym rozdziale zostaną poruszone kwestie związane z dozwolonym i niedozwolonym wykorzystaniem przestrzeni wirtualnej przez jej użytkowników. Szczególnie palący jest problem cyberprzestępczości, ponieważ szybki rozwój techniki spowodował powstanie zupełnie nowej kategorii przestępstw, które są trudne do wykrycia, ścigania i efektywnego osądzenia między innymi ze względu na trudności w zebraniu dowodów, w tym dowodów cyfrowych. Nie mniej istotnym zagadnieniem - szczególnie ważkim w obliczu zwiększającej się siły Państwa Islamskiego i innych ekstremistów - jest wykorzystanie cyberprzestrzeni przez terrorystów, którzy za pomocą sieci wirtualnej zbierają fundusze, rekrutują nowych członków oraz prowadzą działania propagandowe.

W niniejszej dysertacji zostaną opisane podstawowe zagadnienia związane z kwestią obrotu gospodarczego w przestrzeni cybernetycznej. Internet usprawnił, przyśpieszył i umożliwił wymianę towarów i usług na ogromną skalę. Należy zadać pytania, czym jest obrót gospodarczy w cyberprzestrzeni, w jaki sposób następuje zawarcie umów oraz jakie reguły należy stosować przy zastosowaniu najnowszych elektronicznych form płatności. Inne problemy prawa zobowiązań w cyberprzestrzeni (delikty, odpowiedzialności za produkty niebezpieczne i tym podobne), choć ciekawe, nie będą szczegółowo poruszone w niniejszej pracy. W dalszych rozważaniach zostanie pokrótce opisane stosunkowo nowe zjawisko pieniędzy wirtualnych oraz kwestie związane z najnowszymi problemami własności intelektualnej, ochrony danych osobowych oraz praw człowieka w przestrzeni cyfrowej. Identyfikacja i szczegółowy opis tych obszarów jest konieczny do wskazania istniejących uregulowań prawnych, obszarów pozostających poza systemem prawa krajowego i międzynarodowego oraz inicjatyw podjętych w tym przedmiocie.

4.1 Zwalczanie cyberprzestępczości a prawo międzynarodowe

Wojny, terroryzm i przestępczość to problemy, z którymi świat zmaga się od setek lat. Jednakże wejście w nową erę - erę komputerów, telefonów komórkowych, Internetu, GPS-ów

oraz satelitów spowodowało, iż stanęliśmy w obliczu zupełnie nowych wyzwań i zagrożeń. Punktem wyjścia do dalszych rozważań będzie wskazanie podstawowych rodzajów zagrożeń w cyberprzestrzeni (tabela 11).

Tabela 11. Podstawowe rodzaje cyberzagrożeń

Zjawisko	**Cechy charakterystyczne**
Cyberprzemoc	Wykorzystanie cyberprzestrzeni w celu wymuszenia odbioru niepożądanych komunikatów zawierających informacje (dane, obrazy, treści), sprzecznych z wartościami adresata.
Cyberprzestępstwo	Wykorzystanie cyberprzestrzeni w celu dokonania aktów kryminalnych pospolitych i zorganizowanych skierowanych na zasoby osób prywatnych i/lub organizacji (instytucji).
Cyberinwigilacja	Wykorzystanie cyberprzestrzeni w celu kontroli i/lub pozyskiwania informacji o zachowaniach i działaniach obywateli (społeczności, społeczeństwa) (efekt „Big Brother").
Cyberterroryzm	Wykorzystanie cyberprzestrzeni w celu działań terrorystycznych (państwowych i pozapaństwowych).
Cyberautorkatyzm	Wykorzystanie cyberprzestrzeni w życiu politycznym państwa niezgodnie z zasadami demokracji liberalnej (przeciwieństwem - cyberdemokracja).
Cyberwojna	Wykorzystanie cyberprzestrzeni w celu realizacji działań politycznych realizowanych przez siły zbrojne (cyberwarriors) i skierowanych na zasoby i struktury państwa przeciwnika (również w działaniach innych niż wojna).

Źródło: K. Węderska, *Cybernetyczny Pearl Harbor - mit czy rzeczywistość?,* [w:] M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku*, Warszawa 2014, s.71-71 na podstawie: P. Sienkiewicz (red.) *Metody badań nad bezpieczeństwem i obronnością*, Warszawa 2010.

Pytanie czym jest cyberprzestępczość i jak ją zdefiniować budzi szereg wątpliwości. Maciej Siwicki stoi na stanowisku, że dzieje się tak dlatego, że „przestępczość ta ciągle ewaluuje i dostosowuje w sposób elastyczny swoje wielorakie przejawy do zmian technologicznych, często reaguje przy tym z dużą ruchliwością na stosowane wobec niej społeczne środki kontroli"[758]. Krzysztof Gienas uznał, że na specyfikę cyberprzestrzeni składają się dwa elementy: pierwszy, jakim jest eksterytorialny jego charakter oraz drugi, na który składa się możliwość korzystania z jego zasobów w sposób pozornie anonimowy[759].

[758] M. Siwicki, *Cyberprzestępczość* …, s. 15.
[759] K. Gienas, *Cyberprzestępczość*, „Jurysta" 2003, nr 12, s. 9.

Termin cyberprzestępczość wywodzi się z anglojęzycznego słowa *cybercrime*, które należy podzielić na dwa człony - *cyber* i *crime*. Drugi ze wskazanych terminów oznacza ‘zbrodnię, przestępstwo czy występek’. Większe trudności nastręcza zdefiniowanie słowa *cyber*, które samo w sobie nie jest oddzielnym terminem, zostało wyodrębnione ze słowa cybernetyka (ang. *cybernetics*). Słowo te pochodzi z greckiego *kybernetes,* które oznacza ‘sternika, zarządcę’, a *kybernán* tłumaczyć należy jako ‘sterowanie, kontrolowanie’. Cybernetyka jest nauką o systemach sterowania oraz związanym z tym przetwarzaniem i przekazywaniem informacji, komunikacji[760].

Pierwsza definicja cyberprzestępczości została sformułowana w 1973 roku przez Doon B. Parkera, który uznał, iż jest to „każdy nielegalny czyn, do którego popełnienia i ścigania jest niezbędna specjalistyczna wiedza o technice komputerowej”[761]. Z kolei według Debry Littlejhon Shinder za cyberprzestępczość uznać należy wszelkiego rodzaju przestępstwa, do których popełnienia użyto Internetu lub sieci komputerowej, z tym, że przestępstwa te mogą być popełnione na kilka sposobów:

- komputer lub też sieć komputerowa może być narzędziem przestępstwa, czyli zostają one użyte do popełnienia czynu,
- komputer lub sieć komputerowa mogą być celem, czyli ofiarą przestępstwa,
- komputer lub sieć komputerowa mogą być użyte do dodatkowych czynności związanych z popełnieniem przestępstwa, na przykład mogą być na nim przechowywane dane niezgodne z prawem[762].

W trakcie X Kongresu ONZ w sprawie Zapobiegania Przestępczości i Traktowania Przestępców (*Tenth United Nations Congress on the Preventing of Crime and Treatment of Offenders*) zaproponowano podział cyberprzestępczości na:

- cyberprzestępstwa w sensie wąskim, czyli przestępstwa komputerowe rozumiane jako wszelkie zamachy przeciwko bezpieczeństwu systemów komputerowych i danych przetwarzanych elektronicznie,
- cyberprzestępstwa w sensie szerokim, czyli przestępstwa dotyczące komputerów. W tej kategorii mieszczą się czyny popełniane przy użyciu lub przeciwko systemowi

[760] M. Siwicki, *Cyberprzestępczość* …, s. 15.
[761] B. Hołyst, *Kryminologia.* Warszawa 2007, s. 326.
[762] D. Littlejohn Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci,* Gliwice 2004, s. 25.

komputerowemu lub sieci komputerowej; przykładami takich zachowań jest udostępnianie za pomocą komputera lub sieci treści lub informacji[763].

W kwietniu 2001 roku na zjeździe Stowarzyszenia Kryminalistycznego[764] (ang. *Forensic Science Society*) wyodrębniono sześć kategorii tak zwanych przestępstw cybernetycznych. Uznano, iż są nimi:

- przestępstwa, których popełnienie zostało ułatwione przez komputer (ang. *computer assisted*) - są to czyny zabronione, które mogą być popełnione w sposób konwencyjny, ale użycie komputera ułatwia ten proces,
- przestępstwa, których popełnienie umożliwia komputer (ang. *computer enabled*),
- przestępstwa, których nie da sie popełnić bez zastosowania technik komputerowych (ang. *computer only*),
- przestępstwa trudne do popełnienia w sposób konwencjonalny, ale także z wykorzystaniem Internetu (ang. *Internet assisted*),
- przestępstwa trudne do popełnia w sposób konwencjonalny, ale znacznie łatwiejsze do wykonania przy wykorzystaniu Internetu (ang. *Internet enabled*),
- przestępstwa, których dokonanie możliwe jest tylko dzięki wykorzystaniu Internetu (ang. *Internet only*), czyli przestępstwa przeciwko wirtualnym jednostkom[765].

Z kolei w Komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 roku W Kierunku ogólnej strategii zwalczania cyberprzestępczości[766] termin ten został zdefiniowany jako czyny zabronione dokonane za pomocą lub skierowane przeciwko sieci łączności elektronicznej i systemom informatycznym. Termin cyberprzestępczość jest używany w odniesieniu do trzech rodzajów przestępstw. Pierwszy z nich obejmuje tradycyjne formy przestępstw, czyli oszustwo czy fałszerstwo, popełnione jednak za pomocą komputerów. Drugi jest związany z publikacją w mediach elektronicznych treści nielegalnych, na przykład pornografii dziecięcej. Trzeci obejmuje przestępstwa typowe

[763] M. Siwicki, *Cyberprzestępczość* …, s. 17.
[764] Stowarzyszenie Kryminalistyczne (ang. *Forestic Science Society*) - jest to międzynarodowa organizacja zawodowa (założona w 1959 roku), zrzeszająca lekarzy medycyny sądowej, badaczy, naukowców i specjalistów z zakresu kryminalistyki. Celem działania organizacji jest wymiana informacji, komunikacji, prowadzenia wspólnych badań, wprowadzania najlepszych praktyk i publikacji z zakresu kryminalistyki.
[765] B. Hołyst, *Kryminologia,* …, s. 331.
[766] COM/2000/0890.

dla sieci łączności elektronicznej takie, jak ataki przeciwko systemom informatycznym, ataki typu odmowa usługi (ang. *Denial of Servise - DoS*[*]) czy ataki hackerskie.

Konwencja Rady Europy z 23 listopada 2001 roku o cyberprzestępczości nie zawiera w swych postanowieniach definicji legalnej terminu cyberprzestępczość, lecz został w niej zawarty katalog przestępstw wraz z ich definicjami, które państwa członkowskie powinny poddać penalizacji w swych wewnętrznych systemach prawa. Obejmuje:

- „przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych,
- przestępstwa związane z użyciem komputera,
- przestępstwa komputerowe ze względu na charakter informacji stanowiącej ich przedmiot,
- przestępstwa przeciwko własności intelektualnej"[767].

Rozwijając wyżej wskazaną klasyfikację, Andrzej Adamski zaliczył do pierwszej kategorii czynów popełnianych za pomocą cyberprzestrzeni przestępstwa takie, jak hacking, rozpowszechnianie wirusów internetowych czy też sabotaż komputerowy. Do grupy występków związanych z użyciem komputera zaliczył natomiast czyny skierowane przeciwko tradycyjnym dobrom prawnym, popełnione jednakże przy użyciu komputera: oszustwa komputerowe, znieważenie za pomocą systemu informatycznego, fałszerstwo dokumentów w formie elektronicznej. Jako zupełnie odmienną kategorię Andrzej Adamski wskazał przesyłanie lub rozpowszechnianie w przestrzeni wirtualnej treści zabronionych: pornografii dziecięcej czy propagandy rasistowskiej[768]. Z kolei Brunon Hołyst i Jacek Pomykała dzielą cyberprzestępczość na dwa typy: te popełniane z użyciem przemocy (rzeczywistej lub potencjalnej) oraz te popełniane bez użycia przemocy. Do pierwszej kategorii czynów zaliczać należy pornografię dziecięcą, *cyberstalking*[769] czy cyberterroryzm. Bez użycia przemocy są dokonywane z kolei czyny takie, jak cyberoszustwa[770], cyberkradzieże[771],

[*] Więcej o atakach typu DoS w rozdziale 4.1.2. *Naruszenie integralności danych komputerowych i systemu komputerowego*.

[767] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001, s. 17.

[768] Idem, *Cyberprzestępczość - aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4, s. 52.

[769] B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1, s. 1. Cyberstalking (cyberprześladowanie) - jest to nękanie za pomocą Internetu i urządzeń elektronicznych, często połączone z jawnym lub pośrednim wyrażeniem gróźb, powodujących obawę i strach ofiary.

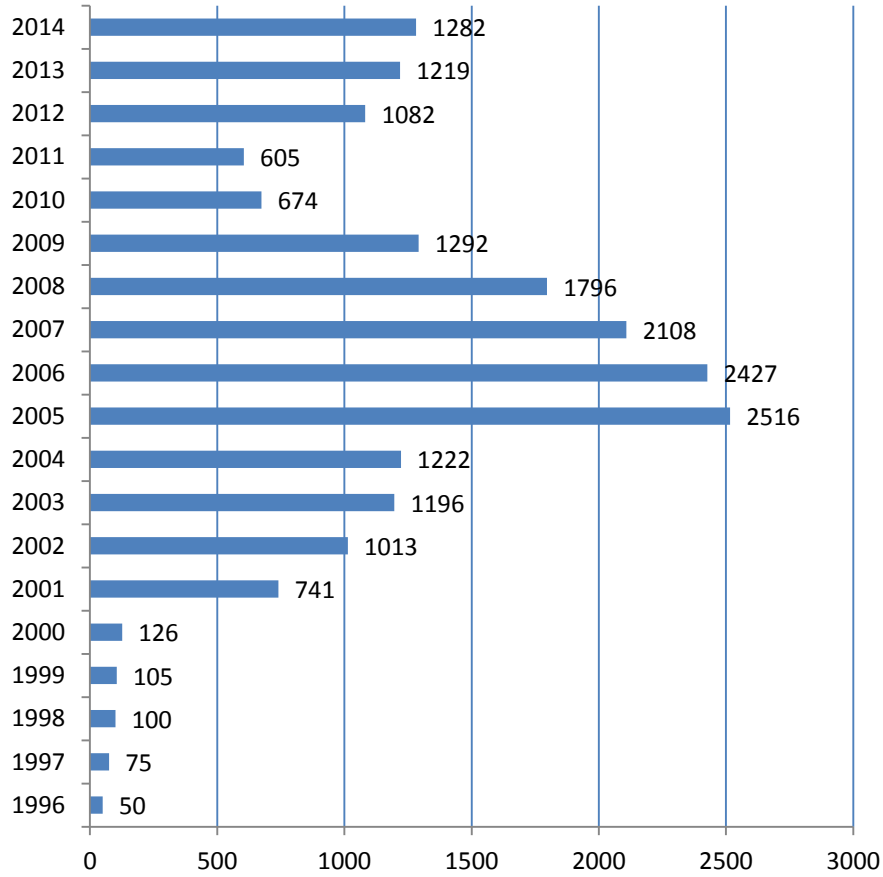
[770] Ibidem: Cyberoszustwa -jest to posługiwanie sie kłamstwem w celu osiągnięcia konkretnych korzyści. Ofiara przez wprowadzenie w błąd przez cyberprzestępcę dobrowolnie podaje dane lub pieniądze.

cyberwyargnięcia[772], cyberzniszczenia[773] i inne formy cyberprzestępstw[774]. Wymienione wyżej propozycje i klasyfikacje, choć każde na swój sposób trafne, opierają się na wspólnym czynniku popełnienia przestępstwa za pomocą przestrzeni wirtualnej. Realnym problemem jest jednak brak międzynarodowych, akceptowalnych definicji samej cyberprzestępczości, jak i konkretnych, najpoważniejszych cyberprzestępstw.

CERT Polska od lat monitoruje Internet Polski. Coroczne raporty ujawniają stan bezpieczeństwa przestrzeni wirtualnej w Polsce. Jak wynika z rysunku 3, pierwszy istotny wzrost incydentów popełnionych z użyciem Internetu przypadł na 2001 rok, co z całą pewnością wiązało się z popularyzacją Internetu w Polsce w ówczesnym czasie. Największą liczbę naruszeń bezpieczeństwa CERT Polska odnotował w latach 2005-2007, kiedy liczba incydentów przekroczyła dwa tysiące. Od kilku lat liczba incydentów utrzymuje się na mniej więcej tym samym poziomie około tysiąca incydentów rocznie. W raporcie podkreślono, że skala incydentów zaobserwowanych na poziomie ogólnoświatowym była znacznie większa niż ta zaobserwowana wyłącznie przez jednostkę CERT Polska.

[771] Ibidem: Cyberkradzież -jest to kradzież informacji za pomocą komputera lub sieci informatycznej, której skutkiem jest przywłaszczenie sobie cudzej własności. Wyróżnić można różne typy cyberkradzieży: kradzież tożsamości, malwersacja, piractwo komputerowe, szpiegostwo przemysłowe.
[772] Ibidem: Cyberwtargnięcia - jest to uzyskanie przez cyberprzestępcę nieautoryzowanego dostępu do zasobów komputerowych lub sieci komputerowych, ale bez zamiaru przestępczego użycia lub zniszczenia danych. Niejednokrotnie celem takich działań jest udowodnienie swoich umiejętności.
[773] Ibidem: Cyberzniszczenia - celem tego przestępstwa jest przerwanie możliwości wykonywania usług sieciowych. Dane dostępne na serwerach są zazwyczaj niszczone lub kasowane. Skutkiem takich działań jest pozbawienie właściciela zasobów oraz użytkowników możliwości korzystania z danych i sieci.
[774]Ibidem, s. 17-18.

Rysunek 3. Liczba incydentów zarejestrowana przez CERT Polska w latach 1996-2014



Źródło: *CERT Polska Raport 2014*, s. 45, r., http://www.cert.pl/PDF/Raport_CP_2014.pdf [31.07.2015].

Na podstawie raportów z ostatnich dziecięciu lat można zidentyfikować zagrożeń, z którymi borykać muszą się polscy internauci. Użytkownicy sieci najbardziej narażeni są na oszustwa komputerowe, które stanowią niemal 30% incydentów zgłaszanych do CERT. Na drugim miejscu znajdują się obraźliwe i nielegalne treści, które stanowią aż 24,12% naruszeń w czasie ostatniej dekady. Niecałe 20% incydentów związanych było z gromadzeniem informacji i naruszeniami takimi, jak podsłuch, czy skanowanie. 16,43 % naruszeń stanowiło użycie złośliwego oprogramowania (tabela 12).

Tabela 12. Typy incydentów odnotowanych w CERT Polska w latach 2005-2014

Typ/podtyp incydentu	**Liczba zgłoszeń**										**Suma - typ**	**Udział [%]**
	2005	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**		
Obraźliwe i nielegalne treści	-	2	-	-	-	2	2	5	-	-	**3640**	**24,12**
Spam	275	857	531	466	438	192	144	107	151	365		
Dyskredytacja, obrażanie	8	21	10	8	8	2	3	-	3	-		
Pornografia dziecięca,	-	8	3	8	3	2	3	2	2	2		

przemoc												
Niesklasyfikowane	bd*	bd	Bd	Bd	bd	bd	Bd	bd	4	3		
Złośliwe oprogramowanie	1	63	86	143	150	90	39	216	-	-	**2479**	**16,43**
Wirus	11	28	16	3	1	-	2	-	5	-		
Robak sieciowy	462	55	78	24	10	-	-	-	9	-		
Koń trojański	117	191	105	104	32	1	5	10	63	8		
Oprogramowanie szpiegowskie	-	3	7	2	-	-	-	-	1	-		
Dialer	3	-	3	0	-	-	-	-	-	-		
Niesklasyfikowane	Bd	bd	Bd	Bd	bd	bd	bd	bd	242	90		
Gromadzenie informacji	-	-	1	-	2	8	1	4	-	98	**2999**	**19,87**
Skanowanie	1292	658	511	84	102	54	42	37	42	13		
Podsłuch	6	2	-	-	-	1	-	-	-	-		
Inżynieria społeczna	7	5	9	2	3	3	3	-	2	-		
Niesklasyfikowane	bd	bd	Bd	bd	bd	bd	bd	bd	2	5		
Próby włamań	-	1	1	11	8	16	7	9	-	-	**620**	**4,10**
Wykorzystanie znanych luk systemowych	18	28	60	24	10	12	11	11	10	4		
Próby nieuprawnionego logowania	99	62	36	62	23	14	5	24	17	5		
Wykorzystanie nieznanych luk systemowych	-	-	1	-	1	-	-	-	-	1		
Niesklasyfikowane	bd	bd	Bd	bd	bd	bd	bd	bd	3	26		
Włamania	-	3	1	2	-	2	3	4	-	-	**239**	**1,58**
Włamanie na konto uprzywilejowane	9	3	10	6	8	1	4	9	-	1		
Włamanie na konto zwykłe	7	8	19	16	13	3	2	1	5	7		
Włamanie do aplikacji	2	1	4	57	14	3	1	-	-	-		
Niesklasyfikowane	bd	bd	Bd	bd	bd	bd	bd	bd	6	5		
Atak na dostępność zasobów	-	2	-	-	1	-	-	-	-	-	**302**	**2,00**
Atak blokujący serwis (DoS)	13	20	8	4	5	1	3	8	7	6		
Rozproszony atak blokujący serwis (DDoS)	14	19	32	22	11	10	11	17	22	63		
Sabotaż komputerowy	1	1	-	-	-	-	-	-	-	-		
Niesklasyfikowane	bd	bd	Bd	bd	bd	bd	bd	bd	1	-		
Atak na bezpieczeństwo informacji	-	0	3	1	-	-	-	35	-	-	**144**	**0,95**
Nieuprawniony dostęp do informacji	2	3	4	5	6	5	2	9	14	8		
Nieuprawniona zmiana informacji	1	2	4	1	3	-	1	0	2	-		
Niesklasyfikowane	bd	bd	Bd	bd	bd	bd	bd	bd	17	17		
Oszustwa komputerowe	1	9	5	10	13	3	1	13	-	-	**4502**	**29,84**
Nieuprawnione wykorzystanie zasobów	26	23	14	5	2	1	-	0	7	5		
Naruszenie praw autorskich	31	24	135	316	1	1	1	5	5	-		
Kradzież tożsamości, podszycie się (w tym phishing)	79	304	403	400	387	241	305	541	560	383		
Niesklasyfikowane	bd	bd	Bd	bd	bd	bd	bd	bd	17	225		
Inne	31	21	8	10	24	9	4	15	-	40	**162**	**1,06**
SUMA	2516	2427	2108	1796	1292	674	605	1082	1219	1379	15.087	**100**

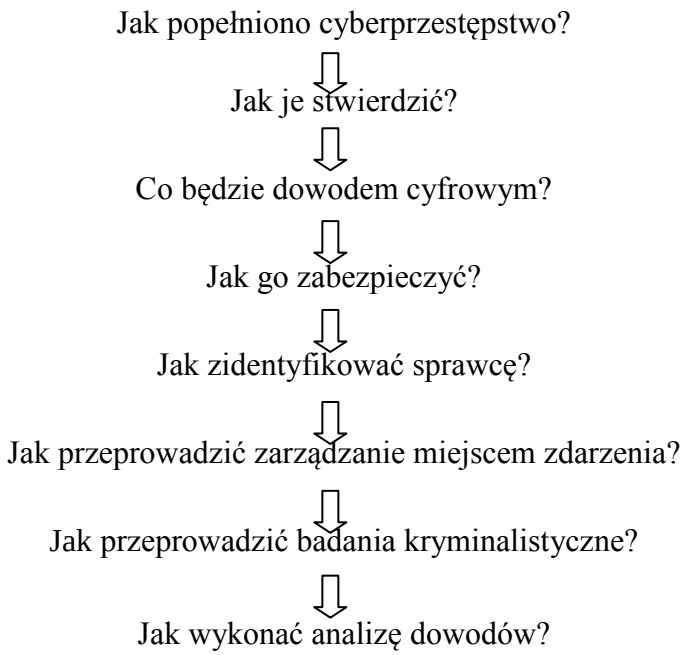
[a]bd - brak danych

Źródło: opracowanie własne na podstawie raportów CERT Polska z lat 2005-2014.

Z badań przeprowadzonych przez firmę Symantec ujawnionych w Raporcie Norton 2013[775] wynika, że na ataki przestępców najbardziej są narażeni posiadacze urządzeń mobilnych (63%), użytkownicy mediów społecznościowych (63%), użytkownicy niezabezpieczający lub korzystający z publicznego Wi-Fi (68%), rozwijające się rynki (68%), oraz rodzice dzieci w wieku 8-17 lat (65%). Jeżeli chodzi o narodowość ofiar to ich największy odsetek znajduje się w następujących krajach: Rosja (85%), Chiny (77%), Republika Południowej Afryki (73%), Meksyk (71%), Indie (65%), Kanada (68%), USA (63%), Australia, Brazylia i Polska (60%).

Wydaje się, że w praktyce zdefiniowanie terminu cyberprzestępczość nie nastręcza tak dużych problemów. Prawdziwym wyzwaniem jest jej efektywne zwalczanie. Organy sprawiedliwości borykają się z problemem jurysdykcji właściwej do ścigania i osądzenia sprawcy, wyboru prawa właściwego, wymogami podwójnej karalności, konieczności ekstradycji, ale również utrudnionym prowadzeniem postępowania dowodowego związanego między innymi z koniecznością zbierania śladów cyfrowych czy chociażby przesłuchania świadków czy pokrzywdzonych znajdujących się w różnych zakątkach globu. Jerzy Kosiński wyraził pogląd, by zdać sobie sprawę z jakimi problemami borykają się organy ścigania należy postawić sobie całą listę pytań. Formułuje je on następująco:

Rysunek 4. Problemy w zwalczaniu cyberprzestępczości



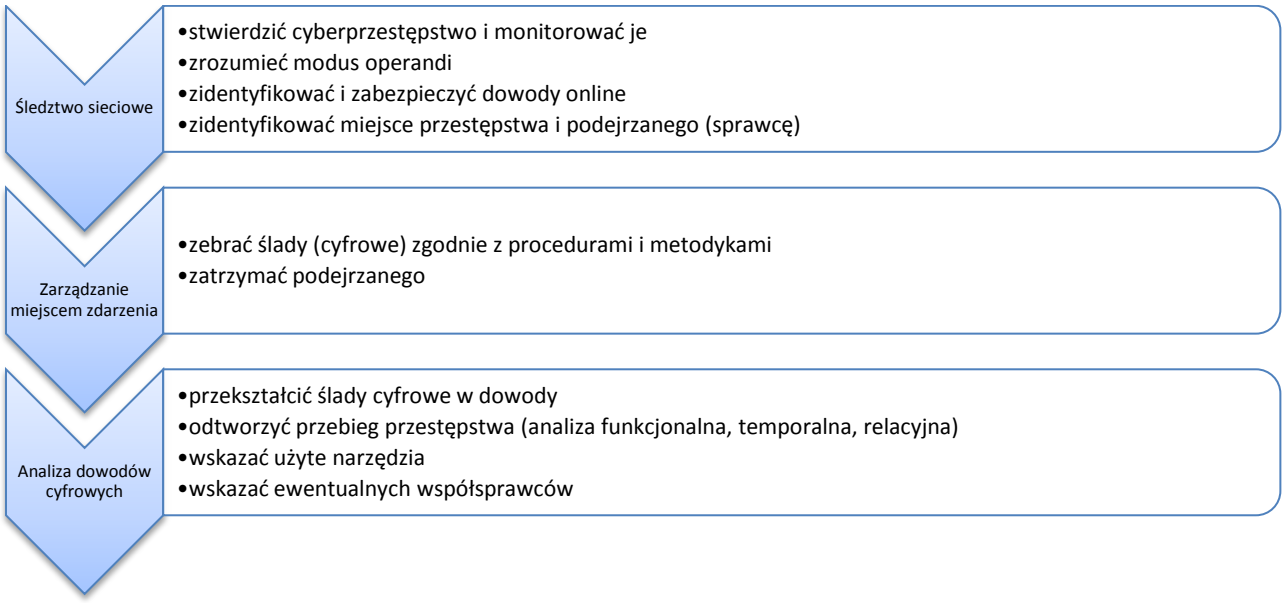
[775] Raport Norton 2013: http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf [08.05.2014].

Źródło: J. Kosiński, *Paradygmaty …*, s. 213.

Praca organów ścigania i sprawiedliwości w sprawach cyberprzestępczości nie należy do łatwych. W Polsce, ale również w innych krajach część policjantów czy prokuratorów nie do końca rozumie ideę niektórych typów cyberprzestępstw (wątpliwości może budzić kradzież wirtualnego przedmiotu na przykład w grze komputerowej, który ma jednak wymierną wartość finansową), bądź nie wiedzą jak prowadzić takie postępowanie, jak zebrać i zabezpieczyć dowody.

Zaproponowany przez Jerzego Kosińskiego model systemu zwalczania cyberprzestępczości oparty został na trzech fazach postępowania: śledztwie sieciowym, zarządzaniem miejscem zdarzenia oraz na analizie dowodów cyfrowych. Szczegółowy opis poszczególnych etapów przedstawiono na rysunku 5.

Rysunek 5. Model systemu zwalczania cyberprzestępczości



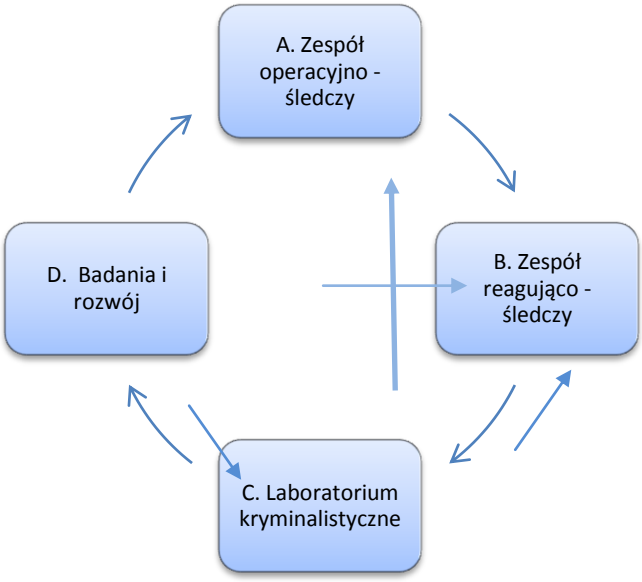
Źródło: J. Kosiński, *Paradygmaty …*, s. 214.

Jak wynika z rysunku 5 pierwszym etapem jest śledztwo sieciowe, które ma na celu wykrycie i monitorowanie cyberprzestępstwa. Konieczne jest zrozumienie *modus operandi* sprawcy, zidentyfikowanie i zabezpieczenie dowodów elektronicznych, a w konsekwencji zlokalizowanie miejsca popełnienia przestępstwa i zidentyfikowanie sprawcy. Kolejnym etapem będą czynności podejmowane w miejscu zdarzenia. Niejednokrotnie okazuje się to wyjątkowo trudne, ponieważ czyn lub też skutek czynu może wystąpić w kilku miejscach jednocześnie. Po zlokalizowaniu miejsca popełnienia przestępstwa należy zebrać ślady

cyfrowe zgodnie z odpowiednią procedurą, a następnie zatrzymać cyberprzestępcę - o ile jest to możliwe. Trzecia - ostatnia - faza łoży na organach ścigania obowiązek przekształcenia śladów cyfrowych w dowody, które mogą być następnie wykorzystane w sądzie, odtworzenie przebiegu popełnienia czynu (stosując analizę funkcjonalną, temporalną i relacyjną) oraz wskazanie ewentualnych współsprawców oraz narzędzi użytych do popełniania czynu[776].

Przyjęcie przedstawionego na rysunku 5 modelu systemu zwalczania cyberprzestępczości jest możliwe wyłącznie w przypadku najprostszych cyberprzestępstw. Czyny o bardziej skomplikowanym charakterze winny być zwalczane za pomocą wsparcia i współpracy zespołowej. Jerzy Kosiński proponuje przyjęcie struktury jednostki zwalczającej cyberprzestępczość opartej na wzajemnie powiązanych podmiotach (rysunek 6).

Rysunek 6. Proponowana struktura jednostki zwalczającej cyberprzestępczość



Źródło: J. Kosiński, *Paradygmaty* ..., s. 214.

Do zadań przedstawionych wyżej zespołów zaliczyć należy:

A. „Zespół operacyjno - śledczy:
   - prowadzenie aktywnego monitoringu sieci,
   - prowadzenie białego wywiadu,
   - prowadzenie działań operacyjno - rozpoznawczych.

B. Zespół reagująco - śledczy:

[776] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 2013 -214.

- wyszukiwanie urządzeń, w których można ujawnić ślady i dowody cyberprzestępstwa,
- wykonywanie *triange* i *live forensic* (to zadanie przeszło z laboratorium kryminalistycznego w tradycyjnym modelu tego zespołu),
- zabezpieczanie śladów,
- typowanie podejrzanych.

C. Laboratorium kryminalistyczne:

- badanie zabezpieczonych śladów, analizowanie danych i informacji, które będą mogły być użyte jako dowody,
- weryfikowanie hipotez kryminalistycznych.

D. Badania i rozwój:

- opracowanie modeli popełniania cyberprzestępczości, opisywanie *modus operandi,*
- opracowanie procedur, przewodników, poradników, dobrych praktyk,
- przeprowadzanie szkoleń (na przykład na temat techniki pozyskiwania informacji, wyszukiwania i gromadzenia, nowych technologii na przykład cyber lokery)
- zarządzanie i rozdzielanie informacją (na przykład dla przesyłu i nauki),
- opracowanie narzędzi wymaganych do pracy (na przykład do monitoringu i przeszukiwania sieci społecznościowych, badania sprzętu telekomunikacyjnego, sprzętu SSD)"[777].

Walka i przeciwdziałanie cyberprzestępczości musi być prowadzone systemowo na poziomie krajowym, regionalnym i międzynarodowym. Trafnym rozwiązaniem jest przyjęcie wyżej wymienionego modelu. Wyłącznie prowadzenie wielopłaszczyznowych działań w zakresie monitoringu, reagowania na incydenty, badań i szkoleń oraz w zakresie ogólno pojętych technik kryminalistycznych, pozwoli na efektywną walkę z cyberprzestrzenią. Brak chociażby jednego elementu może spowodować zupełną nieskuteczność prowadzonych działań, nie wykrycie sprawcy, a nawet w przypadku jego wykrycia - nie zebranie dowodów wystarczających do jego osądzenia.

[777] Ibidem, s. 214-215.

4.1.1 Cyberprzestępstwa przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji

Nielegalny dostęp do systemu komputerowego (hacking)

Artykuł 2 Konwencji o cyberprzestępczości stanowi, że nielegalnym dostępem do systemu komputerowego jest umyślny, bezprawny dostęp do całości lub części systemu informatycznego. Stronom Konwencji pozostawiono wybór, czy wprowadzić do swego ustawodawstwa krajowego wymóg, że przestępstwo to musi zostać popełnione przez naruszenie zabezpieczeń z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym.

Andrzej Adamski wyraża pogląd, że hacking to jest uzyskanie nieuprawnionego dostępu do systemu komputerowego za pomocą urządzeń telekomunikacyjnych, jest on „klasyczną formą zamachu na bezpieczeństwo elektronicznie przetwarzanej informacji. Skuteczne dokonanie takiego zamachu i przejęcie kontroli nad zaatakowanym systemem umożliwia popełnienie innych przestępstw, które mogą być skierowane przeciwko różnorodnym dobrom prawnym (na przykład ochronie informacji, życiu i zdrowiu, mieniu, danym osobowym, wiarygodności dokumentów, tajemnicy przedsiębiorstwa)”[778]. Nielegalny dostęp do komputera lub systemu komputerowego może być uzyskany przez różnego typu działania, na przykład przez zalogowanie się do cudzego komputera lub sieci. Uzyskanie dostępu może nastąpić bezpośrednio, czyli przez fizyczne użycie przez hackera komputera ofiary, na przykład w miejscu jego pracy, ale również przez uzyskanie za pomocą sieci zdalnego dostępu. Bez znaczenia pozostaje czy hacker uzyskał dostęp na poziomie użytkownika (ang. *user level*), czy też na poziomie administratora (ang. *root level* lub *god acces*)[779].

Wstępnym etapem uzyskania nielegalnego dostępu do systemu komputerowego jest jego przeszukiwanie (ang. *port scanning technic*) w celu odnalezienia łatwego obiektu ataku ze względu na luki w oprogramowaniu czy podatności systemu. Dalsze etapy uzyskania

[778] A. Adamski, *Przestępczość* ..., s. 19.
[779] M. Siwicki, *Cyberprzestępczość*…, s. 95.

dostępu do systemu wymagają posłużenia się odpowiednim, specjalistycznym oprogramowaniem określanym, jako „złośliwe" lub „przestępcze". Jest ono niezbędne do uzyskania informacji poufnych znajdującym się na komputerze ofiary. Dane mogą obejmować imię, nazwisko, numer ubezpieczenia, numer PESEL, numer karty płatniczej lub konta bankowego[780].

Sebastian Bukowski wyróżnia kilka rodzajów ataków hackerskich:

- przerwanie (ang. *interruption*) - atak na dyspozycyjność systemu przez częściowe zniszczenie lub spowodowanie jego niedostępności (na przykład przez fizyczne zniszczenie komputera),
- przechwycenie (ang. *interception*) - atak na poufność, występuje w sytuacji, gdy osoba nieuprawniona uzyskuje dostęp do zasobów systemu informatycznego (na przykład przez kopiowanie danych znajdujących się w systemie),
- modyfikacja (ang. *modificatio*n) - atak na nienaruszalność systemu przejawiający się w zdobyciu dostępu do zasobów przez osobę nieuprawnioną, która następnie wprowadza w nich zmiany,
- podrobienie (ang. *fabrication*) - atak na autentyczność danych zgromadzonych w systemie, występuje wówczas, gdy osoba nieuprawniona wprowadza do systemu fałszywe obiekty, pliki, informacje[781].

Motywy działań hackerów bywają rozmaite. Część z nich przełamuje zabezpieczenia w celu osiągnięcia korzyści majątkowej, kradzieży danych bądź innego przestępczego czynu są to tak zwani „hackerzy w czarnych kapeluszach" (ang. *black hat hackers*). Drugą grupą są „hackerzy w białych kapeluszach" (ang. *white hat hacker*), którzy przełamują zabezpieczenia systemów i sieci wyłącznie w celu wykazania słabych punktów, które następnie mogą być poprawione i zabezpieczone. Do grupy tej należy zaliczyć również hackerów, którzy ujawniają nadużycia władzy czy też informują o działających w cyberprzestrzeni zorganizowanych grupach przestępczych czy pedofilskich. Istnieje również grupa hackerów, którzy dokonują cybernetycznych włamań wyłącznie w celu wykazania swoich umiejętności i złamaniu skomplikowanych zabezpieczeń.

[780] Ibidem, s. 96.
[781] S. Bukowski, *Ataki hackerskie, Próba analizy prawno - karnej*, „Gazeta Sądowa" 2003, nr 7/8, s. 49.

Social engineering[782]

Inżynieria społeczna (ang. *social engineering*), nazywana również socjotechniką, jest metodą uzyskania dostępu do informacji niejawnych wykorzystującą niewiedzę, niekompetencję lub łatwowierność użytkowników systemów informatycznych. Techniki manipulacyjne mają na celu uzyskanie od „ofiary" informacji, które pozwolą cyberprzestępcy na uzyskanie dostępu do systemu komputerowego lub innych danych. Użytkownicy sieci często nie zdają sobie sprawy, jak trudno uzyskać z zewnątrz dostęp do danego systemu i zdarza się, że w rozmowie udzielają informacji newralgicznych umożliwiających następnie przełamanie zabezpieczeń komputerowych. Jako przykłady socjotechniki wskazać można następujące metody:

- zakłopotana osoba dzwoni do administratora z prośbą zmianę hasła,
- dzwoniący podając się za dyrektora żąda natychmiastowego dostępu do swojego konta,
- osoba zdobywa hasła w czasie pracy pracowników (wstęp na teren firmy ułatwiają na przykład znajomi),
- próbuje zjednać sobie zaufanie jednego z wybranych pracowników,
- podając się za administratora banku przesłać ofiarom adres swojej strony łudząco przypominającej stronę banku internetowego, z prośbą o zweryfikowanie danych[783].

Nielegalny podsłuch komputerowy

Podsłuchem komputerowym jest nieuprawnione przechwycenie informacji polegające na przejmowaniu transmisji danych teleinformatycznych lub na analizie fal elektromagnetycznych, które są emitowane przez urządzenia elektroniczne takie, jak komputery, monitory, tablety[784]. Nielegalnego podsłuchu komputerowego dokonuje się za pomocą specjalnego programu szpiegującego (ang. *spyware*), umożliwiającego zarówno przechwycenie treści samej informacji, jak i monitorowanie ruchu sieciowego,

[782] *Social engineering* (ang.) - inżynieria społeczna. W bezpieczeństwie teleinformatycznym zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę.
[783] S. Bukowski, op. cit., s. 49.
[784] B. Fischer, *Przestępstwa komputerowe, ochrona informacji. Aspekty prawno – kryminalistyczne*, Kraków 2000, s. 66.

przechwytywanie początkowej sekwencji bajtów użytkowników w celu uzyskania danych poufnych, czyli loginu czy hasła[785].

Maciej Siwicki wyróżnia następujące programu szpiegujące:

- *sniffer* - umożliwiające przechwytywanie haseł dostępu,
- *keyloggers* - program rejestrujący wszelkie czynności użytkownika dokonane za pomocą klawiatury komputerowej,
- *cookies* - mają one na celu rejestrację stron internetowych odwiedzanych przez użytkownika;
- *web bugs* - programy te są instalowane na stronie internetowej lub poczcie internetowej w celu zbierania informacji o aktywności użytkowników w czasie pozostawania na danej witrynie www (czas pozostawania na stronie, adresy IP),
- *browser hijacker* - program umożliwiający przejęcie kontroli nad stroną internetową i zmianę jej ustawień powodujących automatyczne przekierowywanie na inne strony, dodawanie zakładek lub reklam,
- *web crawler* (nazywane też *web spider, web robot* lub *web scraper*) - jest to program wyszukujący informacje lub też kopiujący i pobierający dane z innych witryn internetowych, wykorzystywany przez spamerów do pozyskiwania adresów e-mail użytkowników[786].

Wyszczególniona wyżej lista nie wyczerpuje wykorzystywanych przez przestępców metod. Cyberprzestępcy wciąż doskonalą istniejące programy szpiegujące oraz wymyślają nowe.

Sniffing

Podsłuchiwanie transmisji (ang. *sniffing*) jest stosowane w sieciach typu Ethernet[787], gdzie każdy z wysyłanych pakietów danych dociera do każdego komputera podłączonego do tej sieci, na przykład lokalnej. Oznacza to, że wskazany wyżej pakiet informacji może być odebrany przez którykolwiek z komputerów, niezależnie od tego czy dane były skierowane konkretnie do tego komputera. Sebastian Bukowski wskazuje techniczną stronę *sniffingu*, stwierdzając że przebiega w następujący sposób: „interfejs sieciowy otrzymuje od wyższych

[785] M. Siwicki, *Cyberprzestępczość*... s. 122.
[786] Ibidem.
[787] Ethernet - technika, w której zawarte są standardy wykorzystywane w budowie głównie lokalnych sieci komputerowych. Ethernet jest najpopularniejszym standardem w sieciach lokalnych.

warstw modelu ISO/OSI[788]. Właśnie ze względu na tę specyfikę przesyłania bardzo łatwo newralgiczne dane (bardzo często są to hasła dostępu), mogą »wpaść« w niepowołane ręce. Do podsłuchiwania transmisji sieciowej służą tak zwane *sniffery*, często określane mianem analizatorów ruchu sieciowego. Są to najczęściej wyspecjalizowane programy komputerowe, a w wersjach komercyjnych, specjalnie zaprojektowane komputery z odpowiednim oprogramowaniem"[789].

Konwencja o cyberprzestępczości w art. 3 stwierdza, że nielegalnym przechwytywaniem danych jest umyślne, bezprawne, przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Konwencja w zdaniu drugim przytoczonego artykułu wprowadza przepis, iż od państw - stron zależy, czy penalizacja tego czynu będzie uzależniona od tego, czy przestępstwo zostało popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym.

Określenie „niepubliczna transmisja danych komputerowych" odnosi sie nie do natury danych, które są przesyłane, lecz do charakteru procesu transmisji[790]. Andrzej Adamski podkreśla, że „Nielegalne przechwytywanie przy użyciu środków technicznych transmisji danych pomiędzy systemami komputerowymi dotyczy przekazów »niepublicznych«. Pojęcie to oznacza, że przekazy informacji adresowane lub przeznaczone dla indywidualnego odbiorcy lub określonego kręgu odbiorców, również wtedy, gdy wykorzystywane są w tym celu sieci publiczne, a treść przekazywanych informacji jest publicznie dostępna, lecz w intencji nadawcy lub odbiorcy jej przekaz ma mieć charakter poufny"[791].

---

[788] „Pod koniec lat siedemdziesiątych organizacja ISO (ang. *International Standards Organization*) zaproponowała model współpracy sieci komputerowych przeznaczony do zaimplementowania we wszystkich sieciach na całym świecie. Prace nad nim były prowadzone od 1977 do 1984 roku i w rezultacie doprowadziły do powstania dokumentu - *Reference Model of Open System Interconnection* (OSI). Internet i wszystkie sieci przyjęły ten standard, jako że był on dobrze znany. Za nazwę przyjęto: model ISO/OSI. Model ten został podzielony na siedem warstw grupujących sprzęt i oprogramowanie w dokładnie wydzielonych i zdefiniowanych modułach funkcjonalnych, każda z wydzielonych warstw pełni określone funkcje lub oferuje sąsiednim warstwom określone usługi. Ponadto, każda z warstw stanowi barierę oddzielającą warstwę wyższą od szczegółów implementacyjnych zastosowanych w warstwach niższych, co należy rozumieć, jako możliwość komunikacji danej warstwy wyłącznie z następną warstwą sieci. Warstwy te poczynając od najniższej to warstwa fizyczna, łącza danych, sieciowa, transportowa, sesji, prezentacji i aplikacji" S. Bukowski, op. cit., s. 55.

[789] S. Bukowski, op. cit., s. 51.

[790] M. Siwicki, *Cyberprzestępczość*, …, s. 124.

[791] A. Adamski, *Przestępczość …*, s. 26.

Podobne przepisy znalazły się w *ITU Toolkit for Cybercrime Legislation*[792]. Artykuł 3 przewiduje, iż przestępstwem podsłuchu komputerowego w typie podstawowym jest nieautoryzowane uzyskanie dostępu lub naruszenie środków bezpieczeństwa w celu pozyskania programu komputerowego, danych komputerowych, treści danych lub danych o ruchu[793]. Za kwalifikowaną formę przestępstwa uznano: nieautoryzowany dostęp lub pozyskanie zabezpieczonych programów komputerowych lub danych (lit. b), nieuprawniony dostęp do rządowego programu lub danych komputerowych (lit. c), nieuprawniony dostęp lub pozyskanie programu lub danych komputerowych dotyczących infrastruktury krytycznej (lit. d), nieautoryzowany dostęp lub pozyskanie programu lub danych komputerowych dotyczących instytucji finansowych lub też danych lub programów komputerowych, które mogą być wykorzystane do celów przestępczych (lit. e) oraz nieuprawniony dostęp lub pozyskanie programu lub danych komputerowych dla celów terrorystycznych (lit. f).

4.1.2 Naruszenie integralności danych komputerowych i systemu komputerowego

Sabotaż komputerowy. Systemy teleinformatyczne jako infrastruktura krytyczna

Sabotaż komputerowy jest to zakłócanie lub paraliżowanie funkcjonowania systemów informatycznych o kluczowym znaczeniu dla bezpieczeństwa państwa i jego obywateli[794]. Andrzej Adamski stoi na stanowisku, iż jest to jeden z najbardziej rozpowszechnionych metod ataku, gdyż „zamachy te są wymierzone w dostępność informacji, czyli atrybut decydujący o zaufaniu do techniki komputerowej, a ich szkodliwość jest wprost proporcjonalna do stopnia zależności danej organizacji lub instytucji od technologii informatycznej"[795].

Za systemy kluczowe dla bezpieczeństwa państwa i jego obywateli zalicza się infrastrukturę krytyczną. Do jej elementów zaliczyć można systemy: zaopatrzenia w energię,

[792] Zbiór zasad legislacyjnych związanych z cyberprzestępczością został opracowany w lutym 2010 r. przez Międzynarodowy Związek Telekomunikacyjny. Tekst *ITU Toolkit for Cybercrime Legislation,* http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf [31.07.2015].
[793] Por. art. 3 lit a (*Unauthorized Access to Computer Programs, Computer Data, Content Data, Traffic Data* - nieuprawniony dostęp do programów komputerowych, danych dotyczących treści, danych o ruchu).
[794] B. Fischer, *Przestępstwa …*, s. 51.
[795] A. Adamski, *Przestępczość …*, s. 32.

surowce energetyczne i paliwa, łączność, sieci teleinformatyczne, finansowe, zaopatrzenia w żywność, zaopatrzenie w wodę, ochronę zdrowia, transport, ratownictwo, systemy zapewniające ciągłość działania administracji publicznej, produkcji składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych w tym rurociągi substancji niebezpiecznych[796]. Zmasowany atak na tego typu systemy może doprowadzić do paraliżu państwa, ogromnych strat finansowych i śmierci tysiąca ludzi.

Dla przykładu, w polskim porządku prawnym dyrektor Rządowego Centrum Bezpieczeństwa sporządza niejawny wykaz obiektów, urządzeń, instalacji i usług, który wchodzi w skład infrastruktury krytycznej. Zgodnie z art. 3 pkt 3 polskiej ustawy o zarządzaniu kryzysowym[797] ochrona infrastruktury krytycznej winna obejmować wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na skutek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. Artykuł 6 wskazanej ustawy stanowi, że do zadań administracji publicznej związanych z ochroną infrastruktury krytycznej należy: gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej, opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej, odtwarzanie infrastruktury krytycznej oraz współpraca między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.

Do wykonania sabotażu komputerowego można wykorzystać metodę fizyczną bądź metodę logiczną. Pierwsza z nich polega na niszczeniu obiektów materialnych, czyli budynków, sprzętu informatycznego czy też powodowanie awarii przez zalanie cieczami, podpalenie czy wysadzenie ładunkami wybuchowymi. Natomiast sprawcy korzystający z drugiej z nich ingerują w systemy informatyczne za pomocą specjalnych programów komputerowych, mających na celu niszczenie, zakłócanie lub spowolnienie pracy serwerów czy też innych systemów komputerowych[798].

[796] P. Fajgielski, *Rozwój technologii informacyjnych i komunikacyjnych oraz związanych z nimi zagrożeń - wybrane aspekty prawne*, [w:] R. Wieruszewski (red.), *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010, s. 147.
[797] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007, Nr 89, poz 590 ze zm.
[798] B. Fischer, *Przestępstwa …*, s. 51.

Hackerzy często stosują metodę ataku nazywaną DoS (ang. *Denial of Service*)[799], której celem jest zablokowanie usługi sieciowej lub systemu komputerowego przez przeciążenie serwerów lub aplikacji obsługującej określone dane. Ataki tego typu opierają się na założeniu, że każdy serwer może obsłużyć w danym czasie określoną liczbę zapytań płynących z sieci. Wysłanie przez hackera bardzo dużej ilości danych w krótkim czasie powoduje, iż serwer nie będzie w stanie działać prawidłowo, w związku z czym nastąpi odmowa usługi, a strona internetowa będzie niedostępna.

Odmianą ataku DoS jest DDoS (ang. *Distributed Denial of Service*). Atak DDoS jest przeprowadzany równocześnie z wielu komputerów w celu zajęcia wszystkich wolnych zasobów. Do przeprowadzenia ataku często wykorzystuje się komputery zombie, czyli komputery, nad którymi przejęto kontrolę (niejednokrotnie bez wiedzy ich właścicieli) za pomocą specjalnego oprogramowania. Zainfekowane komputery na sygnał sprawcy zaczynają atakować system komputerowy ofiary wysyłając ogromną liczbą zapytań, których system ofiary nie jest w stanie obsłużyć. Metodą taką posłużyli się hakerzy atakujący portale rządowe w Estonii w 2007 roku.

Jeszcze inną metodą sabotażu komputerowego wykorzystywaną przez cyberprzestępców jest DRDoS (ang. *Distributed Reflected Denial of Service*), będący odmianą ataku DoS. Atak ten polega na generowaniu specjalnych pakietów SYN, które powodują zalewanie ofiary ogromną liczbą pakietów z wielu hostów, co bardzo utrudnia wykrycie rzeczywistego źródła ataku.

Konwencja o cyberprzestępczości dosyć szeroko ujęła problem niezakłóconego działania systemów komputerowych. W art. 5 jest przepis stanowiący, że penalizacji podlega umyślne, bezprawne zakłócenie funkcjonowania systemu informatycznego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzania, dokonywanie zmian lub usuwanie danych informatycznych. Z kolei w raporcie Komitetu Ekspertów Rady Europy za sabotaż komputerowy uznano: „wprowadzenie, modyfikację, wymazanie lub usunięcie danych lub programów komputerowych albo inne oddziaływanie na system komputerowy mające na celu wywołanie zakłóceń w funkcjonowaniu systemu komputerowego lub telekomunikacyjnego.”[800]

[799] Więcej na ten temat w: F. Radoniewicz, op. cit.
[800] *Council of Europe, Computer - Realated Crime: Recommendation No. R (89)9 on computer - related crime and final report of the European Committee on Crime Problems*, Strasburg 1989, s. 46-49.

Niszczenie danych lub programów komputerowych

Dane i programy komputerowe z zasady mogą być niszczone w dwojaki sposób: przez ich fizyczne zniszczenie lub też ingerencję mającą na celu destrukcję oprogramowania. Pierwszy z wymienionych sposobów polega na mechanicznym, magnetycznym czy też chemicznym uszkodzeniu systemów komputerowych. Taki typ zniszczenia danych wymaga jednakże osobistej, lub chociażby bliskiej styczności z danym komputerem. Częściej spotykaną metodą jest ingerencja w oprogramowanie, a więc stosowanie wirusów lub innych programów o takim charakterze[801]. Wirus jest „programem, który przyłącza swój kod do określonych plików w systemie, przez co ich kod własny zostaje nadpisany w pewnej części lub w całości. Proces ten nazywa się infekcją. Zainfekowane pliki mają możliwość powielania się i infekowania innych plików - proces ten to replikacja"[802].

Bogdan Fischer wskazuje, iż istnieją trzy podstawowe przyczyny, dzięki którym cyberprzestępcy uzyskują możliwość zniszczenia danych. Pierwsza z nich jest spowodowana lukami w systemie, które powstały jeszcze na etapie projektowania programu. Hakerzy wyszukując przerwy w kodzie programu aktywują wirusa, który ma na celu osiągnięcie zaplanowanego przez nich efektu. Drugim ze sposobów aktywowania wirusa jest dostarczenie go na nośniku informacji takim, jak pendrive, CD czy też ściągnięcie pirackiego oprogramowania lub programu. Trzecią, i najprostszą drogą dostania się wirusa do systemu komputerowego jest rozbudowana łączność teleinformatyczna[803].

Typologia wirusów przedstawia się następująco:

- *Rootkit* - program wykorzystywany do ukrycia wirusa, który uzyskuje pełen dostęp do systemu. Niektóre wersje programów uzyskują dostęp do jądra systemu, co znacznie utrudnia jego usunięcie[804].
- Koń trojański (*trojan horse*) – odmiana *rootkita,* jest to: „obcy kod dołączony do prawidłowego programu, koń ten realizuje funkcje nieznane użytkownikowi i zapewnie przez niego niepożądane, każdy program, który wydaje się realizować

[801] B. Fischer, *Przestępstwa …*, s. 40.
[802] S. Bukowski, op. cit. s. 54.
[803] B. Fischer, *Przestępstwa …*, s. 41.
[804] F. Radoniewicz, op. cit., s. 86.

pożądane i pożyteczne dla użytkownika funkcje, lecz realizuje również takie zadanie, które nieznane są użytkownikowi i przez niego niepożądane"[805].

- „Bomba logiczna – kod umieszczony w programie, który uaktywnia się po spełnieniu określonych warunków;
- Bomba czasowa – bomba logiczna, która uaktywnia się po upływie określonego czasu (w założonym terminie);
- Królik – program wypełniający określone zasoby systemu wskutek niekontrolowanego powielania się;
- Łańcuch szczęścia – replika komunikatu wysłanego pocztą elektroniczną;
- Muł trojański – pobudza nieprawdziwe komunikaty, naśladujące normalny dialog z komputerem, bez właściwych efektów;
- Robak (*worm*) – ma zbliżone zasady funkcjonowania do wirusa, z pewnymi jednak odmiennościami. Działa w sieci, przesyłając swoje kopie do różnych systemów. Jest samodzielnym programem wykonywalnym w środowisku systemu operacyjnego. W przeciwieństwie do wirusa nie potrzebuje nosiciela"[806];
- „Tylne drzwi – funkcja programu wbudowana przez programistę, umożliwiająca wykonanie operacji polegającej na nieuprawnionym wejściu do systemu operacyjnego, którym zainteresowany jest włamywacz komputerowy. Zabieg ten umożliwia wbudowanie do systemu hasła dostępu, niezależnie od zawartości pliku haseł systemu;.
- Zapadnia – funkcja programu wykorzystywana przy okazji dokonywania ataków hackerskich, stanowiąca odmianę »tylnich drzwi«. Zabiegi tego typu umożliwiają uprzywilejowany dostęp do sieciowego systemu operacyjnego z pominięciem identyfikacji użytkownika systemu i jego hasła"[807].
- *Exploit* - program wykorzystujący luki w oprogramowaniu,
- *Keylogger* - „program odczytujący i zapisujący wszystkie znaki wpisywane przez użytkownika za pomocą klawiatury"[808]. Dzięki temu cyberprzestępca może uzyskać dostęp do loginów i haseł.

[805] S. Bukowski, op. cit., s. 54.
[806] B. Fischer, *Przestępstwa …*, s. 42.
[807] M. Białkowski, *Niszczenie danych i programów komputerowych, „*Gazeta Sądowa" 2002, nr 7/8, s. 57.
[808] B. Fischer, *Przestępstwa …*, s. 87

- Metoda salami – „stosowana przy oszustwach finansowych, a polegająca na wprowadzeniu programu, który niezauważalnie odcina małe sumy pieniężne z jednego konta i odprowadza na wskazane konto oszusta”[809].

Wirusy komputerowe mogą oddziaływać na dowolny element systemu komputerowego. Gdy dojdzie do zainfekowania komputera wirus może powodować, w zależności od jego celu, różne skutki, a mianowicie może:

- „wyświetlać nietypowe obrazy na akranie, rysunku, znaki firmowe albo napisy zawierające - często - komunikaty polityczne, personalne albo ideologiczne;
- zakłócać lub zmieniać pliki danych użytkownika, w tym:
  - wymieniać lub zmieniać dane,
  - oznaczać miejsca na dysku jako 'uszkodzone', zmniejszając tym samym użyteczną przestrzeń dysku,
  - uszkadzać blok parametrów BIOS-u, kodu sektora ładowania albo tablicy partycji, co stwarza wrażenie zreformowania lub zniszczenia danych,
  - reformować partycje dysku albo formatować na niskim poziomie;
- zakłócać lub oddziaływać na porty komunikacyjne, w tym:
  - wymieniać bajty i zakłócać dane w połączeniach modemowych,
  - inicjować 'fałszywe' połączenia telefoniczne, dopuszczając możliwość przesyłania informacji osobom nieupoważnionym,
  - umieszczać niszczące polecenia w zdalnych sesjach rejestracji,
  - przejmować lub zmieniać wyjścia na drukarkę lub monitor,
  - zmieniać położenie lub kierunek działania myszki;
- przechwytywać lub zmieniać informacje z klawiatury przez wysyłanie kodów klawiszy symulujących błędy maszynowe albo dysleksję, odrzucanie pewnych znaków, umieszczanie zabawnych albo kłopotliwych, dodatkowych informacji w buforze klawiatury, a także zmianę wskaźników stanu klawiatury;
- spowalniać pracę systemu komputerowego przez modyfikowanie zegara systemowego (przyśpieszanie lub zwalnianie, przypadkowe zerowania lub skoki) albo działanie tzw. ślepych programów powodujących zwolnienie całego systemu lub wybranych programów;
- spowodować fizyczne uszkodzenie podzespołów systemu komputerowego”[810].

[809] Ibidem, s. 44.

Należy pamiętać o tym, że użytkownik komputera może w ogóle nie mieć wiedzy, że jego system został zainfekowany. Programy te są niezauważalne dla większości internautów, gdyż często nie powodują problemów z użytkowaniem komputera. Ważne jest zatem, zabezpieczenie komputera odpowiednim oprogramowaniem antywirusowym, który wyeliminuje, bądź co najmniej znacznie ograniczy możliwość zainfekowania systemu.

4.1.3 Cyberprzestępstwa przeciwko mieniu

Oszustwo komputerowe

Rozwój technologiczny, informatyzacja systemów bankowych, komputeryzacja systemów rachunkowo - księgowych stworzyła nowe możliwości działań przestępczych. W ramach oszustw komputerowych można wyróżnić trzy rodzaje manipulacji: manipulację danymi, manipulację programami, manipulowanie urządzeniami preferencyjno-systemowymi (manipulowanie wynikiem)[811].

Manipulacja danymi (ang. *imput manipulation*) polega na „wprowadzeniu fałszywych informacji do bazy danych w celu uzyskania nieuprawnionych korzyści"[812]. Przykładem takich działań może być między innymi regulowanie niezapłaconych należności finansowych, podwyższanie kwot wpłat czy też defraudacja w administracji państwowej. Ten rodzaj manipulacji nie wymaga wiedzy hakera, najczęściej manipulatorami są pracownicy firm, obeznani z wyspecjalizowanymi programami obsługującymi konta bankowe.

Manipulacja programem (ang. *software manipulation*) jest to grupa działań trudna do wykrycia. Podstawę tych działań stanowi „przekształcenie komend lub dopisywanie nowych w ramach programu, które powodują wykonanie zadań niezależnie od woli operatora. Mogą być dokonywane przez samego operatora w celu na przykład osłony właściwych obrotów w działalności gospodarczej (tzw. podwójna księgowość)"[813].

Manipulacja wynikiem (ang. *output manipulation*) zwana jest również manipulacją urządzeniami preferencyjno–systemowymi czy urządzeniami wejścia – wyjścia. Polega ono

[810] K.J. Jakubski, *Przestępczość komputerowa - zarys problematyki*, „Prokuratura i Prawo" 2006, nr 12, s. 40-41.
[811] B. Fischer, *Przestępstwa …*, s. 33.
[812] Ibidem, s. 34.
[813] Ibidem.

na manipulacji tymi urządzeniami w celu uzyskania pożądanego wyniku. Najczęściej dokonuje się ich przy użyciu kart magnetycznych lub chipowych takich, jak karty bankomatowe lub telefoniczne. Częstym działaniem jest posługiwanie się skradzionymi przez hakerów numerami kart kredytowych, czyli tak zwany *carding,* który opiera się na „zdobywaniu" numerów kart istniejących lub tworzeniu fałszywych[814].

Inni przedstawiciele doktryny wskazują, że oszustwa związane z wykorzystaniem nowych technologii mogą być sklasyfikowane w następujący sposób:

- nielegalna transakcja *on-line* (ang. *fraudulent sales on-line*) - oferowanie nieistniejących towarów, usług, wyłudzanie świadczeń na podstawie przerobionych bądź skradzionych kart płatniczych,
- zaawansowane oszustwa związane z opłatami (ang. *advance - fee schemes*) - oferowanie odpłatnego dostępu do usług, świadczeń bądź serwisów, które tak naprawdę są bezpłatne, oferowanie wysokich zysków z „inwestycji"
- oszustwa związane z elektronicznym elektronicznym transferem środków (ang. *electronic funds transfer crime)* - przechwytywanie haseł, informacji oraz innych danych umożliwiających nieuprawnione uzyskanie dostępu do internetowej bankowości elektronicznej ofiary,
- oszustwa inwestycyjne (ang. *fraudulent investments*) - tworzenie serwisów internetowych oferujących szybkie i wysokie zyski z inwestycji, rozpowszechnianie nieprawdziwych informacji o przedsiębiorstwie (na przykład w formie podrobionych doniesień prasowych), które mogą wpłynąć na wysokość akcji firmy,
- podszycie się pod inną osobę w celu popełnienia przestępstwa (ang. *Identity Crime*)[815].

Sprawca musi dysponować odpowiednimi narzędziami i wiedzą, by dopuścić się cyberoszustwa. Narzędziami tymi są zazwyczaj specjalistyczne programy komputerowe, czyli złośliwe oprogramowanie:

- *session hijackiers* - nazwa pochodzi od angielskiego słowa *hijack* – 'porywać, uprowadzać'; programy tego typu mają na celu przechwycenie sesji i uzyskanie dostępu do sesji legalnego użytkownika między innymi przez przejęcie dokonywanego przez użytkownika sieci transferu środków pieniężnych,

[814] Ibidem.
[815] J. Clough, *Principles of cybercrime*, Nowy Jork 2010, s. 183-199.

- *web trojans* - jest to złośliwe oprogramowanie umożliwiające wyświetlenie adresu internetowego, który zbiera dane poufne, czyli login, hasło - zamiast lub przed oryginalną stroną logowania na przykład do internetowego konta bankowego,
- *transaction generator* - w przeciwieństwie do wyżej wymienionych metod, ten rodzaj złośliwego oprogramowania nie atakuje komputera użytkownika, lecz komputery pośredniczące w transakcjach transferu danych komputerowych. Celem ataku może być na przykład komputer odpowiedzialny za przetwarzanie danych w transakcjach dokonywanych kartami płatniczymi[816].

Artykuł 8 Konwencji Rady Europy o cyberprzestępczości definiuje oszustwo komputerowe, jako „umyślne bezprawne spowodowanie utraty własności przez inną osobę, z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby poprzez: 1) wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych komputerowych, 2) każdą ingerencję w funkcjonowanie systemu komputerowego". Andrzej Adamski podnosi, iż dokonanie tego czynu zabronionego jest uwarunkowane wywołaniem skutku w postaci utraty własności (ang. *loss of property*) przez ofiarę przestępstwa[817]. W doktrynie wskazuje się, iż pojęcie „utraty własności" winno być interpretowane szeroko i obejmować nie tylko straty materialne, ale również niematerialne. Czyn popełnić można zarówno w zamiarze bezpośrednim, jak i ewentualnym[818].

Podobna definicja oszustwa komputerowego zaproponowana została w art. 8 ust 2 ITU *Cybercrime Legislation Toolkit*, który stanowi, że jest to „umyślne, bezprawne spowodowanie utraty własności przez inną osobę przez:

- wprowadzenie, pozyskiwanie, zamienienie, usuwanie lub ukrywanie programu komputerowego, danych komputerowych, danych tekstowych, danych o ruchu lub
- zakłócenie funkcjonowania komputera, systemu komputerowego i/lub połączonych systemów lub sieci

  - z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby"[819].

[816] M. Siwicki, *Cyberprzestępczość* …, s. 243-244.
[817] A. Adamski, *Przestępczość* ..., s. 48.
[818] M. Siwicki, *Cyberprzestępczość* …, s. 245.
[819] Tłumaczenie za: M. Siwicki, *Cyberprzestępczość* …, s. 245-246.

Maciej Siwicki stoi na stanowisku, iż wskazaną wyżej regulację należy rozpatrywać w kontekście Konwencji o cyberprzestępczości. Postanowienia w niej zawarte w znacznym stopniu stanowią uzupełnienie oraz wypełnienie braków, które ujawniły się w wyniku postępu technologicznego. Powoływane przepisy zapewniają szerszą ochronę procesów technicznych związanych z przetwarzaniem danych. Konwencja Rady Europy ograniczała się jedynie do systemów komputerowych, nie uwzględniając danych tekstowych, danych o ruchu oraz połączeń systemów i sieci[820].

Oszustwa komputerowe są najczęściej spotykanymi czynami przestępczymi w cyberprzestrzeni. Nieświadomi użytkownicy sieci, nie dochowując podstawowych zasad bezpieczeństwa często padają ofiarą cyberprzestępców. Wynika to z bagatelizowania zagrożeń, naiwności czy też niedostatecznego sprawdzenia kontrahenta (na przykład przez sprawdzenie opinii innych użytkowników). Poza świadomością zagrożeń, by bezpiecznie poruszać się w przestrzeni wirtualnej konieczne jest dysponowanie odpowiednimi zabezpieczeniami komputerowymi, ale przede wszystkim zdrowym rozsądkiem i pewną dozą podejrzliwości w przypadku ofert o zbyt atrakcyjnej, niskiej cenie bądź wątpliwych, wysokich zyskach.

Fałszerstwo komputerowe

Manipulowanie treścią dokumentu w jego wersji elektronicznej jest nazywane fałszerstwem komputerowym. Bogdan Fischer rozróżnia dwa rodzaje fałszerstw komputerowych. Pierwszy z nich należy rozpatrywać jako wykorzystanie komputera wraz z oprogramowaniem i urządzeniami peryferyjnymi (na przykład drukarki) jako narzędzia do fałszowania dokumentów klasycznych. Drugi odnosi się do dokumentów elektronicznych, gromadzonych i tworzonych za pomocą komputera, w jego pamięci bądź na innych nośnikach informacji[821].

Pierwszy, wskazany wyżej rodzaj fałszerstw komputerowych jest związany z możliwością wykorzystania komputera do fałszowania dokumentów klasycznych takich, jak

[820] Ibidem, s. 246.
[821] B. Fischer, *Przestępstwa …*, s. 36.

pieniądze czy papiery wartościowe. Wysoki poziom technologiczny współczesnych drukarek, w szczególności laserowych, ułatwia przestępcom podrabianie różnorakiego rodzaju dokumentów. Taki stan rzeczy powoduje, iż powszechną praktyką w przypadku środków płatniczych jest nieustanne dodawanie ulepszeń zabezpieczeń przez wprowadzanie znaków wodnych czy hologramów. Bogdan Fischer stoi na stanowisku, iż w tej kategorii czynów mieścić się będą również fałszerstwa z zastosowaniem specjalistycznych programów komputerowych pozwalających na przetworzenie obrazu pierwotnego, jego zmianę czy przetworzenie poprzez dodanie lub odjęcie treści. W ten sposób fałszerz na bazie dokumentu autentycznego tworzy nowy - podrobiony. Są to przestępstwa trudno wykrywalne, zwłaszcza, że dokumenty elektroniczne, dzięki swojej specyfice, dają możliwość utworzenia nieokreślonej liczby kopii i dokonywania niezauważalnych zmian[822].

Fałszerstwa komputerowe dokonywane przez podrabianie czy też modyfikację dokumentów elektronicznych: ewidencje, księgi handlowe, podatkowe są bardziej podatne na dokonywanie czynów zakazanych. Tego typu przestępstwa można podzielić na dwie grupy: dokonywane przez samego właściciela dokumentu (na przykład w celu prowadzenia podwójnej księgowości) lub też przez osoby trzecie (w celu zmiany lub fałszerstwa danych zawartych w systemie komputerowym)[823].

Konwencja o cyberprzestępczości w art. 7 uznaje za fałszerstwo komputerowe „umyślne, bezprawne wprowadzenie, dokonywanie zmian, wykasowywanie lub usuwanie danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to czy są one możliwe do bezpośredniego odczytania i zrozumiałe". Dopuszcza jednakże możliwość ograniczenia zakresu karalności fałszerstwa komputerowego od tego czy sprawca działał z zamiarem oszustwa lub w innym szczególnym zamiarze.

Wydaje się, że w kolejnych latach zwiększać się będzie liczba obu wyżej wymienionych typów fałszerstw komputerowych. Spowodowane jest to coraz lepszą jakością drukarek cyfrowych, ale również osób biegłych w obróbce komputerowej. Realnym zagrożeniem jest podrabianie dokumentów elektronicznych, ale również walut wirtualnych, których obrót jest niereglamentowany.

[822] Ibidem, s. 36-37.
[823] Ibidem, s. 38.

Phishing

Jedną z form fałszerstwa komputerowego jest *phishing* (ang. *password harvesting fishing,* czyli łowienie haseł). Przestępstwo te polega na wyłudzaniu informacji osobistych, czyli haseł dostępu, w szczególności do kont bankowych lub kart kredytowych, przez podszywanie się pod firmę lub instytucję godną zaufania. *Phishing* jest odmianą *social engenering* (inżynierii społecznej). Celem działania cyberprzestępców jest uzyskanie dostępu do środków finansowych zgromadzonych na rachunku bankowym klienta banku przez kradzież jego tożsamości. Sprawcy dopuszczający się *phishingu* zazwyczaj preparują wiadomości e-mail, w taki sposób, by były łudząco podobne do tych pochodzących z banku (przez skopiowanie form graficznych, układu strony oraz jego treści). Tak podrobione wiadomości są wysyłane do potencjalnych klientów banku z prośbą o skorzystanie z załączonego linku, którego kliknięcie powoduje, iż użytkownik zostaje przekierowany na stronę internetową hackera, która formą graficzną łudząco przypomina oficjalną stronę banku. Ofiara *phishingu* proszona jest o weryfikację danych (podanie hasła, loginu, numerów PIN, haseł jednorazowych), dzięki którym cyberprzestępca może uzyskać dostęp do środków finansowych zgromadzonych na prawdziwym koncie klienta[824].

Złośliwe oprogramowanie stosowane przez cyberprzestępców wobec użytkowników bankowości elektronicznej może spowodować następujące skutki:

- podmianę numeru konta docelowego oraz kwoty tuż przed zatwierdzeniem przelewu,
- podmianę aktualnego stanu konta,
- modyfikację danych na liście wykonywanych operacji,
- pojawienie się okienka internetowego proszącego o podanie kodów jednorazowych w celu aktywacji lub sprawdzenia funkcji bezpieczeństwa,
- pojawienia się okienka internetowego proszącego o podanie numeru telefonu oraz wybrania modelu aparatu,
- wyświetlenie użytkownikowi monitu proszącego o zwrot środków pochodzących z błędnego lub podejrzanego przelewu,

[824] A. Kiedrowicz-Wywiał, *Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6, s. 24-25.

- wyświetlenie użytkownikowi monitu proszącego o wykonanie testowego przelewu w ramach aktywacji lub sprawdzenia nowych funkcji bezpieczeństwa[825].

Cyberprzestępcy używają do popełniania przestępstwa *phisingu* złośliwego oprogramowania (tak zwanego *malware*), które może być zarówno aktywne (wyskakujące okienka *pop-up*, formularze dialogowe), jak i pasywne (*keylogery*, które przechwytują wprowadzane dane). Jerzy Kosiński zaznacza, że cechami charakterystycznymi *malware* używanego przez cyberprzestępców do *phishingu* są:

- samoobrona - *malware* dezaktywuje programy antywirusowe (następuje głównie zablokowanie funkcji aktualizacji oprogramowania), zmienia zasady działania zapór sieciowych,
- zdalne zarządzanie - *malware* instaluje oprogramowanie umożliwiające dostęp do komputera oraz zapory sieciowe umożliwiające przekierowywanie połączeń z hosta na inny serwer pośredniczący,
- kradzież tożsamości - przejmowanie haseł, identyfikatorów, adresów e-mail, certyfikatów klucza publicznego (certyfikatów SSL)[826].

Fałszywa strona internetowa, którą posługują się przestępcy jest łudząco podobna do swojego oryginału. Zawiera wszystkie elementy graficzne odpowiadające prawdziwej stronie banku, a nawet wyjaśnienie trudniejszych pojęć, na przykład co to jest i gdzie znajduje się CVV2[827] na karcie kredytowej. Informacje uzyskane przez cyberprzestępców zostają natychmiast wykorzystane[828].

Pharminig

Bardziej skomplikowaną oraz niebezpieczną dla użytkowników przestrzeni wirtualnej formą *phishingu* jest *pharming*. Przestępstwo to polega na: „automatycznym

[825] Raport CERT Polska z 2012. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, s. 40.
[826] J. Kosiński, *Cyberprzestępczość*, [w:] W. Jasiński (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013, s. 475.
[827] CVV2 - (ang. *Card Verification Value 2*) to numer znajdujący się na odwrocie karty kredytowej bądź debetowej identyfikujący kartę. Numer ten składający się z trzech cyfr, podobnie jak PIN służy do identyfikacji karty.
[828] J. Kosiński, *Cyberprzestępczość*…, s. 475.

przekierowywaniu użytkowników na fałszywe strony internetowe, które do złudzenia przypominają oryginalne, aby właściwy adres URL prowadził do fałszywej strony www, konieczne jest przeprowadzenie dodatkowego ataku. W tym celu jest wykorzystywany atak polegający na »zatruciu« globalnego serwera DNS[829] (ang. *cache poisoning*) przez atak na system nazw domenowych (ang. *Domain Name System*) odpowiedzialny za zmianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową, w celu skojarzenia prawdziwego adresu URL z serwerem zawierającym fałszywą stronę internetową. Cyberprzestępcy mogą również przeprowadzić atak z wykorzystaniem trojanów, modyfikujących lokalne pliki w systemie użytkownika, odpowiedzialne za wstępne tłumaczenie nazw URL na fałszywy adres IP z pominięciem globalnego serwera DNS. Atak z wykorzystaniem trojanów może także polegać na wyświetlaniu użytkownikowi dodatkowej (fałszywej) strony z prośbą o podanie danych identyfikacyjnych w momencie, kiedy będzie on odwiedzał legalną stronę"[830]. Metoda ta jest trudna do wykrycia, zwłaszcza dla normalnego użytkownika przestrzeni wirtualnej. Dla *pharmingu* charakterystyczne jest to, że nawet po wpisaniu prawidłowego adresu www, użytkownik zostanie przekierowany na stronę internetową cyberprzestępcy.

Znawcy tematu stoją na stanowisku, iż *pharming* nie ma jednolitej postaci. Aleksandra Kiedrowicz-Wywiał, wskazuje, iż *pharming* może przybrać dwie formy ingerencji w system:

1. Ingerencja w pamięć podręczną DNS komputera lokalnego - wpisując w pasek przeglądarki internetowej określony adres witryny system komputerowy odnajduje go na podstawie przypisanego każdej stronie adresu IP. Każdy z komputerów chcąc przyśpieszyć proces wyszukiwania zazwyczaj zapisuje w pamięci podręcznej adresy stron www odwiedzonych uprzednio przez użytkownika. Sprawcy *pharmingu* modyfikując treść pamięci podręcznej komputera automatycznie przekierunkowują użytkownika pod niewłaściwy adres (na przykład na stronę www stworzoną przez cyberprzestępcę), mimo że użytkownik będzie widział prawidłowy adres witryny internetowej. Działania mające na celu modyfikację pamięci podręcznej są nazywane „zatruwaniem" adresów DNS. Zazwyczaj następuje to przez przesłanie pocztą elektroniczną tak zwanego konia trojańskiego lub ściągnięciem bezpłatnego programu

[829] DNS - (ang. *Domain Name System* - system nazw domenowych) - jest to protokół komunikacyjny umożliwiający zmianę adresów internetowych zapisanych w postaci mnemonicznej na adresy w postaci numerów IP, zrozumiałych dla urządzeń tworzących sieć komputerową, [za:] A. Kiedrowicz - Wywiał, op. cit., s. 25.
[830] M. Siwicki, *Cyberprzestępczość* …, s. 299.

dostępnego w sieci wirtualnej. Ofiarą tego typu *pharmingu* stają się użytkownicy zainfekowanych komputerów.

2. Ingerencja w pamięć adresów DNS na serwerze - ten typ *pharmingu* jest skierowany nie przeciwko użytkownikom końcowym, lecz przeciwko serwerowi używanemu przez dostawcę usług internetowych. Gdy cyberprzestępcy uda się zaingerować w dane serwera wówczas wszyscy użytkownicy z niego korzystający są automatycznie przekierowywani na stronę sprawcy, a następnie proszeni o zalogowanie lub weryfikację danych[831].

4.1.4 Cyberprzestępstwa związane z treścią informacji

Cyberstalking

Termin *stalking* w języku angielskim oznacza prześladowanie, rozumiane jako „zachowania polegające na wywołaniu uczucia strachu i zagrożenia poprzez świadome i zamierzone naruszenie strefy życia prywatnego i publicznego”[832]. Jolanta Kosińska uznaje za *stalking* „postępowanie sprawcy skierowane bezpośrednio do osoby prześladowanej, obejmujące powtarzające się fizyczne lub wirtualne zbliżanie się do danej osoby, komunikowanie się wbrew jej woli lub werbalne i pisemne groźby, które u każdej rozsądnie myślącej osoby mogą wywołać strach. Przyjmuje się, że *stalking* to zamierzone nękanie przez rozmowy telefoniczne, SMS-y, e-maile czy listy, któremu towarzyszą groźby i agresywne zachowania, śledzenie, obserwowanie, podglądanie, wywołujące u ofiary negatywne emocje, od strachu po skrępowanie”[833].

Cyberstalking jest odmianą tradycyjnej formy *stalkingu.* Jerzy Akińcza uznaje go za: „dręczenie ofiary za pomocą sieci Internet, co może być dokonywane poprzez podszywanie się pod daną osobę na różnych forach, czatach, portalach społecznościowych, rozpowszechnianie nieprawdziwych informacji, a w skrajnych przypadkach włamywanie za pomocą odpowiednich narzędzi do komputera ofiary i przeglądaniu jej osobistych

[831] A. Kiedrowicz-Wywiał, op. cit., s. 26-27.
[832] M. Siwicki, *Cyberprzestępczość* …, s. 274.
[833] J. Kosińska, *Prawnokarna problematyka stalkingu*, „Prokuratura i Prawo” 2008, nr 10, s. 33.

dokumentów"[834]. Według innej definicji polega ono na „prześladowaniu e-mailowym w postaci przekazywania wiadomości na konto pocztowe ofiary wbrew jej woli, uniemożliwianiu korzystania ze skrzynki pocztowej, rozsyłaniu niechcianych przesyłek od ofiary, jako nadawcy. Prześladowanie w Internecie polega na podszywaniu się pod ofiarę na chatach (czatach), grupach usenetowych, forach itp., rozpowszechnianiu informacji o ofierze, może także objawiać się we włamaniach do komputera osobistego ofiary"[835]. Niezależnie od stosowanych definicji *cyberstalking* powoduje u ofiary poczucie skrępowania, zastraszenia i obawy o życie swoje bądź osób bliskich.

Stalkerem jest osoba stosująca przemoc, grożąca popełnieniem przestępstwa, rozpoczęciem postępowania karnego bądź rozgłaszająca informacje naruszające cześć ofiary lub osób jej najbliższych[836]. Zachowanie stalkera, czyli prześladowcy obejmuje szeroki wachlarz zachowań. Może ono polegać na natrętnym wykonywaniu „głuchych" telefonów, wysyłaniu SMS-ów, e-maili, składaniu w imieniu ofiary zamówień (na przykład pocztowych), śledzenie, kontrolowanie ofiary, włamania do domu, samochodu ofiary, kradzież jej rzeczy osobistych czy nawet napaści i pobicia rodziny i przyjaciół ofiary[837].

Ofiarami *stalkingu* może być każdy, najczęściej jest nią były partner czy współpracownik prześladowcy, jednakże mogą być nimi osoby zupełnie obce, w stosunku do których *stalker* stworzył wyimaginowany związek uczuciowy, na przykład gwiazdy filmu czy sportu[838]. W zagranicznej doktrynie wyróżnia się trzy podstawowe rodzaje *stalkingu*:

- *after-intimate-relationship-stalking* - *stalking* po związku intymnym z ofiarą; w przypadku tego rodzaju *stalkingu*, prześladowca i ofiara dobrze się znają, tworzyli wcześniej parę, byli kolegami z pracy czy sąsiadami,
- *acquaintance-stalking* - gdzie stalkerem jest znajomy; cechą charakterystyczną jest mniejszy stopień znajomości i zażyłości, jednakże ofiara osobiście poznała stalkera,

[834] J. Akińcza, *Stalking - zjawisko, odpowiedzialność karna*, „Jurysta" 2012, nr 12, s. 6.
[835] J. Kosińska, op. cit., s. 34.
[836] Ibidem, s. 33.
[837] A. Siemaszko (red.), *Stalking w Polsce - rozmiary - formy - skutki -. Raport z badania nt. uporczywego nękania*, „Archiwum Kryminologii" 2010, t. 32, s. 46.
[838] Ibidem, s. 217.

- *stranger-stalking* - występuje w przypadku, gdy ofiara nigdy nie poznała swego prześladowcy, najczęściej dotyczy on osób sławnych, gwiazd kina, sportowców czy polityków[839].

Monika Raszkowska i Irena Malinowska wyrażają pogląd, że: „stalker ma zafałszowane poczucie własnej wartości, silnie uzależnione od osoby, która go porzuciła. Odrzucenie przez obiekt uczuć wzbudza w nim poczucie wstydu i poniżenia, co wpływa na obniżenie się jego samooceny. W celu pozbycia się tego poczucia oraz przywrócenia poprzedniego *status quo* stara się sprawować kontrolę nad życiem swej ofiary. Prowadzi do ciągłego nachodzenia tej konkretnej osoby, szukania z nią kontaktu, składania propozycji, wysyłania listów, prezentów, aranżowania spotkań. Dalsze kontakty z ukochaną pozwalają na odzyskanie równowagi oraz powrót do poprzedniego poziomu samooceny"[840].

Cyberstalking jest zachowaniem analogicznym do tradycyjnej formy *stalkingu* w aspekcie jego skutków (wywołania poczucia strachu i zagrożenia), jednakże rozwój nowych technologii, w tym Internetu, spowodował, że prześladowanie przybrało zupełnie nową formę. Emma Ogilvie wyodrębniła następujący katalog *cyberstalkingu*:

- *e-mail stalking* - polegający na bezpośredniej komunikacji za pośrednictwem e-maila. Wysyłanie niechcianych wiadomości e-mail jest jedną z podstawowych form nękania, do pozostałych zaliczyć można wysyłanie ofierze wirusów komputerowych; Emma Ogilvie stoi na stanowisku, iż wysyłanie wirusów samo w sobie nie będzie wyczerpywało znamion *stalkingu*, chyba że programy te będą powodowały automatyczne pobieranie treści niepożądanych na przykład pornografii,
- *Internet stalking* - globalna komunikacja za pomocą sieci Internet; cyberstalkerzy używają Internetu by oczernić i zastraszyć swoje ofiary; ten rodzaj *stalkingu,* w przeciwieństwie do *e-mail stalkingu* ma wymiar publiczny, a nie prywatny, odbiorcami jest nie tylko sama ofiara, lecz szersza rzesza użytkowników sieci; sprawcy *cyberstalkingu* posługujący się tą metodą podszywając się pod ofiarę na czatach internetowych, forach dyskusyjnych, portalach społecznościowych bądź za pomocą wspomnianych mediów zamieszczają nieprawdziwe i krzywdzące informacje o ofierze, udostępniają ich dane osobowe, numery telefonów,

[839] U. Smart, *The Stalking Phenomenon: Trends in European and International Stalking and Harassment Legislation*, "European Journal of Crime, Criminal Law and Criminal Justice" 2001, s. 209.
[840] M. Raszkowska, I. Malinowska, *Stalking jako problem społeczny*, „Przegląd Policyjny" 2013, nr 2, s. 218.

- *computer stalking* - nieuprawnione przejęcie przez *stalkera* kontroli nad komputerem ofiary[841].

Maciej Siwicki powołując się na amerykańskie Narodowe Centrum dla Ofiar Przestępstw podaje, iż ofiarą *stalkingu* jest co 12 kobieta i co 45 mężczyzna, a rocznie w USA nękanych jest ponad milion kobiet i 370 tysięcy mężczyzn. Dane z innych krajów kształtują się podobnie: ofiarami *stalkerów* pada 12% badanych w Anglii i Walii, 9% w Szwecji, 11,6% w Niemczech a we Włoszech aż 20%[842]. Justyna Skarżyńska - Sernaglia przeprowadziła podobne badania w Polsce, w trakcie których okazało się, że:

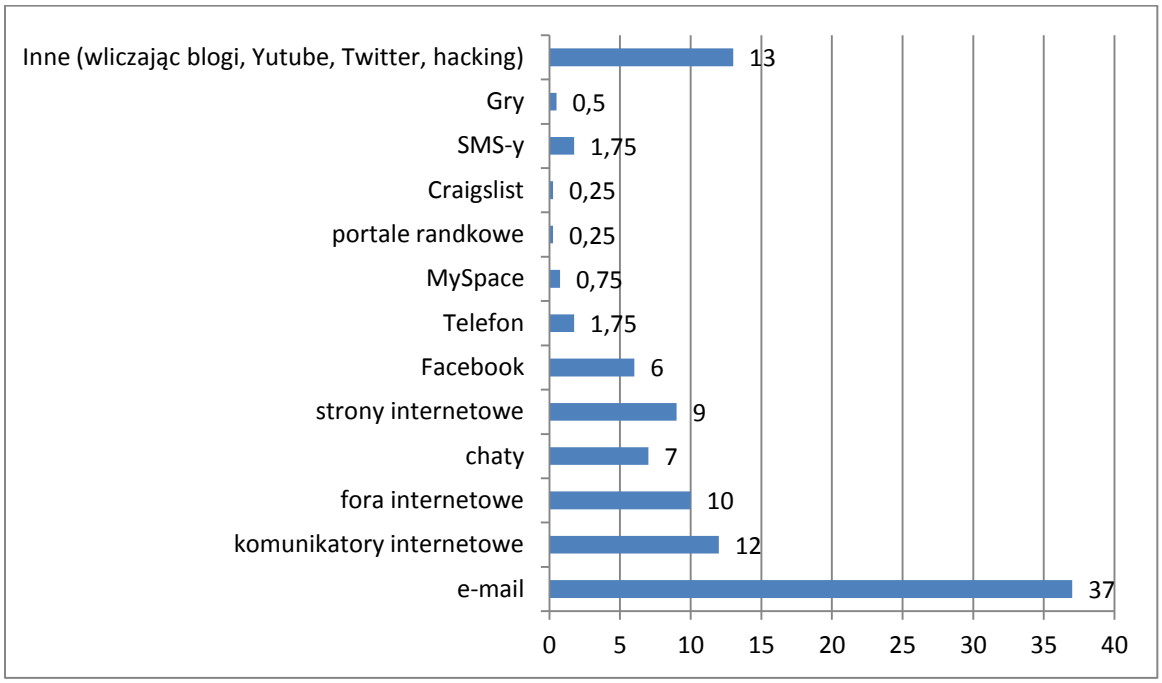
- „12% osób badanych jest lub było ofiarą stalkingu,
- ofiarami stalkingu w 72% są kobiety a w 28% – mężczyźni,
- 63% ofiar stalkingu to kobiety w wieku poniżej 40 lat,
- 82% ofiar (mężczyzn i kobiet) wskazało na mężczyznę jako swojego prześladowcę,
- 75% sprawców to mężczyźni poniżej 40 roku życia,
- w 88% przypadków stalkingu istniała relacja znajomości między ofiarą i napastnikiem, z czego w 58% autorem stalkingu był partner lub była partnerka,
- średni okres prześladowania to półtora roku (18 miesięcy), dla 81% ofiar okres prześladowania trwał od kilku miesięcy do 2 lat; najdłuższy okres prześladowania to 8 lat,
- tylko 15% ofiar podało, iż fakt prześladowania zgłaszało policji (brak danych o formie tych zgłoszeń i krokach podjętych przez policję),
- u 62% ofiar doświadczenie stalkingu wpłynęło negatywnie na ich życie i zdrowie, wywołując poczucie zagrożenia, niepokój, zaburzenia psychosomatyczne i problemy w relacjach interpersonalnych (skutki psychiczne i relacyjne), w tym: zaburzenia niepokoju (ataki paniki, fobie itp.) – u 49% ofiar, zaburzenia snu, zaburzenia odżywiania – u 22% ofiar, zmiany lub trudności w kontaktach interpersonalnych – u 57 % ofiar,
- 22% ofiar nie opowiedziało nikomu o tych wydarzeniach, 36% opowiedziało przyjacielowi, 12% - koledze z pracy, 62% - rodzinie, 53% - partnerowi, 8% - znajomym, 4% - ex-partnerowi,

[841] E. Ogilvie, *Cyberstalking*, artykuł dostępny na oficjalnej stronie internetowej Australian Institute of Criminology, http://www.aic.gov.au/documents/4/7/A/%7B47A7FA60-8EBF-498A-BB9E-D61BC512C053%7Dti166.pdf [16.05.2014].
[842] M. Siwicki, *Cyberprzestępczość*..., s. 275-276.

- w 73,3% przypadków – prześladowanie już się zakończyło, a w 26% przypadków trwało w okresie przeprowadzanego badania”[843].

Wyniki badań organizacji WHOA (ang. *Working to Halt Online Abuse*)[844] przeprowadzone w latach 2000-2013 wskazują, iż cyberprzestępczość przybiera formy wyszczególnione na rysunku 6:

Rysunek 7. Formy *cyberstalkingu*



Źródło: opracowanie własne na podstawie statystyk WHOA z lat 2000-2013. Statystyki dostępne na stronie: http://www.haltabuse.org/resources/stats/Cumulative2000-2013.pdf [17.05.2014] .

Najczęściej wykorzystywaną formą komunikacji w przypadku *cyberstalkingu* były e-maile, komunikatory i fora internetowe, czaty i portale społecznościowe. Facebook wydaje się być idealnym narzędziem do *cyberstalkingu* i zdobywania informacji o ofierze. Przedstawione zestawienie wprawdzie obejmuje lata 2000-2013, jednakże organizacja WHOA monitoruje nękanie za pośrednictwem Facebooka dopiero od 2009 roku, stąd też w odniesieniu do całej dekady to stosunkowo niski wynik.

[843] J. Skarżyńska - Sernaglia, *Stalking w Polsce - występowanie i charakterystyka zjawiska*, Artykuł dostępny na http://psychologia.net.pl/artykul.php?level=415 [16.05.2014].
[844] WHOA (ang. *Working to Halt Online Abuse*) - założona w 1997 r. amerykańska organizacją, powołana do zwalczania internetowego nękania. Cel organizacji ma zostać osiągnięty poprzez edukację społeczeństwa, w tym społeczności internetowej, czym jest cyberstalking, pomoc ofiarom cyberstalkingu oraz walka ze tą formą przestępczości.

Maciej Siwicki odnosząc się do kwestii norm krajowych zagadnienia *cyberstalkingu* podaje, że przestępstwo to znalazło między innymi uregulowanie w 18 USC § 2261A, według którego „czyn zabroniony stanowi wykorzystanie poczty elektronicznej, jakiejkolwiek interaktywnego serwisu komputerowego lub też jakiejkolwiek usługi komercyjnej (krajowej lub zagranicznej), w celu spowodowania znaczącego uczucia dyskomfortu innej osobie (ang. *substantial emotional distress*) lub też wzbudzenie u niej uzasadnionego strachu o zdrowie (ang. *resonable fear of the death of, or serious bodily injury*) własne lub członków rodziny, małżonka lub partnera"[845].

Z kolei australijski stan Wiktoria w rozdziale *Stalking i przemoc domowa* (ang. *Stalking and Family Violence*) w art. 21 A ust. 2 kodeksu karnego[846] ustanowił, iż *cyberstalkingiem* jest:

- kontaktowanie się z ofiarą lub jakąkolwiek inną osobą za pomocą telefonu, faksu, SMS-a, e-maila lub za pomocą innych form komunikacji elektronicznej (lit. b),
- publikowanie w Internecie, za pomocą e-maila lub innego środka komunikacji elektronicznej materiałów lub informacji odnoszących się do ofiary lub jakiejkolwiek innej osoby, lub też mających sprawiać wrażenie, iż pochodzą one od ofiary lub jakiejkolwiek innej osoby (lit. ba),
- spowodowanie nieuprawnionych działań i czynności w komputerze ofiary lub w komputerze jakiejkolwiek innej osoby (lit. bb),
- śledzenie wykorzystywania przez ofiarę lub jakąkolwiek inną osobę Internetu, e-maila lub innego środka komunikacji elektronicznej (lit bc).

Przedstawiciele doktryny stoją na stanowisku, że porównanie porządków prawnych różnych państw odnoszących się do *stalkingu* pozwala na określenie dwóch metod jego penalizacji: syntetyczną i kazuistyczną. Pierwsza jest uwarunkowana syntetycznym sposobem postępowania sprawcy. Jako elementy składowe czynów wymienia się okres nękania czy też liczbę czynów niezbędnych do uznania za wyczerpanie znamion *stalkingu*. Oznacza to, iż najistotniejszym aspektem tego przestępstwa będzie powtarzalność zachowań sprawcy i ich długotrwałość. Zaletą *stalkingu* w takiej postaci jest elastyczność, wadą nieostrość pojęć i trudność stwierdzenia czy określona kategoria czynów będzie już wyczerpywała znamiona

[845] M. Siwicki, *Cyberprzestępczość*…, s. 278.
[846] Tekst australijskiego kodeksu karnego w języku angielskim dostępny na: http://www.austlii.edu.au/au/legis/vic/consol_act/ca195882/s21a.html [17.05.2014].

przestępstwa[847]. Druga polega na wyliczeniu, nierzadko w zamkniętym katalogu, kategorii czynów, które za *stalking* zostaną uznane. Rozwiązanie takie sprzyja klarownej sytuacji prawnej, jednakże nie można mu przypisać cech elastyczności, przez co może nastręczyć szczególnych problemów w kontekście postępu technologicznego i pojawiających się nieustannie nowych metod działania cyberprzestępców[848].

Wolność słowa a mowa nienawiści w cyberprzestrzeni

Za mowę nienawiści (ang. *hate speach*) uznać należy wszelkiego rodzaju wypowiedzi nawołujące do nienawiści wobec określonych grup czy mniejszości. Anna Śledzińska - Simon uznaje, że jest to „wypowiedź pisemna, ustna, symboliczna, która czyni przedmiotem ataku jednostkę lub grupę osób ze względu na kryterium rasy, pochodzenia etnicznego, narodowego, religii, języka, płci, wieku, niepełnosprawności, statusu społecznego czy przekonań politycznych. Mowa nienawiści może zastraszać, grozić, poniżać, obrażać a także utrwalać stereotypy i prowadzić do dyskryminacji a nawet przemocy fizycznej"[849]. Mowa nienawiści może przybrać postać aktywną w postaci publikacji czy też dystrybucji zakazanych materiałów, ale również postać bierną, polegającą na posiadaniu materiałów zakazanych. Niejednokrotnie penalizacja tego czynu jest uzależniona od spełnienia dodatkowych czynników takich, jak wypowiedź o charakterze publicznym czy też powodowanie zakłócenia spokoju społecznego[850].

Przedstawiciele doktryny podkreślają, że mowa nienawiści podnosi kwestię konfliktu dwóch różnorodnych wartości - wolności słowa i dóbr osobistych jednostek. „Wolność słowa oznacza bowiem, że każdy człowiek ma prawo do wolności opinii i wyrażania jej bez ingerencji władz publicznych i bez względu na granice państwowe"[851]. Z tego powodu bezwzględne uznanie mowy nienawiści za czyn zabroniony może potencjalnie prowadzić do

[847] M. Siwicki, *Cyberprzestępczość*…, s. 279.
[848] Ibidem, s. 279-280.
[849] A. Śledzińska-Simon, *Decyzja ramowa w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii Europejskiej,* [w:] R. Wieruszewski (red.) *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010, s. 94.
[850] Ibidem, s. 95.
[851] Por. art. 19 Powszechnej Deklaracji Praw Człowieka (PDPC), 10 i 11 Karty Praw Podstawowych Unii Europejskiej, art. 19 Międzynarodowego Paku Praw Obywatelskich i Politycznych (MPPOiP), art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (EKPCz), art. 13 Amerykańskiej Deklaracji Praw i Obowiązków Człowieka (AKPCz).

konfliktu normatywnego z prawem do wolności słowa. Każde zatem z przeciwstawnych sobie praw, a więc z jednej strony ochrona prawa do wyrażania indywidualnych opinii, z drugiej zaś ochrona społeczeństwa jako całości, z punktu widzenia roli w społeczeństwie demokratycznym na równy status. Przeciwstawienie ich sobie nie stwarza łatwych możliwości do wytyczania istniejących między nimi granic. Z tego względu nie jest możliwe także sformułowanie wyczerpującej definicji tego, co stanowi dopuszczalną ingerencję w realizację prawa do wolności słowa tam, gdzie jest ona skierowana przeciwko innym podmiotom. Przyczynę takiego stanu rzeczy należy upatrywać również w fakcie, że nie da się ustalić dla całej Europy, a tym bardziej dla całego świata jednej koncepcji znaczenia wolności słowa. Stąd też mowa nienawiści na gruncie poszczególnych systemów prawnych jest tolerowana, wśród innych - zakazana"[852]. Granice wolności słowa będą wyznaczane odmiennie w europejskim porządku prawnym, odmiennie w USA. Swoboda wypowiedzi związana z obrazą uczuć religijnych będzie wywoływała inne skutki w państwach laickich, inne w krajach katolickich czy muzułmańskich. Dlatego też ciężko jest przyjąć jeden, globalny paradygmat wolności słowa w cyberprzestrzeni.

Maciej Siwicki zauważa, że „w prawie porównawczym klasyfikacja prawna mowy nienawiści nie ma jednolitego charakteru. Z jednej strony część państw przyjmuje pogląd, że stanowi ona zagrożenie dla porządku publicznego, z drugiej jednak strony niektóre państwa wskazują, że przez wzgląd na prawo do wolności słowa powinna być ona dopuszczalna. Stąd też w prawie porównawczym można mówić o ukształtowaniu się dwóch generalnych podejść jej kryminalizacji. Pierwsze, bardziej restrykcyjne, przyjmuje, że określone propagandowe lub dyskryminujące wypowiedzi będą zawsze karalne. Rozwiązania takie występują przede wszystkim w ustawodawstwie państw europejskich, które w wyniku doświadczeń spowodowanych II wojną światową dążą do eliminacji podstaw, które mogą stanowić zagrożenie dla jednostek, społeczeństwa i demokracji. Inny schemat karalności mowy nienawiści przyjęty został między innymi w ustawodawstwie karnym krajów systemu anglosaskiego. Według niego penalizowane są tylko takie wypowiedzi, które połączone są z konkretnym przestępstwem (lub zagrożeniem), na przykład atakiem czy przemocą skierowaną przeciwko określonej grupie, jak i jednostce"[853]. Pogląd ten wydaje się również podzielać Anna Śledzińska - Simon, która stwierdza że „walka z rasizmem i ksenofobią jest bowiem konsekwencją naczelnej zasady poszanowania godności ludzkiej oraz podstawowych

[852] M. Siwicki, *Karalność mowy nienawiści w Internecie - aspekty prawnoporównawcze*, „Palestra" 2007, nr 5-6, s. 63-64.
[853] Ibidem, s. 61-62.

wolności i praw, na których oparł się powojenny europejski porządek prawny. Rasizm stanowi zaś zaprzeczenie uznania równej wolności godności wszystkich ludzi praz ich praw podmiotowych. Karanie mowy nienawiści skierowanej do jednostek lub grup jest uzasadnione z jednej strony względami ochrony praw jednostki, a z drugiej koniecznością zapewnienia porządku publicznego oraz zapobiegania konfliktom społecznym"[854].

Podkreślić należy, iż mowa nienawiści może wyczerpywać znamiona wielu różnych czynów zabronionych, czyli zniewagi, zniesławienia, nawoływania do popełnienia przestępstw przeciwko życiu i zdrowiu, pochwalania lub umniejszania zbrodni ludobójstwa, zbrodni przeciwko ludzkości czy też propagowanie nazizmu i faszyzmu. W Stanach Zjednoczonych za mowę nienawiści uznaje się wypowiedzi nawołujące do przemocy - z kolei w Europie te nawołujące od nienawiści, lub też wyrażające zniewagę czy pogardę[855]. Przesłanką przemawiającą za tym, iż nie każda wypowiedź powinna podlegać penalizacji jest fakt, iż zbytnie obostrzenie mowy nienawiści doprowadziłoby tak naprawdę do cenzury i zanegowania dozwolonej krytyki, a nawet ograniczenia swobody badań naukowych czy twórczości artystycznej[856].

Pornografia dziecięca w Internecie

Termin pornografia (z gr. *porné* – 'najtańsza prostytutka, niewolnica' oraz *gràphō* – 'pisać, rytować lub rysować') zdefiniować można, jako „przedstawienie przejawów życia seksualnego ze szczególnym zwróceniem uwagi na uwidocznienie narządów płciowych i z wyłączeniem wszelkich psychicznych oraz społecznych związanych z seksualnością człowieka"[857]. Jarosław Warylewski uważa, że „treści pornograficzne" oraz synonimiczna dla nich „pornografia" w rozumieniu wąskim (normatywnym) to treści zawarte w dającym się wyodrębnić przekazie informacyjnym (prezentacji) bądź w jego istotnych i odpowiednio spójnych fragmentach w formie materialnej lub zdematerializowanej, utrwalone za pomocą dowolnego nośnika lub nieutrwalone, charakteryzujące się tym, iż przedstawiają w jakiejkolwiek formie autentyczne lub tylko wyobrażone (wykreowane) przejawy płciowości

[854] A. Śledzińska-Simon, op. cit., s. 94-95.
[855] Ibidem, s. 96.
[856] Ibidem, s. 95.
[857] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011, s. 132.

lub życia seksualnego człowieka w wymiarze ograniczonym (sprowadzonym) do funkcji fizjologicznych oraz aspektów techniczno - biologicznych"[858]. Można wyróżnić trzy rodzaje pornografii: pornografię twardą (ang. *hardcore pornography*), pornografię miękką (ang. *soft core pornography*) i pornografię dziecięcą (ang. *child pornography*). W niniejszym opracowaniu zostanie opisana pornografia dziecięca w Internecie.

W art. 9 ust. 1 Konwencji o cyberprzestępczości państwa strony zobowiązują się podjąć wszelkie niezbędne kroki ustawodawcze w celu uznania za przestępstwa w prawie krajowym umyślnych i bezprawnych czynów popełnianych za pomocą systemu informatycznego:

- produkowania pornografii dziecięcej i jej rozpowszechniania,
- oferowania lub udostępniania pornografii dziecięcej,
- rozpowszechniania lub transmitowanie pornografii dziecięcej,
- pozyskiwania pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby,
- posiadania pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych.

Pornografia dziecięca w świetle art. 9 ust. 2 Konwencji winna być rozumiana jako materiał pornograficzny, który w sposób widoczny przedstawia a) osobę małoletnią w trakcie czynności wyraźnie seksualnej, b) osobę, która wydaje się być nieletnią, w trakcie czynności wyraźnie seksualnej, c) realistyczny obraz przedstawiający osobę małoletnią w trakcie czynności wyraźnie seksualnej. Za osobę małoletnią uznano w ust. 3 osobę poniżej 18 roku życia. W omawianym traktacie przyznano państwom - stronom uprawnienie do ustalenia innej granicy wieku małoletniego, lecz nie może być ona niższa niż 16 lat.

Konwencja o cyberprzestępczości nie zawiera definicji materiału pornograficznego, pozostawiając regulację tej kwestii państwom - stronom. Jednakże w pkt. 100 raportu wyjaśniającego do Konwencji wskazano, że termin „czynność wyraźnie seksualna" (ang. *sexually explicit conduct*) odnosić się winien do rzeczywistego bądź udawanego:

[858] J. Warylewski, *Pornografia - próba definicji*, [w:] M. Mozgawa (red.), *Pornografia*, Warszawa 2011, s. 125.

- stosunku seksualnego, wliczając w to stosunki pomiędzy organami płciowymi, stosunki analne, oralne oraz oralno - genitalne, pomiędzy małoletnimi bądź pomiędzy dorosłym a małoletnim, tej samej lub różnej płci,
- sodomię (ang. *bestiality*),
- masturbację,
- sadystyczne lub masochistyczne wykorzystanie w kontekście seksualnym,
- lubieżne przedstawianie (obnażanie) genitaliów lub miejsc intymnych małoletniego.

Z kolei dyrektywie Parlamentu Europejskiego i Rady 2011/93/UE z 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującą decyzję ramową Rady 2004/68/WSiSW - art. 2 c) uznano, że pornografia dziecięca to:

- wszelkie materiały ukazujące dziecko uczestniczące w rzeczywistych lub symulowanych zachowaniach o wyraźnie seksualnym charakterze,
- wszelkie przedstawienia organów płciowych dziecka w celach głównie seksualnych,
- wszelkie materiały ukazujące osobę wyglądającą na dziecko uczestniczącą w rzeczywistych lub symulowanych zachowaniach o wyraźnie seksualnym charakterze oraz przedstawienia organów płciowych osób wyglądających jak dziecko, w celach głównie seksualnych, lub
- realistyczne obrazy dziecka uczestniczącego w zachowaniach o wyraźnie seksualnym charakterze lub realistyczne obrazy organów płciowych dziecka, w celach głównie seksualnych.

Podkreślić w tym miejscu należy, iż opisywana dyrektywa w art. 2 a), jako dziecko określa każdą osobę poniżej 18 roku życia. Jednakże nie zdecydowano się na wprowadzenie do jej postanowień granicy wieku poniżej którego, zakazane jest podejmowanie czynności seksualnych z udziałem dziecka. Kwestię tę pozostawiono w gestii prawa krajowego państw członkowskich (art. 2 b). Polskie standardy prawne przewidują niższą granicę wieku ochrony małoletnich niż wskazane wyżej akty prawne. Polski Kodeks karny penalizuje przestępstwa przeciwko wolności seksualnej i obyczajności na szkodę małoletniego poniżej 15 roku życia.

Ustawodawstwo większości państw nie zawiera szczegółowego katalogu czynów uznanych za przestępstwo seksualne na szkodę małoletnich. Definicje charakteryzują z zasady dwa czynniki powodujące penalizację czynu. Pierwszym z nich jest wskazanie rodzaju

aktywności seksualnej, której poddawany jest małoletni, drugim, zastosowanie dodatkowych elementów wprowadzających karalność czynu. Definicja pornografii dziecięcej w prawie niemieckim ma wąski zakres i oznacza seksualne wykorzystanie dzieci (niem. *sexullen Mißbrauch*). Judykatura niemiecka zalicza również do pornografii dziecięcej materiały fotograficzne przedstawiające dzieci z widocznymi narządami płciowymi, mające wzbudzić w odbiorcy pobudzenie seksualne (niem. *anreißerischer Hervorhebung des Geschlechtsteils*). Wąską definicję przyjęto również w ustawodawstwie Holandii i Austrii, w których warunkiem penalizacji czynu jest „płciowy"[859] bądź „seksualny"[860] charakter treści. Z kolei w Kanadzie elementem warunkującym kryminalizację czynu jest przedstawienie czynności seksualnej (ang. *sexual activity*) bądź organów płciowych (ang. *sexual organ*)[861] małoletniego[862].

W doktrynie został wyrażony pogląd, że „zakres znaczeniowy pojęcia pornografia dziecięca jest wieloznaczny. W prawie porównawczym wyróżnia się zazwyczaj dwa rodzaje aktywności kwalifikowanej, jako pornografia dziecięca. W pierwszym dochodzi do kontaktu fizycznego pomiędzy dzieckiem a sprawcą, zmierza on do zaspokojenia lub pobudzenia popędu seksualnego (akt spółkowania i wszelkie jego surogaty traktowane - zarówno obiektywnie, jak i subiektywnie z punktu widzenia sprawcy - jako ekwiwalentne i równoważne spółkowaniu, polegające na bezpośrednim kontakcie płciowym części ciała sprawcy z ciałem dziecka). Drugi obejmuje zachowania bez takiego kontaktu, czyli onanizowanie się, obnażanie narządów płciowych czy też zmuszanie dziecka do podobnych czynności, w tym również w oglądanie materiałów pornograficznych"[863].

W celu przeprowadzenia dalszych rozważań należy ustalić, w jaki sposób następuje dystrybucja pornografii dziecięcej w Internecie. Zazwyczaj przeprowadzana jest ona dwoma kanałami. Pierwszy z nich następuje za pomocą komercyjnych sieci komputerowych, które udostępniają treści o określonej tematyce odpłatnie. Drugim jest wykorzystanie niekomercyjnych metod wymiany informacji. Zaliczyć do nich można pocztę e-mail czy też zamknięte grupy dyskusyjne umożliwiające wymianę plików[864]. Pornografia dziecięca to nie tylko fotografie czy zdjęcia rzeczywistych dzieci, lecz również komputerowe czy też animowane postacie przedstawiające małoletnich. Uznanie tego typu obrazów za pornografię

[859] Austriacki kodeks karny (*österreichisches* StGB), art. 207a.
[860] Holenderski kodeks karny ("[...] *seksuale gedraging* [...]"), art. 240b.
[861] Canadian Criminal Code, art. 163.1(1), 163.1(1).
[862] M. Siwicki, *Cyberprzestępczość*…, s. 181.
[863] Ibidem, s. 183.
[864] M. Siwicki, *Nielegalna …*, s. 44.

jest zasadne. Mimo, że prawdziwe dziecko nie pada ofiarą tego typu przestępstwa, to odbiorca tego typu pornografii rozbudza w sobie pociąg seksualny dzieci, który może zostać wykorzystany na prawdziwym dziecku.

Wydaje się, że wirtualny, anonimowy charakter przestrzeni wirtualnej znacznie ułatwił środowiskom pedofilskim dostęp do pornografii dziecięcej - ale również wewnętrzną komunikację tej grupy. Przed rozpowszechnieniem się przestrzeni wirtualnej osoby o skłonnościach pedofilskich nie znały w ogóle, bądź znały jedynie nieliczną garstkę osób o podobnych preferencjach, a wymienianie się materiałami wiązało się z ogromnym ryzykiem.

Niestety Internet umożliwił tym środowiskom, ekspansję dokonywanych czynności między innymi:

1) „stały kontakt z innymi osobami zainteresowanymi wykorzystywaniem seksualnym dzieci,
2) możliwość dyskusji o swoich seksualnych preferencjach,
3) możliwość wymiany informacji na temat sposobów pozyskiwania ofiar,
4) wsparcie dla swoich preferencji seksualnych,
5) stały dostęp do potencjalnych ofiar,
6) możliwość podszycia się pod rówieśnika potencjalnej ofiary,
7) łatwość pozyskiwania danych o potencjalnych ofiarach (jak np. adres zamieszkania, e-mail, numer telefonu itp.),
8) możliwość nawiązania długoterminowej znajomości internetowej w celu późniejszego nawiązania kontaktów seksualnych z nieletnim”[865].

Ostatnie z wymienionych zjawisk jest nazywane *groomingiem* (ang. *child grooming*). Działanie to jest podejmowane w celu zaprzyjaźnienia się z dzieckiem, zdobyciem jego zaufania, by następnie wykorzystać je seksualnie. *Grooming* jest jedną z czterech kategorii czynów przestępczych związanych z pornografią dziecięcą. Drugą kategorią jest produkcja, trzecią - rozpowszechnianie, dystrybucja, oferowanie oraz udostępnianie, a czwartą - przechowywanie i posiadanie pornografii dziecięcej[866]. *Grooming* polega na bezpośrednim kontakcie z małoletnim, wobec czego może doprowadzić do spotkania z pedofilem i

[865] A. Wrona, *Cyberpornografia i cyberseks*, [w:] J. Bednarek, A. Andrzejewska (red.), *Cyberświat - możliwości i zagrożenia*, Warszawa 2009, s. 312.
[866] M. Siwicki, *Cyberprzestępczość*…, s. 187.

popełnienia kolejnych czynów zabronionych takich, jak porwanie, gwałt, zmuszanie do prostytucji.

Grooming nie jest zjawiskiem nowym. Zaprzyjaźnianie się pedofili ze swoim ofiarami było metodą wykorzystywaną wcześniej przez osoby o takich skłonnościach (z kręgu rodziny, znajomych czy nauczycieli). Cyberprzestrzeń rozszerzyła zasięg i możliwości działania przestępców seksualnych. Rachell O'Connell przedstawił następujące etapy rozwoju *groomingu:*

- etap zaprzyjaźniania się (ang. *Friendship-Forming Stage*) - jest to etap, w którym pedofil podejmuje pierwszy kontakt z dzieckiem; prawca pyta się dziecko, czy ma swoje zdjęcie, a jeżeli odpowiedź jest twierdząca pedofil prosi o przesłanie swojej fotografii; jeżeli małoletni mieszka w pobliżu sprawcy nadesłana fotografia może pozwolić mu na zidentyfikowaniu dziecka w rzeczywistym świecie,
- etap nawiązania przyjaźni (ang. *Relationship - Forming Stage*) - w tym etapie sprawca poznaje lepiej dziecko przez zadawanie pytań na temat szkoły czy życia rodzinnego. Sprawca zdobywa zaufanie ofiary, zbiera informacje na jego temat, sprawia wrażenie przyjaciela,
- etap oceny ryzyka (ang. *Risk - Assessment Stage*) - na tym etapie pedofil próbuje zdobyć informacje na temat potencjalnej możliwości zbliżenia się do ofiary; sprawca pyta o położenie komputera w domu, liczbę osób z niego korzystających, nadzoru dorosłych bądź rodzeństwa,
- etap wyłączności (ang. *Exclusivity Stage*) - pedofil przekonuje dziecko na tym etapie, że jest jego najlepszym przyjacielem, tylko on rozumie jego problemy, a dziecko może bezpiecznie powierzyć mu każdy sekret; w ten sposób dorosły stara się zbudować poczucie wzajemnego zaufania, które będzie mógł wykorzystać w przyszłości,
- etap o charakterze seksualnym (ang. *Sexual Stage*) - na tym etapie sprawca podejmuje w rozmowie z dzieckiem tematy o charakterze seksualnym, pyta się o doświadczenia dziecka w tym przedmiocie i tym podobne,

- etap końcowy (ang. *Conclusion*) - jest to próba nawiązania fizycznego kontaktu z ofiarą, propozycja spotkania, ale również nagłe zerwanie kontaktu w celu uniknięcia schwytania[867].

Problem *groomingu* został poruszony między innymi w art. 23 Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystaniem i niegodziwym traktowaniem w celach seksualnych. Wskazany wyżej artykuł stanowi, że państwa strony konwencji przyjmą konieczne środki ustawodawcze lub inne środki w celu zapewnienia karalności umyślnego składania dziecku (które nie ukończyło wieku, poniżej którego istnieje zakaz uczestnictwa w czynnościach seksualnych) przez osobę dorosłą za pośrednictwem technologii informacyjnych i telekomunikacyjnych, propozycji spotkania w celu popełnienia przestępstwa przeciwko wolności seksualnej na szkodę dziecka. Warunkiem karalności jest faktyczne podjęcie działania przez sprawcę mające na celu doprowadzenie do takiego spotkania.

Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW w art. 6 również podjęła kwestię *groomingu*, stanowiąc, że państwa członkowskie UE winny zapewnić karalność czynu umyślnego polegającego na składaniu za pośrednictwem technologii informacyjno - komunikacyjnych przez osobę dorosłą dziecku, które nie osiągnęło jeszcze wieku przyzwolenia, propozycji spotkania w celu popełnienia przestępstw opisanych w art. 3 ust. 4[868] i art. 5 ust. 6[869] dyrektywy. Jeżeli sprawca po złożeniu propozycji podjął kroki służące do doprowadzenia do spotkania z dzieckiem czyn winien podlegać karze co najmniej roku pozbawienia wolności.

Zagadnienie produkcji pornografii dziecięcej zostało poruszone w wielu dokumentach prawnych o charakterze międzynarodowym. Wymóg penalizacji takich czynów znajduje się chociażby w Konwencji Rady Europy o cyberprzestępczości (art. 9), Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystaniem i niegodziwym traktowaniem w celach seksualnych (art. 20) czy też w dyrektywie Parlamentu Europejskiego i Rady 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i

[867] R. O'Connell, *A Typology of Child Cybersexploitation and Online Grooming Practices*, Lancashire 2003, http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf [04.08.2015].
[868] Podejmowanie czynności seksualnych z udziałem dziecka, które nie osiągnęło wieku przyzwolenia.
[869] Produkcja pornografii dziecięcej.

wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (art. 5 ust. 6).

W wymienionych wyżej umowach międzynarodowych strony postanowiły też, że karalna winna być dystrybucja i rozpowszechnianie pornografii dziecięcej. Dokumenty posługują się różną terminologią używając takich słów, jak „publikowanie", „dystrybucja", „udostępnianie", „oferowanie". Można przyjąć, że oferowanie pornografii dziecięcej za pomocą systemu komputerowego oznacza nakłanianie innych osób do nabycia takich materiałów, a „udostępnianie" za zamieszczanie takich materiałów na stronach internetowych w celu skorzystania przez inne osoby.

Międzynarodowe standardy prawne przewidują zbliżony zakres kryminalizacji czynów w zakresie pornografii dziecięcej. Zarówno konwencja o cyberprzestępczości, jak i dyrektywa 2011/93/UE wprowadza szeroką definicję pornografii dziecięcej, przewiduje karalność *groomingu,* rozpowszechniania, udostępniania i posiadania materiałów pornograficznych z udziałem osób poniżej 18 roku życia. Jednakże mimo szeroko zakrojonej międzynarodowej współpracy ściganie przestępstw o charakterze pedofilskim napotyka duże trudności. Podstawową jest transgraniczny charakter tych przestępstw, który powoduje, że organy ścigania mogą napotkać na problemy proceduralne w niejednolitym reżimie prawnym określającym wiek małoletniego czy też cel działania sprawcy[870]. Ma to szczególne znaczenie, ponieważ w przestrzeni wirtualnej można napotkać tak zwane kręgi pedofilskie (ang. *pedophile rings*) - są to międzynarodowe grupy pedofilów, którzy za pośrednictwem cyberprzestrzeni kontaktują się ze sobą, wymieniają treści pornograficzne. Jako przykład można podać rozbity w 1998 roku przez brytyjską policję klub Wonderland - międzynarodową grupę pedofilów, która działała się za pośrednictwem Internetu. W wyniku działań organów ścigania aresztowano 170 podejrzanych z 12 krajów oraz zatrzymano 750 tysięcy zdjęć dzieci oraz 18 tysięcy filmów[871].

Badania dotyczące zjawiska cyberpedofillii wykazały, że statystycznym sprawcą przestępstwa związanego z wykorzystaniem seksualnym dzieci przy użyciu Internetu był mężczyzna (99%), rasy białej (92%), powyżej 25 roku życia (86%), działający w pojedynkę (97%). Co dziesiąty z nich był wcześniej zatrzymywany w sprawach o przemoc seksualną

[870] M. Siwicki, *Nielegalna*…, s. 45.
[871] Artykuł dostępny na oficjalnej stronie internetowej „The Guardian" http://www.theguardian.com /uk/2001/feb/11/tracymcveigh.martinbright [10.07.2015].

wobec dzieci[872]. Statystyczny sprawca mieszka też w mieście, jest stanu wolnego, nie posiada dzieci, ale zazwyczaj pracuje zawodowo (58,9%), uczy się lub studiuje (17,7%) i ma wykształcenie średnie lub wyższe (67,7%)[873].

Cyberprzestępczość wzbudza duże emocje na arenie międzynarodowej. Wypracowanie wspólnego stanowiska w kwestii cyberataków, oszustw czy wolności słowa w sieci wirtualnej jest procesem długotrwałym, a przeciwstawne interesy i kultury prawne różnych państw nie ułatwiają wypracowania międzynarodowego konsensusu. Sprawa ma się inaczej w przypadku pornografii dziecięcej. Dobro dzieci jest dobrem najwyższym i niezależnie od zakątku globu małoletni są otaczani specjalną opieką. Społeczność międzynarodowa stosunkowo łatwo osiągnęła porozumienie uznając, iż konieczna jest penalizacja zachowań o charakterze pedofilskim w cyberprzestrzeni. Dzięki Internetowi osoby o tych skłonnościach zaczęli zgromadzić się w internetowe grupy i wymieniać danymi na ogromną skalę. Walka z pornografią dziecięcą musi zatem być podjęta na poziomie międzynarodowym. Na aprobatę zasługują stosunkowo zbieżne postanowienia międzynarodowych traktatów penalizujących pornografię dziecięcą, ale również jej udostępnianie i rozpowszechnianie. Zastrzeżenie budzi jednak fakt, że normy te są rozproszone w kilku aktach prawnych. Rekomendowanym rozwiązaniem byłoby zatem ratyfikowanie Konwencji z Lanzarote przez jak największą liczbę państw - również spoza Rady Europy.

Zaakcentować należy, że pornografia dziecięca i pedofilia w cyberprzestrzeni nie jest jedynym sposobem wykorzystania dzieci za pomocą sieci komputerowych. Przestrzeń wirtualna jest wykorzystana również do handlu dziećmi (głównie do prostytucji), oglądania przez dzieci pornografii przedstawiającej ludzi dorosłych czy też wirtualnego seksu. Kwestie te nie zostaną jednak szczegółowo omówione w niniejszej dysertacji ze względu na chęć uniknięcia zbytniej kazuistyczności podejmowanych tematów.

[872] Ł. Wojtasik, *Materiały dla uczestników konferencji wojewódzkich realizowanych w ramach kampanii "Dziecko w sieci" i programu UE "Safer Internet Action Plan" w latach 2006-2016*, s. 18.
[873] M. Mozgawa, P. Kozłowska-Kalisz, *Pornografia dziecięcia w świetle badań empirycznych (aspekty prawnokarne)*, [w:] M. Mozgawa, *Pornografia*, Warszawa 2011, s. 189.

4.1.5 Kradzież tożsamości w cyberprzestrzeni

Przywłaszczenie tożsamości innej osoby jest nazywane potocznie kradzieżą tożsamości. Czyn taki określa się również jako defraudację tożsamości, fałszerstwo tożsamości czy też przejmowanie tożsamości[874]. Za kradzież tożsamości uznać należy bezprawne, instrumentalne przywłaszczenie lub wykorzystanie tożsamości innej, żyjącej, zmarłej lub fikcyjnej osoby fizycznej w celu osiągnięcia korzyści majątkowej lub naruszenia innych dóbr prawnie chronionych, pod groźbą kary[875]. Podszywanie się pod inną osobę penalizowane jest jedynie wówczas, gdy sprawca działa w celu popełnienia jakiegoś przestępstwa lub wyrządzenia szkody danej osobie[876].

Pierwsza legalna definicja kradzieży tożsamości pojawiła się w amerykańskiej ustawie o kradzieży tożsamości (*Identity Theft and Assumption Deterrence ACT*) z 30 września 1998 r., uznano w niej, iż jest to świadome transferowanie (ang. *knowing transfer*), posiadanie (ang. *possession*) lub użycie (ang. *use*) bez upoważnienia informacji służących do identyfikacji innej osoby (ang. *identyfying information*), w celu popełnienia przestępstwa federalnego, stanowego lub lokalnego[877].

Zjawisko kradzieży tożsamości upowszechniło się wraz z rozwojem techniki. Arkadiusz Lach wyraził pogląd, że „nowoczesne technologie przetwarzania informacji oraz usługi dostępne w społeczeństwie informacyjnym opierają się na nowych sposobach identyfikacji, w których często nie ma bezpośredniego kontaktu pomiędzy osobą posiadającą dane osobowe, a osobą je sprawdzającą. Częściej także weryfikuje się to, co dana osoba wie (login i hasło) lub posiada (token, dokument, karta dostępu) niż bezpośrednio to, kim ona jest (na przykład przez weryfikację linii papilarnych lub wzoru siatkówki oka). Z tego względu popełnienie przestępstwa jest ułatwione. Mniejsze jest także ryzyko wykrycia. Poza tym dane osobowe przetwarzane są na coraz większą skalę i dostępne zarówno w Internecie oraz bazach danych. Zarówno podmioty publiczne, jak i prywatne posiadają ogromne nieraz bazy danych osobowych, które stanowią cel ataku przestępców. Z tego względu pokrzywdzony

[874] K. Czaplicki, *Kradzież tożsamości w Internecie,* [w:] G. Szpor (red.), *Internet. Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011, s. 399.
[875] M. Siwicki, *Cyberprzestępczość*…, s. 284.
[876] A. Lach, *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3, s. 29.
[877] § 003 Identity Theft and Assumption Deterrence ACT z 30.09.1998 r. Tekst w języku angielskim dostępny na: http://www.ftc.gov/node/119459#003 [22.05.2014].

często nie wie, w jaki sposób sprawca wszedł w posiadanie jego danych. Dla uzupełnienia obrazu sytuacji należy sobie uzmysłowić, że dane osobowe stały się towarem, który na internetowym czarnym rynku posiada określoną wartość"[878]. Pogląd ten jest wyjątkowo trafny. Zwłaszcza w cyberprzestrzeni jesteśmy często proszeni o udostępnienie naszych danych osobowych (na przykład przez wypełnienie formularza). Przestępca, który wejdzie w posiadanie naszych danych osobowych (imię, nazwisko, PESEL, imiona rodziców), potencjalnie może wyłudzić kredyt, czy dokonać innego oszustwa w naszym imieniu.

Chociaż kradzież tożsamości nie jest zjawiskiem nowym, wykorzystanie do tego celu przestrzeni wirtualnej upowszechniło to zjawisko. Działania przestępcze są szczególnie groźne nie tylko dla bezpośrednich ofiar, ale również dla samej gospodarki. Uzyskanie dostępu na przykład do danych posiadaczy rachunków bankowych powoduje zachwianie zaufania do handlu elektronicznego, elektronicznych instrumentów płatniczych i szeregu innych usług związanych z obrotem w cyberprzestrzeni[879].

Kradzież tożsamości nie jest tematem jednolitym, ponieważ działanie przestępcze może przyjąć wiele różnorakich zachowań. Znawcy tematu wyliczają, że kradzież tożsamości może polegać na przywłaszczeniu:

1. „informacji biometrycznych (ang. *biometric identity*), obejmujące odciski palców, głos, profil DNA, itp.,
2. nadanej tożsamości (ang. *attributed identity*), obejmujące unikalne dane nadawane człowiekowi wraz z urodzeniem (np. imię i nazwisko, dzień i data urodzenia, imiona rodziców, adres itp.)
3. biograficznej tożsamości (ang. *biographical identity*), obejmującej te aspekty ludzkiej tożsamości, które są nabyte przez nią z biegiem czasu (np. historia zatrudnienia, prawo jazdy, paszport, rachunki bankowe itp.)"[880].

Marco Gercke w opracowanym w ramach projektu Rady Europy dokumencie *Project on cybercrime*[881] stwierdził, iż kradzież tożsamości może odbyć się zarówno bez wykorzystania żadnych dodatkowych środków technicznych, ale również za pomocą

[878] A. Lach, *Kradzież* ..., s. 29-30.
[879] Ibidem, s. 30.
[880] M. Siwicki, *Cyberprzestępczość*…, s. 285.
[881] M. Gercke, *Internet - related identity theft*, Strasburg, 2007, tekst w języku angielskim dostępny na: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf [21.05.2014].

technologii informatycznych. Metody działania cyberprzestępców mogą być rozmaite, lecz można je zakwalifikować w pięć podstawowych grup:

1. Metody fizyczne (ang. *physical methods*) - polegają na kradzieży urządzeń pamięci (telefony komórkowe, laptopy, pendrive'y), przeszukiwaniu śmieci (ang. *dumpster diving*) lub poczty elektronicznej w celu uzyskania dostępu lub informacji do danych przydatnych przestępcy.
2. Wyszukiwarki internetowe (ang. *search engines*) - jest to wykorzystanie wyszukiwarek internetowych (Google czy Yahoo!) w celu uzyskania informacji przydatnych do kradzieży tożsamości innej osoby. Cyberprzestępcy za pomocą wskazanych serwisów internetowych znajdują informacje o systemach komputerowych chronionych hasłem lub specjalistycznym oprogramowaniu, w celu obejścia zabezpieczeń tych systemów. Zaznaczyć trzeba, iż oprogramowanie przeznaczone do indeksowania i wyszukiwania plików (ang. *file - sharing software*) jest używane nie tylko do znajdowania plików z muzyką czy filmami udostępnionymi na komputerze użytkownika - ale również do czynów przestępczych. Niejednokrotnie użytkownicy nieświadomie udostępniają dane zawierające informacje prywatne czy dane osobowe, które mogą być następnie wykorzystane przez cyberprzestępców.
3. Ataki wewnętrzne (ang. *insider attacks*) - są dokonywane przez pracowników firmy lub osoby wykonujące prace zlecone, którzy kradną dokumenty i dane poufne oraz informacje zastrzeżone.
4. Ataki zewnętrzne (ang. *attacks form the outside*) - sprawca tego typu ataku przez ominięcie zabezpieczeń włamuje się do systemu w celu nieuprawnionego uzyskania informacji. Włamań dokonuje się za pomocą oprogramowania szpiegowskiego, robaków i wirusów komputerowych.
5. Wykorzystanie socjotechniki w celu uzyskania informacji niezbędnych do kradzieży tożsamości (ang. *social engineering regarding the disclosure of identity - related information*) - sprawcy wykorzystując socjotechnikę, nazywaną również inżynierią społeczną w celu przekonania ofiary do dobrowolnego ujawnienia danych[882].

[882] Ibidem,

W lutym 2012 roku przestępcy posłużyli się wizerunkiem firmy Magellan Pertoleum Corporation[883] przesyłając do polskich internautów spam zamieszczonej na rysunku 8.

Rysunek 8. Przykładowy e-mail nakłaniający do udostępniania danych osobowych

Szanowni Panstwo!
Wydzial Magellan Petroleum Corporation, duzej miedzynarodowej firmy, przyjmuje aplikacje na stanowisko w swoim dziale Kontroli Kredytowej dla Europy Wschodniej. Obecnie potrzebujemy pracownikow w terenie, poniewaz nasz wydzial rozprowadza produkty firmy w krajach europejskich.

Dzieki poprawie koniunktury po kryzysie ekonomicznym co raz wiecej duzych firm zatrudnia pracownikow do pracy zdalnej. Praca zdalna w znaczacym stopniu obniza koszty utrzymania przestrzeni biurowej w budzecie firmy, a pracownicy nie maja potrzeby codziennego dojazdu do biura. W nowoczesnym swiecie technologii informacyjnej jest to ekonomiczne rozwiazanie, ktore uwalnia fundusze dla wzrostu firmy i pozwala na godziwe wynagradzanie pracownikow.

Obecnie poszukujemy agentow terenowych, ktorych zadaniem bedzie kontrola platnosci pomiedzy nasza firma a klientami w krajach europejskich, ktore nie sa czlonkami strefy euro. Potrzeba ta wynikla z faktu, ze realizacja przelewow internetowych zajmuje duzo czasu i nie posiadaja one wystarczajacego poziomu zabezpieczen przed kradzieza naszych funduszy. Z tego powodu kontrolujemy oplaty za pomoca agentow. Do obowiazkow agenta nalezy wykonywanie przelewow bankowych oraz dokonywanie biezacych przelewow srodkow za pomoca miedzynarodowych systemow platnosci. Plan pracy agenta musi byc wystarczajaco elastyczny, aby umozliwic mu kontrole srodkow przychodzacych na konto w ciagu dnia. Agent musi rowniez posiadac zdolnosc szybkiego finalizowania transakcji.
Nasza firma oferuje pracownikom satysfakcjonujace wynagrodzenie oraz zabezpieczenie spoleczne.

Jesli jestescie Panstwo zainteresowani podjeciem pracy na tym stanowisku, prosimy o wyslanie krotkiego CV na nasz adres e-mail:magellan.petroleum@gmx.com

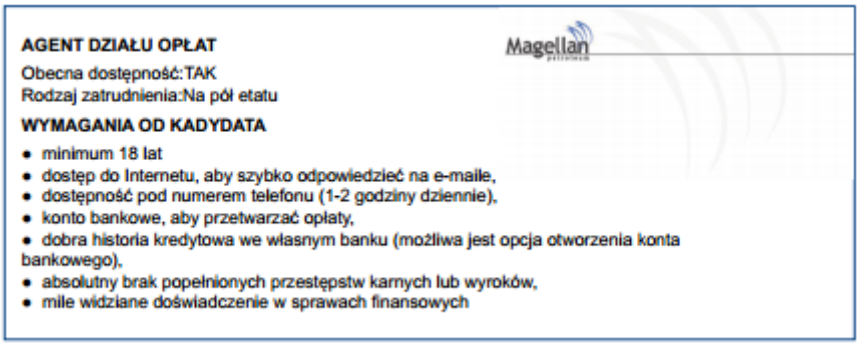
Nasz menedzer skontaktuje sie z Panstwem.

Źródło: *Raport CERT Polska z 2012 Analiza incydentów naruszających bezpieczeństwo teleinformatyczne*, s. 34.

Kontakt z cyberprzestępcami nieświadomi użytkownicy mogli uzyskać przez odpowiedź pod adresem znajdującym sie w treści wiadomości. Po otrzymaniu takiej wiadomości ofiara otrzymywała szczegółowy opis stanowiska (rysunek 9, 10) oraz formularz zgłoszeniowy (rysunek 11), w którym musiała podać swoje szczegółowe dane osobowe. Wypełnione dokumenty należało odesłać na podany adres e-mail.

[883] Analiza incydentów naruszających bezpieczeństwo teleinformatyczne. Raport CERT Polska z 2012, s. 34 - 36.

Rysunek 9. Opis stanowiska pracy - wymagania



AGENT DZIAŁU OPŁAT

Magellan

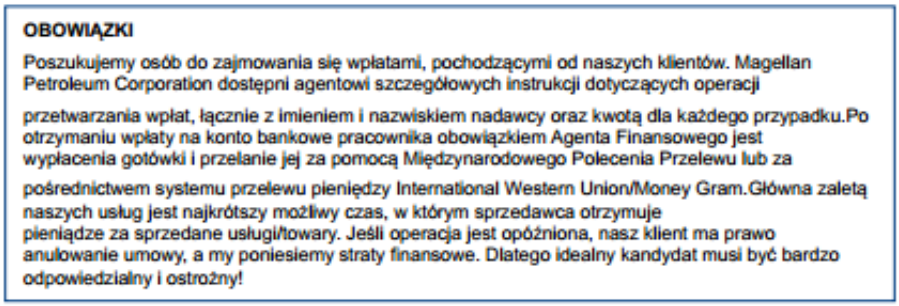
Obecna dostępność:TAK
Rodzaj zatrudnienia:Na pół etatu

WYMAGANIA OD KADYDATA

- minimum 18 lat
- dostęp do Internetu, aby szybko odpowiedzieć na e-maile,
- dostępność pod numerem telefonu (1-2 godziny dziennie),
- konto bankowe, aby przetwarzać opłaty,
- dobra historia kredytowa we własnym banku (możliwa jest opcja otworzenia konta bankowego),
- absolutny brak popełnionych przestępstw karnych lub wyroków,
- mile widziane doświadczenie w sprawach finansowych

Źródło: *Raport CERT Polska z 2012 Analiza incydentów naruszających bezpieczeństwo teleinformatyczne*, s. 35.

Rysunek 10. Opis stanowiska pracy - zakres obowiązków



OBOWIĄZKI

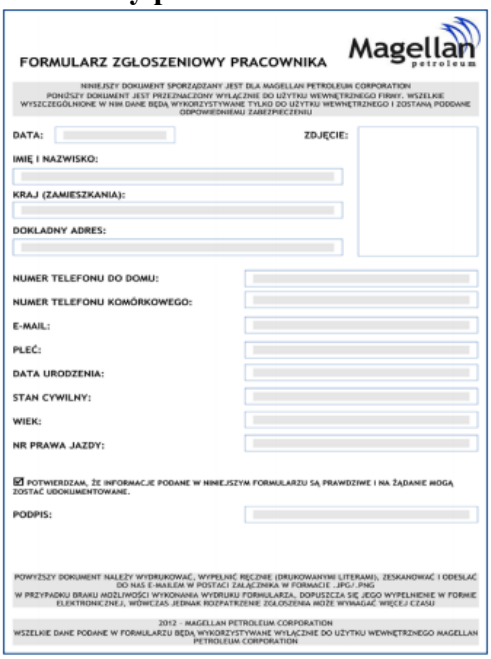
Poszukujemy osób do zajmowania się wpłatami, pochodzącymi od naszych klientów. Magellan Petroleum Corporation dostępni agentowi szczegółowych instrukcji dotyczących operacji

przetwarzania wpłat, łącznie z imieniem i nazwiskiem nadawcy oraz kwotą dla każdego przypadku.Po otrzymaniu wpłaty na konto bankowe pracownika obowiązkiem Agenta Finansowego jest wypłacenia gotówki i przelanie jej za pomocą Międzynarodowego Polecenia Przelewu lub za

pośrednictwem systemu przelewu pieniędzy International Western Union/Money Gram.Główna zaletą naszych usług jest najkrótszy możliwy czas, w którym sprzedawca otrzymuje pieniądze za sprzedane usługi/towary. Jeśli operacja jest opóźniona, nasz klient ma prawo anulowanie umowy, a my poniesiemy straty finansowe. Dlatego idealny kandydat musi być bardzo odpowiedzialny i ostrożny!

Źródło: *Raport CERT Polska z 2012. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne,* s. 35.

Rysunek 11. Formularz zgłoszeniowy pracownika



FORMULARZ ZGŁOSZENIOWY PRACOWNIKA

Magellan petroleum

NINIEJSZY DOKUMENT SPORZĄDZANY JEST DLA MAGELLAN PETROLEUM CORPORATION
PONIŻSZY DOKUMENT JEST PRZEZNACZONY WYŁĄCZNIE DO UŻYTKU WEWNĘTRZNEGO FIRMY. WSZELKIE WYSZCZEGÓLNIONE W NIM DANE BĘDĄ WYKORZYSTYWANE TYLKO DO UŻYTKU WEWNĘTRZNEGO I ZOSTANĄ PODDANE ODPOWIEDNIEMU ZABEZPIECZENIU

DATA: ZDJĘCIE:

IMIĘ I NAZWISKO:

KRAJ (ZAMIESZKANIA):

DOKŁADNY ADRES:

NUMER TELEFONU DO DOMU:

NUMER TELEFONU KOMÓRKOWEGO:

E-MAIL:

PŁEĆ:

DATA URODZENIA:

STAN CYWILNY:

WIEK:

NR PRAWA JAZDY:

☑ POTWIERDZAM, ŻE INFORMACJE PODANE W NINIEJSZYM FORMULARZU SĄ PRAWDZIWE I NA ŻĄDANIE MOGĄ ZOSTAĆ UDOKUMENTOWANE.

PODPIS:

POWYŻSZY DOKUMENT NALEŻY WYDRUKOWAĆ, WYPEŁNIĆ RĘCZNIE (DRUKOWANYMI LITERAMI), ZESKANOWAĆ I ODESŁAĆ DO NAS E-MAILEM W POSTACI ZAŁĄCZNIKA W FORMACIE .JPG/.PNG
W PRZYPADKU BRAKU MOŻLIWOŚCI WYKONANIA WYDRUKU FORMULARZA, DOPUSZCZA SIĘ JEGO WYPEŁNIENIE W FORMIE ELEKTRONICZNEJ, WÓWCZAS JEDNAK ROZPATRZENIE ZGŁOSZENIA MOŻE WYMAGAĆ WIĘCEJ CZASU

2012 - MAGELLAN PETROLEUM CORPORATION
WSZELKIE DANE PODANE W FORMULARZU BĘDĄ WYKORZYSTYWANE WYŁĄCZNIE DO UŻYTKU WEWNĘTRZNEGO MAGELLAN PETROLEUM CORPORATION

Źródło: *Raport CERT Polska z 2012.Analiza incydentów naruszających bezpieczeństwo teleinformatyczne*, s. 36.

Niejednokrotnie zdarzało się, iż ofiary były proszone o podanie numeru telefonu oraz adresu zamieszkania członka rodziny lub przesłania zeskanowanej kopii paszportu, dowodu tożsamości lub prawa jazdy. Po pomyślnym przejściu całego etapu „rekrutacji" ofierze była przesyłana do podpisania umowa na okres próby, zawierająca szczegółowe zasady wynagrodzenia podpisana przez „Dyrektora" i opatrzona firmową pieczęcią (rysunek 12).

Rysunek 12. Fragment umowy zawierający podpis dyrektora i pieczątkę

14. Istotne dane i podpisy Stron

Na dowód czego niżej podpisani zawarli niniejszą Umowę w dniu i w roku podanym powyżej.

Niniejsza Umowa, jak również wszystkie suplementy, zmiany i załączniki do niniejszej Umowy potwierdzone drogą faksową, pozostają w mocy.

PRACOWNIK

Podpis osoby upoważnionej

Imię

Data

SPÓŁKA

Podpis osoby upoważnionej

Meco Owens, Dyrektor

Imię

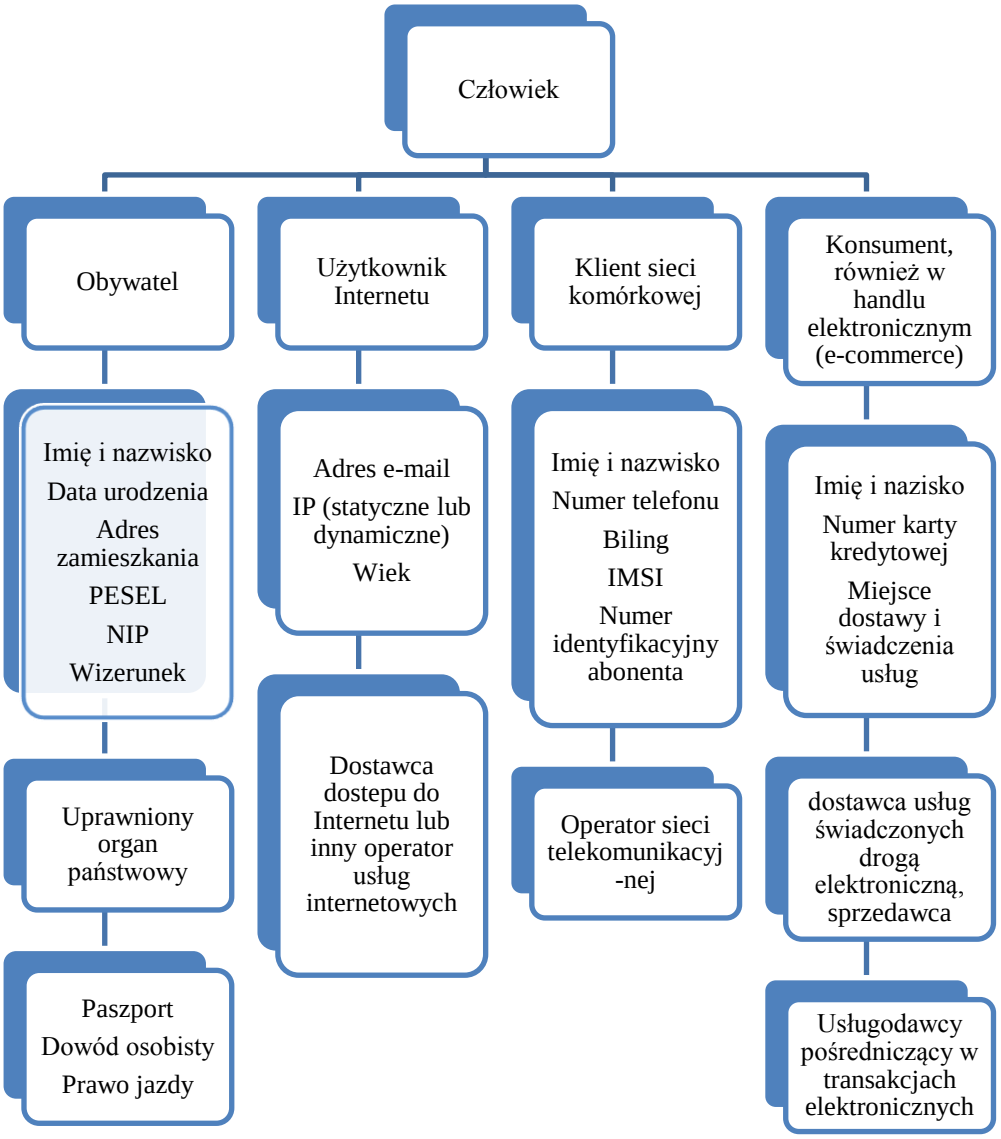
Źródło: *Raport CERT Polska z 2012Analiza incydentów naruszających bezpieczeństwo teleinformatyczne*, s. 36.

Korzystając z socjotechniki oraz żerując na chęci społeczeństwa do znalezienia łatwej i dobrze płatnej pracy cyberprzestępcy weszli w posiadanie setek bądź tysięcy danych

osobowych nieroztropnych internautów. Należy postawić sobie, pytanie jakie informacje i dane musi uzyskać przestępca, by móc mówić o kradzieży tożsamości. Bez wątpienia będą to dane osobowe rozumiane jako „zbiór jakichkolwiek informacji umożliwiających identyfikację osoby co do tożsamości”[884]. Będą to zatem imię i nazwisko, dane adresowe, PESEL, miejsce urodzenia, adres zamieszkania, ale również adres e-mail zawierający imię i nazwisko użytkownika poczty elektronicznej. Za informację potrzebne do identyfikacji osoby w cyberprzestrzeni można uznać login, hasło, kod dostępu lub kod PIN, które to dane umożliwiają uzyskanie dostępu do systemu komputerowego samodzielnie weryfikującego dane jego użytkowników[885].

[884] M. Siwicki, *Kradzież …*, s. 33.
[885] Ibidem, s. 33-34.

Rysunek 13. Informacje będące najczęściej przedmiotem wykonawczym przestępstwa kradzieży tożsamości



Źródło: M. Siwicki, *Kradzież tożsamości - pojęcie i charakterystyka zjawiska*, cz. 1 „Edukacja Prawnicza" 2009, nr 11, s. 34.

W komunikacie Komisji Wspólnot Europejskich W kierunku ogólnej strategii zwalczania cyberprzestępczości z 22 maja 2007 r.[886] podkreślono, że w ustawodawstwach państw członkowskich UE należy wprowadzić karalność czynu kradzieży tożsamości. Za

[886] COM(2007)267 final.

czyn taki uznano „wykorzystanie identyfikujących danych personalnych, np. numeru karty kredytowej, jako narzędzia do popełnienia innych przestępstw”[887].

Może zaistnieć sytuacja, że w wyniku wycieku danych osobowych (atak hackerów, omyłkowe udostępnienie danych) informacje o naszej osobie zostaną wykorzystane przez cyberprzestępców. W takiej sytuacji, gdy mamy podejrzenie, że mogło dojść do wycieku danych i kradzieży tożsamości to możemy sprawdzić, czy nasze dane nie zostały wykorzystane do zaciągnięcia kredytu. Istnieje szereg stron internetowych (np. Biuro Informacji Kredytowej), które umożliwiają sprawdzenie, czy i kiedy ktoś posługiwał się naszymi danymi do złożenia wniosku kredytowego, co więcej instytucje te oferują usługę smsowego alertu w przypadku złożenia zapytania kredytowego zawierającego nasze dane.

4.1.6 Cyberterroryzm

Pierwszy raz termin „cyberterroryzm” pojawił się w 1979 roku w raporcie szwedzkiego Ministerstwa Obrony omawiającym kwestię zagrożeń komputerowych. W latach osiemdziesiątych XX wieku pojęcie to znalazło się też w dokumentach wojskowych armii USA[888]. Rozwój badań nad zjawiskiem przypadł na lata dziewięćdziesiąte, kiedy pojawił się również termin „elektroniczny Pearl Harbor”. Określano nim apokaliptyczną wizję ataku na elektroniczną infrastrukturę krytyczną USA, czyli łączność, telekomunikację, system bankowy, który to atak miałby spowodować paraliż, uniemożliwienie normalnego funkcjonowania społeczeństwa oraz wielkie straty ekonomiczne[889].

Nie ma jednej, powszechnie przyjętej definicji cyberterroryzmu. Niejednokrotnie w literaturze przedmiotu zamiennie stosuje się pojęcia takie, jak: cyberwojna, cyberataki, zagrożenia w cyberprzestrzeni, cyberprzestępczość czy haktywizm. Leszek Wolaniuk definiuje cyberterroryzm, jako „połączenie cyberprzestrzeni z terroryzmem, gdzie cyberprzestrzeń to symboliczne, nieprawdziwe, binarne, metaforyczne przedstawienie

[887] Komunikat Komisji Wspólnot Europejskich W kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r., COM(2007)267.
[888] D. Jagiełło, *Cyberterroryzm*, „Edukacja Prawnicza” 2015, nr 5, s. 11.
[889] A. Podraza, *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku*, [w:] A. Podraza (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013, s. 27.

informacji, miejsce, gdzie działają programy komputerowe i gdzie znajdują się dane, zaś terroryzm to celowy, motywowany politycznie akt przemocy skierowany przez grupy subnarodowe lub tajnych agentów przeciwko celom niewalczącym"[890]. Inną definicję podała Dorothy Denning z Uniwersytetu Georgetown, która została powtórzona w oświadczeniu złożonym przed komisją Izby Reprezentantów USA 23 maja 2000 roku: „cyberterroryzm jest połączeniem terroryzmu i cyberprzestrzeni. Generalnie rozumie się, że oznacza on bezprawne ataki i groźby ataku komputerów, sieci i informacji tam zgromadzonych w celu zastraszenia lub zmuszenia rządu lub jego mieszkańców do realizacji celów politycznych lub społecznych. Ponadto, w celu zakwalifikowania, jako cyberterroryzm, atak powinien skutkować przemocą wobec osób lub majątku lub przynajmniej spowodować wystarczającą szkodę, aby wywołać strach. Przykładami mogą być ataki, które prowadzą do śmierci lub uszkodzenia ciała, eksplozji, katastrof samolotów, zanieczyszczenia wody lub dotkliwych strat gospodarczych w zależności od ich skutków. Do takich nie można zaliczyć ataków, które zakłócają nieistotne usługi lub powodują głównie kłopoty finansowe"[891]. Z kolei Mark Pollitt definiuje cyberterroryzm jako skryty, politycznie motywowany atak przeciwko informacjom, systemom lub programom komputerowym, bazom danych, którego efektem jest przemoc przeciwko celom niewojskowym, realizowanym przez grupy ponadnarodowe lub tajnych agentów[892]. Inni stwierdzają, że: „definicja cyberterroryzmu winna przewidywać występowanie dwóch płaszczyzn: odnosić się do ataków lub ich groźby na systemy i sieci teleinformatyczne, a przy tym nie pomijać ataków zmierzających do wykorzystania działalności organizacji (w tym także terrorystycznych). Postuluje by mianem cyberterroryzmu określać:

- politycznie lub militarnie motywowany atak albo groźbę ataku na systemy i sieci teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia infrastruktury krytycznej państwa oraz zastraszenie i wymuszenie na rządzie lub społeczności daleko idących polityczno - militarnych działań, a także,
- świadome wykorzystanie sieci teleinformatycznych oraz globalnej sieci Internet między innymi przez organizacje terrorystyczne, ruchy narodowo - wyzwoleńcze oraz ruchy powstańcze do propagandy, rekrutacji on-line, komunikowania się, mobilizacji,

[890] L. Wolaniuk, *Cyberterroryzm jako element cywilizacji informacyjnej*, [w:] M. Zuber (red.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i reagowanie kryzysowe*, Wrocław 2006, s. 157.
[891] D. Danning, *Testimony before the Special Oversight Panel on Terrorism. Committee on Armed Services*, U.S. House of Representatives, 23.05.2000, http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf [06.07.2015]. Tłumaczenie za: A. Podraza, op. cit., s. 30.
[892] M. Pollitt, *Cyberterrorism - Fact or Fancy?,* "Computer Fraud & Security", luty1998, s. 9.

zbierania informacji o potencjalnych celach ataku, planowania i koordynacji akcji oraz szeroko pojętej dezinformacji i walki psychologicznej"[893].

Z zagadnieniem cyberterroryzmu łączy się termin wojny sieciowej (ang. *net war*), która polega na „zakłócaniu bądź niszczeniu systemów informacyjnych przeciwnika oraz zdobywaniu jego danych strategicznych, takich jak środki walki i ich rozmieszczenie"[894]. W wojnie sieciowej ogromną rolę odgrywają hakerzy z dwóch walczących stron, którzy starają się niszczyć infrastrukturę sieci komputerowych przeciwnika. Określenie czy mamy do czynienia z cyberterroryzmem, czy z wojną internetową, gdzie wykorzystuje się podobne techniki i narzędzia walki, nie jest łatwe[895]. Nie każdy atak na strony rządowe będzie postrzegany jako działanie cyberterrorystyczne. Ataki hackerskiej grupy Anonymous ze stycznia 2012 roku na polskie strony rządowe był postrzegane nie jako akt cyberterroryzmu, lecz jako przejaw „cyberprotestu" wobec polityki państwa[896]. Podzielić należy pogląd, że: „Internet jest medium doskonale nadającym się do szerzenia strachu i propagandy oraz pozyskiwania wyznawców skrajnej ideologii czy werbowania nowych członków organizacji terrorystycznych, a przy tym doskonałym środkiem łączności w fazie planowania ataków"[897]. Cyberprzestrzeń umożliwia szybkie, tanie i (w teorii) anonimowe dotarcie do dużej rzeszy odbiorców. Z jednej strony pozwala na zastraszenie opinii publicznej, z drugiej pozyskania sławy i aprobaty osób wspierających terroryzm.

Należy zastanowić się dlaczego przestrzeń cyfrowa jest coraz częściej wykorzystywana przez terrorystów. Brunon Hołyst wymienia cechy sieci komputerowych, które wpływają na ich popularność wśród terrorystów:

- skrócenie czasu transmisji za pomocą Internetu, co umożliwia szybkie porozumiewanie się i koordynację zadań pomiędzy rozproszonymi grupami,
- znaczne zredukowanie kosztów komunikacji, co sprzyja rozwojowi zdecentralizowanych, rozproszonych grup terrorystycznych,
- zwiększenie zakresu i kompleksowości informacji[898].

[893] D. Jagiełło, op. cit., s 12.
[894] B. Hołyst, *Terroryzm*…, s. 960.
[895] Ibidem, s. 961.
[896] M. Czyżak, *Strategie zwalczania cyberterroryzmu - aspekty prawne*, [w:] A. Podraza (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013, s. 129.
[897] D. Jagiełło, op. cit., s 10.
[898] B. Hołyst, *Terroryzm*…, s. 953.

Irving Lachov i Countney Richardson rozszerzają wyżej wymieniony katalog o pięć wyróżniających cech, które powodują, iż terroryści wykorzystują Internet do swoich celów:

- Internet umożliwia szybką komunikację w czasie rzeczywistym,
- Internet jest tanim źródłem komunikacji, co powoduje, że terroryści mogą powielać funkcje współczesnych sił zbrojnych, organizacji rządowych i prywatnych, zbierać informacje wywiadowcze oraz prowadzić szkolenia dla swoich członków,
- wszechobecność Internetu powoduje, iż nawet małe grupy terrorystyczne mogą mieć globalny zasięg; terroryści mogą nie tylko komunikować się między sobą z każdego miejsca na świecie, ale także tworzyć strony internetowe, która mogą być oglądane przez miliony,
- wzrost przepustowości łączy i rozwój oprogramowania spowodował, że za pomocą Internetu terroryści mogą publikować i rozpowszechniać nawet skomplikowane informacje na przykład metodę skonstruowania bomby do samobójczego ataku,
- nowoczesne technologie szyfrowania umożliwiły terrorystom korzystanie z sieci, komunikowanie się oraz transfer środków pieniężnych niemalże anonimowo, co jest cechą szczególnie pożądaną przez grupy przestępcze[899].

Różne są cele, jakie terroryści mają zamiar osiągnąć za pomocą Internetu. W głównej mierze cyberprzestrzeń stanowi on dla nich medium wymiany informacji, chociażby o tym, w jaki sposób przygotować się do ataku czy też przygotować bombę domowej roboty. Z drugiej strony terroryści czują się w cyberprzestrzeni anonimowo, starają się prowadzić rekrutację nowych członków, zbierać fundusze, szerzyć swoje idee, ale też zastraszać społeczeństwo. Internetowe czaty, komunikatory, telekonferencje pozwalają na szybkie przesyłanie informacji, co oznacza większą mobilizację i elastyczność członków grup terrorystycznych. Różnorodne podejście przedstawicieli doktryny do kwestii celów, dla których terroryści wykorzystują przestrzeń wirtualną ukazuje tabela 13.

Tabela 13. Cele wykorzystywania Internetu przez terrorystów

Furnell & Warren (1999)	**Cohen (2002)**	**Thomas (2003)**	**Weimann (2004)**
– oddziaływanie na społeczeństwo i propaganda;	– planowanie; – finansowanie; – koordynacja	– profilowanie; – propaganda; – anonimowa, ukryta	– wojna psychologiczna; – oddziaływanie na

[899] I. Lachow, C. Richardson, *Terrorist use of the internet. The real story*, "Joint Force Quarterly" 2007, nr 45, s. 100-101.

– zdobywanie funduszy; – przekazywanie informacji; – bezpieczna komunikacja;	działań; – akcje polityczne; – propaganda;	komunikacja – wytwarzanie atmosfery strachu; – finansowanie; – *Command & Control;* – rekrutacja i mobilizacja; – pozyskiwanie informacji; – obniżenie ryzyka; – kradzież/ manipulacja danymi; – dezinformacja;	społeczeństwo i propaganda; – *data mining;* – zdobywanie funduszy; – rekrutacja i mobilizacja; – *Networking;* – wymiana informacji; – planowanie i koordynacja;

Źródło: J. Kosiński, *Działania terrorystyczne a cyberprzestępczość*, [w:] J. Szafrański, J. Kosiński, *Współczesne zagrożenia terrorystyczne oraz metody ich zwalczania. Materiały pokonferencyjne*, Szczytno 2007, s. 238.

Inną klasyfikację przedstawia Ernest Lichocki, wyróżniając nie tylko powody, dla których terroryści decydują się na atak w cyberprzestrzeni, ale również skutek, jaki wywołują na społeczność międzynarodową. Punktują słusznie, iż w przeciwieństwie do tradycyjnego terroryzmu każdy - z dostępem do komputera i Internetu - może stać się cyberterrorystą.

Tabela 14. Powody skłaniające terrorystów do ataków w cyberprzestrzeni

Powód terrorystycznego ataku w cyberprzestrzeni	**wpływ wywierany na bezpieczeństwo informacyjne**	**Identyfikacja zagrożeń**
Niskie koszty przeprowadzenia ataku	każdy może zostać cyberterrorystą. Wystarczy mieć komputer lub laptopa, odpowiedni program i trochę umiejętności	Infrastruktura krytyczna państwa: –sektor energetyczny; –system zaopatrzenia w wodę; –transport wodny, lądowy i powietrzny; –system i sieci teleinformatyczne; –łączność; –służby ratownicze; –zaopatrzenie w żywność; –bankowość i finanse;
Działania nad wyznaczonymi granicami państw	nie wiadomo, skąd pochodzi atak i kto za nim stoi	
Przewidywanie zagrożeń ataków	nie wiadomo, które zagrożenie jest realne, a które tylko pozorne	
Wykrycie i zlokalizowanie cyberataków	nie wiadomo, jakie są zdolności i intencje atakujących	
Cel ataku	nie wiadomo co będzie celem	

	ataku ani w jaki sposób będzie on dokonany	–urzędy państwowe; –przemysł istotny dla gospodarki; –narodowe pomniki i pamiątki.
Budowa koalicji	nie widomo, kto jest w koalicji, a kto jest nieprzyjacielem	

Źródło: E. Lichocki, *Cyberterroryzm państwowy i niepaństwowy - początki, skutki i formy*, [w:] M.J. Malinowski, *Ewolucja terroryzmu na przełomie XX i XXI wieku*, Gdańsk 2009, s. 162, opracowanie na podstawie: A. Bógdoł-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 88.

Należy podzielić pogląd Wojciecha Gizickiego, że wykorzystanie nowoczesnych technologii do działalności terrorystycznej potęguje dwie zasadnicze cechy terroryzmu. Po pierwsze, jest to wzbudzenie poczucia strachu w społeczeństwie - informacja o ataku lub groźbie ataku za pomocą cyberprzestrzeni jest w stanie w krótkim czasie dotrzeć do szerokiego grona odbiorców i tym samym w krótkim czasie wzbudzić strach lub poczucie zagrożenia w społeczeństwie. Z drugiej strony, mamy do czynienia ze zwiększeniem się stopnia zorganizowania grup terrorystycznych - za pomocą cyberprzestrzeni, terroryści są w stanie zdobyć niezbędne informacje, fundusze, zaplanować akcję terrorystyczną czy też komunikować się z pozostałymi członkami grupy[900].

Atak cyberterrorystyczny może mieć najróżniejszą siłę i charakter zamachu. Skutek ataku może być stosunkowo niewielki, na przykład przez zablokowanie informacyjnej strony rządowej. Jednakże najpoważniejszym w skutkach celem ataków może być infrastruktura krytyczna, której naruszenie może spowodować wielkie straty finansowe, a nawet osobowe oraz panikę społeczeństwa. Klasyfikacja ataków ze względu na umiejętności sprawców została wyszczególniona w 1999 roku w raporcie *Center for the Study of Terrorism and Irregular Warfare* w Kalifornii[901]:

- atak prosty nieskomplikowany (ang. *simple - unstructured*) - są to proste ataki hackerskie na indywidualne systemy informatyczne za pomocą urządzeń i programów stworzonych przez inną osobę,
- atak zaawansowany - strukturalny (ang. *advanced - structured*) - ataki o bardziej zaawansowanym charakterze na systemy złożone popełniane przy pomocy własnych narzędzi,

[900] W. Gizicki, *Państwo wobec cyberterroryzmu*, [w:] A. Podraza (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013, s. 47.
[901] White Paper. *Cyberterror: prospects and implemenations*, Center for the Study of Terrorism and Irregular Warfare, California, October 1999, s. 9, s. 13-17.

- atak kompleksowy - skoordynowany (ang. *complex - coordinated*) - sprawcy mają wiedzę i narzędzia do spowodowania całkowitego zniszczenia zintegrowanego systemu ochrony[902].

Nie można lekceważyć możliwości przeprowadzenia ataków cyberterrorystycznych. Oczywistym zagrożeniem jest atak na systemy infrastruktury państwa. Jednak scenariuszy ataku może być nieskończenie więcej. Przestępcy mogą zaatakować instytucje nie tylko państwowe, ale również prywatne firmy. Jako przykład można wymienić następujące przykłady zagrożeń: zmiana ciśnienia w ropociągach i gazociągach, co w konsekwencji będzie powodować wybuchy, zmiana receptur leków w skomputeryzowanych liniach produkcyjnych firm farmaceutycznych czy też sabotaż przepływu informacji na rynkach finansowych[903].

Brunon Hołyst w swych rozważaniach na temat terroryzmu podkreśla, iż cyberprzestrzeń jest wykorzystywana również do mobilizacji czasowej cyberterrorystów (ang. *parttime cyberterrorists*), czyli osób popierających, lecz niezwiązanych bezpośrednio i stale z grupami terrorystycznymi. Wzywa się ich wówczas do określonego zachowania się. Nie mniej istotna jest możliwość oddziaływania na systemy komputerowe i teleinformatyczne przeciwnika, przez używanie e-bomb, wirusów, robaków internetowych i włamań hakerów[904]. Jako przykład czasowej mobilizacji cyberterrorystów wskazać można apel imama Samudry z 2002 roku do młodych wyznawców islamu do prowadzenia dżihadu w cyberprzestrzeni przez atakowanie komputerów niewiernych i nielegalne wykorzystanie kart kredytowych co pozwoliłoby na prowadzenie i finansowanie walki z Zachodem[905].

Ataków cyberterrorystycznych nie należy kojarzyć wyłącznie z grupami terrorystycznymi. Mogą się ich dopuścić również inne podmioty, czyli państwa - wówczas atak cybernetyczny może być działaniem szpiegowskim lub też elementem prowadzonej wojny, prowadzącym do dezinformacji przeciwnika. Państwa przed inwazją lądową mogą dopuścić się ataków cyberterrorystycznych na urządzenia infrastruktury krytycznej, serwery państwowe lub wojskowe przeciwnika. Mimo, iż sprawcy cyberataków niejednokrotnie pozostają anonimowi, to często uważa się, że stoją za nimi państwa: Chiny, Korea Północna, Rosja, Indie czy Izrael. Przykładem takich działań może być zaatakowanie w 2008 roku za

[902] A. Podraza, op. cit., s. 38.
[903] E. Lichocki, op. cit., s. 161.
[904] B. Hołyst, *Terroryzm*…, s. 955-956.
[905] A. Podraza, op. cit., s. 33.

pomocą ataku DDoS serwerów publicznych Gruzji: stron www prezydenta, Ministerstwa Spraw Zagranicznych, Narodowego Banku Republiki Gruzji, banków komercyjnych i mass mediów. Atak zbiegł się z konfliktem zbrojnym pomiędzy Rosją a Gruzją o separatystyczną enklawę Osetii Południowej. Niewiadomo dokładnie, kto dopuścił się ataków, lecz przyjmując, iż doszło do nich na zlecenie Rosji to było to pierwsze użycie cyberprzestrzeni do pomocy w zdobyciu przewagi w konflikcie zbrojnym[906]. Sprawcami cyberataków mogą być również zorganizowane grupy (ruchy narodowowyzwoleńcze, podmioty gospodarcze operujące w sieciach teleinformatycznych) bądź też pojedynczy sprawcy (hakerzy, aktywiści, crakerzy, frustraci, szpiedzy, wandale), którzy chcą sprawdzić swoje umiejętności włamując się do wysoce strzeżonych systemów[907].

Ernest Lichocki dzieli cyberterroryzm na cyberterroryzm państwowy i cyberterroryzm niepaństwowy. Do pierwszego z wymienionych zalicza: walkę informacyjną, walkę z terroryzmem i organizacjami terrorystycznymi, walkę ze zorganizowaną przestępczością, w tym z handlarzami narkotyków oraz działalność resortów siłowych państwa (służb ochrony państwa). Do cyberterroryzmu niepaństwowego zaliczył: wandali, hakerów, crackerów, aktywistów, haktywistów, szpiegów, frustratów, działalność organizacji terrorystycznych oraz działalności ruchów narodowowyzwoleńczych[908].

Osma Bin Laden, prowadząc „świętą wojnę" przeciwko Stanom Zjednoczonym i całemu Zachodowi wykorzystywał najnowszą technologię do działań o charakterze terrorystycznym. Przebywając w górskiej kwaterze w Afganistanie i dysponując nowoczesnym sprzętem komputerowym, sprzętem telekomunikacyjnym oraz telefonią satelitarną koordynował działalność podlegających mu rozproszonych grup terrorystycznych. Członkowie Al- Kaidy otrzymywali na płytach CD informacje o produkcji bomb, ciężkiej broni, rekrutacji nowych członków. Z kolei Hamas używał programów kodujących, czatów oraz poczty e-mail do przesyłania informacji o atakach terrorystycznych. Terroryści posługują się też steganografią, która jest metodą ukrywania tajnych informacji w innych danych (również plikach graficznych), czy też kodowaniem transmisji telefonów komórkowych, kradzieżą tych numerów, a następnie wprowadzaniem do nich odpowiednich programów

[906] Ibidem, s. 38-39.
[907] E. Lichocki, op. cit., s. 161.
[908] Ibidem, s. 167.

umożliwiających terrorystom komunikowanie sie za pomocą zhakowanych telefonów z każdego miejsca na ziemi[909].

Cyberterroryzm i zagrożenia z nim związane mają charakter asymetryczny i ponadnarodowy. Przeciwdziałanie zjawisku nie jest zagadnieniem prostym, ponieważ należy prowadzić działania systemowe na wielu płaszczyznach. Istnieje wiele powodów, dla których przeciwdziałanie cybertrroryzmowi napotyka wiele przeszkód. Zaliczyć do nich należy: niepaństwowy charakter, niebezpośredniość ataku, prowadzenie ataku na odległość, możliwość rozłożenia go w czasie, łatwość przeprowadzenia ataku, konieczność nieustannego dopracowywania rozwiązań formalnoprawnych służących przeciwdziałaniu cyberterroryzmowi[910]. Aktów cyberterroryzmu można dokonać stosunkowo niskim kosztem, wystarczy laptop i dostęp do Internetu. Korzystanie przez terrorystów z elektronicznych kanałów porozumiewania sie na odległość może dawać wrażenie anonimowości i niemożności ich wykrycia. Jest to jednak mylne przekonanie. Niemalże każda działalność w sieci pozostawia po sobie cyfrowy „ślad". Służby wywiadowcze państw stale przeprowadzają działania w celu zbierania takich dowodów, wykrywania sprawców i zapobieganiu atakom.

Cyberterroryzm zaliczyć należy do jednego z zagrożeń hybrydowych państwa, którego celem jest nie tylko spowodowanie bezpośrednich szkód i wykorzystanie słabości, ale również destabilizacja społeczeństwa. Zagrożenie to jest coraz bardziej realne. W ostatnich latach ISIS intensywnie publikuje filmiki propagandowe dokumentujące brutalne ataki, wychwalające sukcesy oraz nawołujące do dżihadu. Terroryści zrozumieli, że przestrzeń wirtualna ma gigantyczny wpływ na opinię publiczną, a treści publikowane w Internecie, mogą być dodatkowym narzędziem terroru.

4.2 Obrót gospodarczy w cyberprzestrzeni a prawo międzynarodowe

Za pośrednictwem cyberprzestrzeni zawieranych jest coraz więcej umów, w tym tych zawierających czynnik transgraniczny i transnarodowy. Świat, rynek handlowy, zmniejszyły

[909] B. Hołyst, *Terroryzm*…, s. 954.
[910] W. Gizicki, op. cit., s. 50-51.

się do rozmiarów globalnej wioski. Siedząc przed ekranem naszego komputera, tabletu czy telefonu możemy zrobić zakupy *on-line* w USA, uczestniczyć w internetowym kursie w Japonii, kupić bilety lotnicze czy uzyskać dostęp do najnowszych orzeczeń opublikowanych w Lex-ie. Techniczny rozwój narzędzi informatycznych, wprowadzenie nowych metod, narzędzi i procedur porozumiewania się na odległość doprowadziło do wykształcenia się w społeczeństwie informacyjnym elektronicznego obrotu prawnego - handlu elektronicznego, nazywanego również e-commerce.

Wobec braku ogólnie akceptowalnej definicji pojęcia handlu elektronicznego Wojciech J. Kocot uznał, że jest to reklama, sprzedaż i dystrybucja towarów za pomocą sieci teleinformatycznej, w szczególności za pomocą Internetu[911]. Aernout Schmidt i Han Franken uważają, że za e-commerce można uznać formy handlu umożliwione przez elektroniczną komunikację (jak sieć wirtualna), przetwarzanie i procesy, określane czasami jako inteligentne[912]. OECD wyszczególniło dwa rodzaje handlu elektronicznego: w rozumieniu szerokim (jako ogół stosunków wymiany towarów i usług drogą elektroniczną) oraz w znaczeniu wąskim (transakcje dokonywane wyłącznie w Internecie)[913]. Z kolei UNCITRAL za e-commerce uznaje „wszelkie transakcje w handlu międzynarodowym, które są dokonywane za pomocą wymiany danych elektronicznych bądź innych środków komunikacji, niewymagających użycia papieru"[914]. Przemysław Polański uznaje, że w praktyce mamy do czynienia z europejskim prawem handlu elektronicznego *sensu stricto* i *sensu largo*. Za europejskie prawo handlu elektronicznego *sensu stricto* uznaje on przepisy dyrektywy o handlu elektronicznym, a e-commerce *sensu largo* to przepisy Unii Europejskiej poruszające kwestię własności intelektualnej, ochrony prywatności, ale też przepisy dotyczące cyberprzestępczości czy elektronicznych płatności[915].

Z raportu „*The 2015 Global Retail E-Commerce Index*" opublikowanego przez międzynarodową agencję consultingową A. T. Kearney wynika, że wartość światowego handlu elektronicznego została oszacowana w 2015 roku na 994,5 miliarda dolarów. Roczna dynamika rozwoju *e-commerce* w 2015 roku dynamika wynosiła 18,4%. Na koniec 2014 roku

[911] W.J. Kocot, *Wpływ Internetu na prawo umów*, Warszawa 2004, s. 27.
[912] A. Schmidt, H. Franken, *Law as code*, [w:] H. Snijders, S. Weatherill (red.), *E-commerce law. National and Transnational Topics and Perspectives code as law - general remarks on legal requirements engineering*, Haga 2003, s. 117.
[913] W.J. Kocot, op. cit., s. 27.
[914] UNCITRAL „Model Law on Electronic Commerce", United Nations, New York 1997, http://www.uncitral.org/uncitral/index.html, za: K. Kowalik-Bańczyk, op. cit., s. 39-40.
[915] P.P. Polański, *Europejskie …*, s. 43-44.

światowy handel elektroniczny wyceniany był na 839,8 miliarda dolarów, a dynamika wzrostu w stosunku do 2013 roku wyniosła 20,8%. Na 2016 rok A. T. Kearney prognozował dynamikę globalnego e-commerce na poziomie 16,1% z obrotami w wysokości 1,155 biliona dolarów[916]. Z kolei polski rynek e-commerce w raporcie E-commerce w Polsce 2015. Gemius dla e-Commerce został wyceniony na 27 milionów złotych[917]. W rozwoju branży determinantem okazują się być płatności *on-line* oraz płatności mobilne. Dotychczasowy model funkcjonowania społeczeństwa i gospodarki zmienia się wraz z rosnącą popularnością usług internetowych, ponieważ handel wszedł w nowy wymiar - zakupów, usług i płatności *on-line*.

Jacek Janowski jako obrót rozumie „obieg, wymianę, przesunięcie, przejście lub przekazanie świadczeń lub oświadczeń pomiędzy różnorodnymi podmiotami, stronami, uczestnikami czy kontrahentami. Przedmiotem tak pojętego obrotu są byty realne (rzeczy), stany prawne (prawa - zespoły uprawnień i obowiązków) oraz tak zwane dobra informacyjne (produkty digitalne)"[918]. Autor uznał, że możemy mówić o obrocie prawnym (w znaczeniu wymiany prawnie doniosłych czynności i działań), obrocie gospodarczym (przesunięciu składników majątku pomiędzy stronami stosunku prawnego) oraz o obrocie elektronicznym (rozumianym jako każda faktyczna i formalna wymiana realizowana elektronicznie)[919].

W ocenie Jacka Jankowskiego elektroniczny obrót prawny to „wymiana prawna i komunikacja elektroniczna zarazem jako całokształt czynności prawnych i czynności urzędowych, dokonywanych w postaci elektronicznej, tj. z zastosowaniem elektronicznych nośników informacji oraz środków komunikacji elektronicznej. Wykorzystuje on elektroniczną, a zwłaszcza cyfrową postać dokumentu oraz elektroniczną, a zwłaszcza sieciową wymianę informacji, do wyrażenia i składania oświadczeń woli i wiedzy, wywołującą dla ich nadawców i odbiorców skutki prawne. Nośnikiem, w zależności od medium, elektronicznego obrotu prawnego są dane w postaci elektronicznej, kwalifikowane jako: elektroniczne oświadczenia woli, elektroniczne umowy, elektroniczne płatności, elektroniczne podpisy lub elektroniczne dowody"[920]. W niniejszym opracowaniu zostaną

[916] Raport The 2015 Global Retail E-Commerce Index, dostępny *on-line*: https://www.atkearney.com/documents/10192/5691153/Global+Retail+E-Commerce+Keeps+On+Clicking.pdf/abe38776-2669-47ba-9387-5d1653e40409 [27.06.2016.].
[917] Raport „E-commerce w Polsce 2015. Gemius dla e-Commerce", https://www.gemius.pl/files/reports/E-commerce-w-Polsce-2015.pdf [27.06.2016].
[918] J. Janowski, *Kontrakty elektroniczne w obrocie prawnym*, Warszawa 2008, s. 23.
[919] Ibidem, s. 23.
[920] Ibidem, s. 38.

opisane wyłącznie najważniejsze kwestie związane z obrotem gospodarczym w przestrzeni wirtualnej, czyli umowy elektroniczne oraz elektroniczne środki płatnicze. Inne kwestie takie, jak delikty elektroniczne, szczegółowe aspekty świadczenia usług elektronicznych czy niedozwolone klauzule umowne, pozostawiono bez omówienia.

Elektroniczny obrót prawny ma kilka cech - jest on umowny (kontraktowy) i pozaumowny (pozakontraktowy), jednostronny, dwustronny i wielostronny, wzajemny i niewzajemny, odpłatny i nieodpłatny, dokonywany w jednym miejscu lub na odległość. Mimo wyliczenia wszystkich wymienionych elementów, elektroniczny obrót prawny, posiada swoją własną specyfikę, jest on dwustronny, umowny, odpłatny i dokonany na odległość, wobec czego znawcy doktryny wymieniają zasadnicze podstawowe cechy sieciowego i internetowego kontraktowego obrotu elektronicznego:

- nieograniczony zakres wykorzystania cyberprzestrzeni w działalności osobistej, zawodowej, aktywności publicznej i prywatnej,
- swoboda składania i wyrażania oświadczeń woli,
- wysokie ryzyko związane z bezpieczeństwem informacji, przechwycenia i modyfikowania danych,
- anonimowość, znacznie utrudnia identyfikację stron, co wiąże się z ryzykiem ukrycia lub zmiany tożsamości,
- możliwość awarii transmisji danych,
- mobilność umożliwiająca podejmowanie działań z każdego miejsca na ziemi,
- szybkość wymiany informacji,
- szybkie zmiany technologiczne wymuszające ciągłą naukę zmian przez użytkowników cyberprzestrzeni,
- automatyzacja, posługiwanie i tworzenie coraz inteligentniejszego oprogramowania,
- ogólna dostępność, zmniejszenie się kosztów dostępu do cyberprzestrzeni,
- dynamiczna infrastruktura ukierunkowana na zwiększenie efektywności, bezpieczeństwa, niezawodności i przydatności[921].

Powodów tak dynamicznego rozwoju obrotu elektronicznego można upatrywać w kilku czynnikach. Brak granic państwowych i geograficznych doprowadził do powstania wirtualnego rynku o niewyobrażalnych rozmiarach i możliwościach. Na wzrost popularności handlu elektronicznego wpłynęła oszczędność czasu, całodobowa dostępność towarów i

[921] Ibidem, s. 32 - 34.

usług, korzystniejsze ceny oraz bardziej urozmaicona oferta obejmująca też towary trudnodostępne[922]. W przeciwieństwie do handlu tradycyjnego nie ma ograniczenia wąską ofertą lokalnego przedsiębiorcy i zawyżoną ceną uwzględniającą jego marżę. Negatywnym czynnikiem jest jednak brak możliwości wcześniejszego sprawdzenia jakości przedmiotu. Zakupy *on-line* często kończą się rozczarowaniem wynikającym z niezgodności towaru z internetowym opisem.

Przedsiębiorcy, ale również konsumenci coraz chętniej zawierają transakcje za pośrednictwem sieci wirtualnej. W ciągu zaledwie kilku lat powstały internetowe giganty świadczące usługi milionowej rzeszy użytkowników. Wymienić chociażby należy serwisy takie, jak Google, Facebook czy Amazon. Obrót gospodarczy w cyberprzestrzeni jest wart dziś miliardy euro, a jednym z jego najbardziej podstawowych zagadnień jest kwestia elektronicznego obrotu kontraktowego. W niniejszym opracowaniu zostanie omówiona podstawowa problematyka cywilnoprawna, z pominięciem między innymi zagadnień związanych z wadami oświadczeń woli w cyberprzestrzeni.

4.2.1 Zawieranie umów w cyberprzestrzeni

Możliwość swobodnego porozumiewania się na odległość za pomocą Internetu rewolucyjnie wpłynęła na obrót gospodarczy umożliwiając, nieznaną dotąd na tak wielką skalę, swobodę kontraktowania. Użytkownicy sieci dostali interaktywną przestrzeń umożliwiającą im zawarcie umowy niezależnie od granic, miejsca położenia stron czy obowiązującego prawa. Wojciech J. Kocot wyraził pogląd, że: „będąc powszechnie dostępnym i niezależnym medium, Internet tworzy najbardziej przyjazną przestrzeń dla stosowania regulacji cywilnoprawnej, z natury pluralistycznej, opartej na dialogu, autonomii podmiotów i swobodzie wyrażania woli. Umożliwiając nieskrępowany obrót umowny, Internet stał się głównym czynnikiem sprzyjającym rozwojowi stosunków kontraktowych”[923]. W cyberprzestrzeni znajdują się miliony ofert, uwzględniających nasze wymagania cenowe, jakościowe i ilościowe. Nie sposób jest zatem nie zgodzić się z przedstawioną opinią

[922] W.J. Kocot, op. cit., s. 27.
[923] Ibidem, s. 10.

zwłaszcza, jeżeli uwzględni się, że tylko w Polsce w 2015 roku wartość handlu internetowego wyniosła 27 miliardów złotych[924].

Swoboda kontraktowania wiąże się nieodłącznie ze swobodą wyboru statutu jurysdykcyjnego zarówno w międzynarodowym, jak i krajowym obrocie handlowym. Strony, zarówno w obrocie dwustronnie profesjonalnym, jak i w stosunkach z konsumentami mają prawo wyboru prawa właściwego do zawarcia, stosowania, wykładni i ewentualnych sporów, jakie mogą wyniknąć ze stosowania umowy. Umowy elektroniczne ułatwiły obrót gospodarczy i przyczyniły się do rozszerzenia rynków zbytu przedsiębiorców nie tylko na inne regiony kraju, ale również inne państwa. Mimo oczywistych korzyści zawieranie umów za pomocą Internetu zwiększyło ryzyko prowadzenia międzynarodowych sporów z powodu multijurysdykcyjności przestrzeni cyfrowej, czyli możliwości podlegania pod właściwość kilku zupełnie różnych sądów, również sądu kilku państw[925].

Wobec braku procesowych rozwiązań kolizyjnych w odniesieniu do kontraktów elektronicznych w doktrynie postuluje się stosowanie najbardziej pewnego i jednoznacznego rozwiązania, jakim jest właśnie wybór prawa właściwego. Wojciech J. Kocot formułuje następujący wniosek: „Mając na uwadze trudności związane z procesem unifikacji prawa prywatnego międzynarodowego, należy w chwili obecnej postulować jak najszersze upowszechnienie w obrocie elektronicznym stosowanie łącznika subiektywnego, którym jest wybór prawa (*lex voluntatis*)”[926]. Również Marek Świerczyński jest zwolennikiem wyboru prawa podkreślając, że „wybór prawa właściwego nie wymaga zachowania szczególnej formy (...). Brak zatem przeszkód dla zawarcia takiej umowy przy wykorzystaniu dowolnych środków komunikacji elektronicznej (brak nawet wymogu trwałego zapisu, aczkolwiek może on być używany ze względów dowodowych). Nie ma więc konieczności stosowania kwalifikowanych (zaawansowanych) podpisów elektronicznych weryfikowanych za pomocą certyfikatów kwalifikowanych (...). Internet wykształcił własne (tańsze) sposoby uwierzytelniania uczestników obrotu, które są w pełni wystarczające (bankowość internetowa, serwisy społecznościowe, systemy płatnicze)”[927]. Zaprezentowane stanowiska, mimo że zostały wyrażone ponad dekadę temu, wciąż pozostają aktualne i zasługują na aprobatę. Wybór prawa właściwego przez strony umowy jest zgodny z swobodą kontraktowania, ale

[924] Raport Gemius E-commerce w Polsce, https://www.gemius.pl/files/reports/E-commerce-w-Polsce-2015.pdf [21.06.2016].
[925] W.J. Kocot, op. cit., s. 403.
[926] Ibidem, s. 383.
[927] M. Świerczyński, *Internet a nowe prawno prywatne międzynarodowe*, [w:] G. Szpor, W.R. Wiewiórski (red.), *Internet. Prawno - informatyczne problemy sieci, portali i e-usług*, Warszawa 2012, s. 48.

również z zasadą autonomii cyberprzestrzeni, gdzie strony mogą samodzielnie kształtować swoje relacje z innymi podmiotami. Zawarcie klauzuli jurysdykcyjnej eliminuje niepewność prawną, ponieważ strony już od początku związania się umową mają świadomość jaki porządek prawny, a co za tym idzie jakie przepisy, będą właściwe do zawartej umowy.

Dokumentami o szczególnym znaczeniu w kontekście umów zawieranych w cyberprzestrzeni są ustawy modelowe UNCITRAL z 1996 roku przyjęte pod auspicjami ONZ. Mimo, że regulacje nie miały charakteru wiążącego to stanowiły podstawę do zmian legislacyjnych w 67 krajach[*]. W UE aktem prawnym o szczególnym walorze unifikacyjnym była dyrektywa o handlu elektronicznym. Zgodnie z wspomnianą dyrektywą państwa członkowskie UE mają obowiązek zapewnić, by umowy elektroniczne podlegały takiej samej skuteczności i ważności prawnej jak umowy tradycyjne. Kwestie jurysdykcyjne wynikające z konwencji międzynarodowych oraz regulacji regionalnych zostały szczegółowo opisane w rozdziale 2.1.2. *Jurysdykcja cywilna* stąd też zagadnienie to nie będzie szerzej poruszane w niniejszym podrozdziale.

4.2.1.1. Umowa - rodzaje, cechy

W piśmiennictwie wyróżnia się wiele różnych definicji umowy elektronicznej. Paweł Podrecki uznaje, że przez „umowy zawierane w Internecie można rozumieć ogół stosunków prawnych, których istotnym elementem jest wykorzystanie stron sieci jako środka komunikowania się i przekazywania oświadczeń woli w celu zawarcia umowy. Umowy zawierane w Internecie określane są również umowami on-line”[928]. Z kolei Andrzej Stosio, kładzie nacisk na formę składania oświadczeń woli, twierdząc, że „zawarcie umowy za pośrednictwem Internetu polega na wymianie za pomocą tego medium stosownych oświadczeń woli przez strony umowy”[929]. Bez wątpienia należy stwierdzić, że mamy do czynienia z umową elektroniczną, gdy do jej zawarcia wykorzystano środki elektroniczne. Jacek Gołaczyński stawia tezę, że „umowami elektronicznymi będą także umowy zawarte

[*] Szerzej omówione w podrozdziale 3.1.1.3. *Dorobek Komisji Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego (UNICITRAL).*

[928] P. Podrecki, *Podział i rodzaje umów w Internecie*, [w:] *Prawo Internetu*, Warszawa 2004, s. 40.

[929] A. Stosio, op. cit., s. 132.

tradycyjnie, ale które będą wykonywane przez spełnienie świadczenia w postaci elektronicznej"[930]. Pogląd odmienny wyraża Jacek Janowski, który stwierdza, że należy taką umowę uznać za zawartą w formie tradycyjnej, poniważ element elektroniczny ma wówczas charakter uboczny i przypadkowy[931]. Z kolei Wolfgang Kilian uznaje, że „umowy elektroniczne są porozumieniami pomiędzy osobami fizycznymi lub prawnymi komunikującymi się ze sobą za pomocą środków technicznych (przez cyfrowe sieci komunikacyjne) w celu przeprowadzenia transakcji dotyczących dóbr niematerialnych (tak zwane wykonanie *on-line* lub bezpośredni handel elektroniczny) lub stworzenia w drodze elektronicznej podstaw do wydania dóbr materialnych (tzw. wykonanie *offline* lub pośredni handel elektroniczny)"[932]. Wśród wymienionych wyżej propozycji, najbardziej adekwatna wydaje się być ta, wyrażona przez Wolfganga Kiliana. Nie można utożsamiać umów elektronicznych wyłącznie z tymi zawartymi *on-line*, ponieważ zakres tego typu jest znacznie szerszy i obejmuje oświadczenia woli złożone na przykład za pomocą e-maila.

Umowy elektroniczne mogą zostać zaklasyfikowane również ze względu na kryterium zawarcia umowy. Według Jacka Gołaczyńskiego umową elektroniczną będzie taka umowa, która została zawarta:

- przez złożenie oświadczeń woli w postaci elektronicznej (*on-line*),
- przez złożenie oświadczeń woli w postaci elektronicznej (*off -line*) na przykład przez wymianę zapisanych elektronicznie na nośnikach (CD, dyskietka) oświadczeń woli oraz, która według kryterium wykonania umowy została zawarta:

– przez złożenie oświadczeń woli w postaci elektronicznej (*on-line*) i wykonana przez spełnienie świadczenia w postaci elektronicznej (*on-line*) umowa elektroniczna *sensu stricto*,

– złożenie oświadczeń woli w postaci elektronicznej (o*ff-line*) i wykonana przez spełnienie świadczenia (*off-line*) na przykład wręczenie nośników informatycznych z oprogramowaniem,

[930] J. Gołaczyński, *Umowy elektroniczne - próba definicji*, [w:] J. Gołaczyński (red.), *Umowy elektroniczne w obrocie gospodarczym*, Warszawa 2005, s. 19.
[931] J. Janowski, *Kontrakty* ..., s. 57.
[932] W. Kilian, op. cit., s. 209-210.

– przez złożenie oświadczeń woli w postaci elektronicznej (*on-line*) i wykonana przez spełnienie świadczenia w postaci tradycyjnej,

– przez złożenie oświadczeń woli w postaci tradycyjnej i wykonana przez spełnienie świadczenia w postaci elektronicznej (*on-line*)[933].

Podobną klasyfikację wprowadza Jacek Janowski, według którego zawarcie umowy i spełnienie świadczenia drogą elektroniczną może nastąpić:

1) „techniką sieciową - przez transmisję danych elektronicznych:
   - *on-line* - w sposób aktywny i w kontakcie bezpośrednim,
   - *off-line* - w sposób pasywny i w kontakcie pośrednim;
2) techniką pozasieciową - przez wymianę elektronicznego nośnika informacji (*outside-line*):
   - własnoręczne przekazanie nośnika
   - doręczenie nośnika przez pocztę tradycyjną"[934].

Błędem jest zatem utożsamianie umów elektronicznych wyłącznie z umowami *on-line*. Wskazana wyżej klasyfikacja wskazuje, że część z umów uznanych za elektroniczne jest zawierana za pomocą programów pocztowych, czy też wymiana oświadczeń woli za pomocą nośników informatycznych z zapisem tekstowym ujawniającym wolę stron - a zatem *off-line*. Cechą charakterystyczną umów *off-line* jest to, że przedsiębiorca, u którego złożono zamówienie na przykład przez pocztę e-mail, nie odpowiada natychmiastowo na zamówienie. Wyrażone w niniejszym rozdziale poglądy doktryny co do zasady zachowują aktualność pomimo upływu czasu. Specyfiką prawa cywilnego jest elastyczność i dostosowanie się do zmieniających stosunków prawnych.

Umowy elektroniczne można podzielić na bezpośrednie i pośrednie. Pierwsze z nich dotyczą przedmiotu zapisanego w postaci elektronicznej, takiej, jak program komputerowy czy usługa udzielenia dostępu do sieci czy baz danych. Brak fizycznego nośnika przedmiotu umowy umożliwia zatem wykonanie umowy za pośrednictwem sieci wirtualnej. Elektroniczne umowy pośrednie są zawierane za pośrednictwem cyberprzestrzeni, lecz wykonanie ich następuje w sposób tradycyjny. Przykładem pośredniej umowy elektronicznej

[933] J. Gołaczyński, *Umowy elektroniczne - próba definicji*, [w:] idem (red.), *Umowy elektroniczne w obrocie gospodarczym*, Warszawa 2005, s. 19-20.
[934] J. Janowski, *Kontrakty …*, s. 57.

jest zakup *on-line* przedmiotu, a następnie jego fizyczne dostarczenie przez kuriera czy pocztę[935].

Jeszcze inną formę klasyfikacji można przyjąć biorąc pod uwagę strony umowy. Można wyróżnić umowy zawierane między konsumentami (C2C - ang. *Consumer to Consumer*), między przedsiębiorcami (B2B - ang. *Business to Business*) między konsumentami a przedsiębiorcami (C2B - ang. *Consumer to Business*) oraz pomiędzy administracją publiczną a przedsiębiorcami (A2B - ang. *Administration to Business*). Największy obrót z wykorzystaniem umów elektronicznych następuje pomiędzy przedsiębiorcami (B2B)[936]. Ponadto, D. Lubasz do wymienionego wyżej katalogu dodaje relacje pomiędzy przedsiębiorcami a pracownikami (B2E - ang. *Business to Employee*)[937].

Umowy elektroniczne można zaklasyfikować pod względem rodzaju zastosowanego podpisu. Jacek Jankowski wyróżnia:

- zwykłe kontrakty elektroniczne - mające taką samą skuteczność prawną jak umowy zawierane ustnie lub odręcznie,
- bezpieczne kontrakty elektroniczne - nieposiadające takiej samej skuteczności prawnej jak umowy zawierane na piśmie, ale zapewniające wyższy stopień bezpieczeństwa,
- kwalifikowane kontrakty elektroniczne - równie skuteczne jak umowy zawierane w zwykłej formie pisemnej,
- notarialne kontrakty elektroniczne - niewystępujące obecnie, będą miały znaczenie po wprowadzeniu przepisów o elektronicznych aktach notarialnych z oświadczeniami w formie notarialnej[938].

W niniejszym opracowaniu zostaną opisane zagadnienia związane ze zwykłymi kontraktami elektronicznymi, ponieważ występują one w przestrzeni wirtualnej najczęściej i stanowią największą część obrotu handlowego. Jedynie nieliczna grupa użytkowników sieci dysponuje kwalifikowanymi podpisami elektronicznymi, dlatego też są one stosowane stosunkowo rzadko. Podkreślić również należy, iż zgodnie z międzynarodowymi standardami umowy elektroniczne wywierają takie same skutki prawne jak umowy tradycyjne.

[935] J. Gołaczyński, op. cit., s. 21-22.
[936] W. Kilian, op. cit., s. 217-218.
[937] D. Lubasz, op. cit., s. 28.
[938] J. Janowski, *Kontrakty …*, s. 66.

Uwzględniając kryterium przedmiotowe umowy elektroniczne można podzielić na umowy tradycyjne nazwane i nienazwane. Nową kategorią są umowy nienazwane specyficzne dla obrotu elektronicznego sieciowego i pozasieciowego. Są to umowy charakterystyczne dla cyberprzestrzeni, które wprawdzie mogą być zawarte poza Internetem, ale wykonanie ich zawsze następuje w przestrzeni wirtualnej. Do takich umów należą między innymi umowy zawierane z *Network Service Providers*[939] umożliwiające użytkownikom końcowym uzyskanie dostępu do sieci Internet lub świadczeń uzyskiwanych za pomocą cyberprzestrzeni na przykład umowa o transmisji danych czy umowa o krótkotrwałe przechowywanie danych[940]. Do tego typu usług można zaliczyć chmurę obliczeniową[*], dostęp do programów komputerowych czy filmów *on-line*. Umowy nienazwane, specyficzne dla cyberprzestrzeni różnią się co do zasady elektronicznym zawarciem i wykonaniem umowy (miejsce i czas), lecz w pozostałych aspektach, nierzadko możliwe jest stosowanie tradycyjnego prawa zobowiązań.

Nieodzownym elementem umów elektronicznych są wzorce kontraktowe i regulaminy zawierające postanowienia umowy, do których zazwyczaj nie można wprowadzić zmian ani uzupełnić postanowień zaproponowanych przez jedną ze stron. Kontrahent, który chce związać się umową przyjmuje bezwarunkowo wzorzec, mając jednak możliwość kształtowania istotnych elementów transakcji takich, jak rodzaj, gatunek, liczba, waluta czy sposób płatności[941]. Zawarcie umowy za pomocą wzorca kontraktowego w przestrzeni cyfrowej może nastąpić w trzech podstawowych formach[942]. Wyróżnia się mianowicie:

1. Metodę *shrink-wrap* - polegającą na poinformowaniu nabywcy, że będzie on związany postanowieniami wzorca kontraktowego od momentu pierwszego użycia produktu (na przykład instalacji oprogramowania, pierwszego uruchomienia programu). Istotnym elementem jest umożliwienie nabywcy zapoznania się z treścią wzorca jeszcze przed złożeniem zamówienia. Do związania się wzorcem kontraktowym nie zachodzi w momencie zapłaty ceny, lecz później - z chwilą zerwania opakowania produktu, do

[939] *Network Service Providers* - dostawca usług sieciowych, są to przedsiębiorstwa sprzedające dostęp do sieci, z tym że uzyskanie dostępu następuje przez bezpośrednie podłączenie do szkieletu sieci.
[940] J. Janowski, *Kontrakty …*, s. 83.
[*] Więcej o chmurze obliczeniowej w rozdziale 4.3 *Własność intelektualna w cyberprzestrzeni a prawo międzynarodowe.*
[941] W.J. Kocot, op. cit., s. 240.
[942] Więcej: R. Polčák, *Introduction to ICT law (selected issues)*, Brno 2007, s. 71-84.

którego załączona została instrukcja obsługi wraz z ogólnymi warunkami na przykład ochrony licencyjnej.

2. Metodę *click-wrap* - stosuje się zazwyczaj w przypadku pobierania oprogramowania z Internetu, wcześniejszej instalacji oprogramowania na sprzedawanych komputerach, rejestracji na portalach internetowych czy zakupów *on-line*. Związanie się wzorcem kontraktowym następuje zazwyczaj w ten sposób, że na stronie internetowej strony umowy pojawia się wzorzec umowy z komunikatem o konieczności zapoznania się z jego treścią. Użytkownik ma do wyboru dwie opcje - „zgadzam się" i „nie zgadzam się". Kliknięcie na pierwszy z nich powoduje akceptację wzorca umownego i zawarcie umowy. Brak akceptacji warunków umowy z kolei powoduje, skutek odwrotny.

3. Metodę *browse-wrap* - metoda ta w przeciwieństwie do metody *click-wrap* nie wyświetla wzorca kontraktowego na ekranie komputera, a użytkownik nie jest zobowiązany do odrzucenia bądź akceptacji wzorca. Metoda ta polega na tym, iż postanowienia umowy pokazane są po kliknięciu w hiperlinka, który przenosi użytkownika na odpowiednią stronę zawierającą regulamin czy ogólne warunki umowy. Dokonanie tej czynności jest opcjonalnie, ale nie niezbędne[943].

Sposób zawarcia umowy w przestrzeni cyfrowej następuje nieco inaczej niż w formie tradycyjnej. Jacek Gałczyński wskazuje, że „cechą umów elektronicznych jest ich interaktywność, bezpośredniość, multimedialność ofert i reklam, niskie koszty transakcji. Interaktywność polega na zindywidualizowanym sposobie przekazywania informacji między stronami służącymi do zawarcia umowy. W szczególności, chodzi tu o stopniowanie wymiany informacji od pasywnej (przez stronę WWW), do aktywnej przez przesyłanie szczegółowych informacji pocztą elektroniczną. Ostatecznie powstanie problem, z jakim momentem można mówić o złożeniu oferty, oraz przez którą stronę"[944]. Od tradycyjnych umów odróżnia je przede wszystkim sposób zawarcia i wykonania umowy. By umowa została zawarta, konieczne jest złożenie oświadczeń woli, które w przeciwieństwie do umów tradycyjnych nie są składane osobiście, lecz za pomocą odpowiedniego oprogramowania lub sprzętu. Cechą charakterystyczną jest również to, że wiele umów elektronicznych ma

[943] P. Wierzbicki, *Metody zawierania umów z wykorzystaniem wzorców kontraktowych w Internecie - analiza wybranych orzeczeń*, [w:] E. Galewska (red.), *Wybrane aspekty prawa nowych technologii*, Wrocław 2013, s. 69-73.
[944] J. Gołaczyński, Podział ... ,[w:] Idem (red.), *Umowy elektroniczne w obrocie gospodarczym*, Warszawa 2005, s. 15.

charakter umów adhezyjnych. Przedsiębiorcy oferują jednostronnie w cyberprzestrzeni produkty i usługi swojego przedsiębiorstwa posługując się wzorcami umów takimi, jak ogólne warunki umów, formularze, taryfy, regulaminy, a konsument zawierając umowy, z zasady wyraża zgodę na związanie się regulaminem. Internauci w przestrzeni wirtualnej najchętniej zawierają umowy sprzedaży, dostawy, zamiany, umowy o dzieło oraz umowy zlecenia[945].

4.2.1.2. Zawarcie umowy

Zawarcie umowy w różnych systemach prawnych może nastąpić na kilka sposobów i jest uzależnione od spełnienia określonych ustawowo kryteriów. Na przykład w anglosaskim systemie *common law*, aby umowa została zawarta musi wypełniać cztery stadia: ofertę (ang. *offer*), akceptację oferty (ang. *acceptance of the offer*), zamiar stworzenia stosunku prawnego oraz *consideration*[946]. Zawarcie umowy w prawie francuskim następuje przez opisanie jej wartości i przypisanie tej czynności mocy wiążącej[947]. Z kolei prawo niemieckie wymaga jedynie oferty (niem. *Angebot*) i jej przyjęcia (niem. *Annahme des Angebots*)[948]. W Polsce zawarcie umowy zostało uregulowane w Kodeksie cywilnym[949] i może nastąpić na przykład w drodze złożenia oferty i jej przyjęcia (art. 66-70 k.c.), w drodze rokowań (art. 72 k.c.) oraz w drodze przetargu (art. 70^1-70^4 k.c.) bądź w drodze mieszanej, gdy jedna strona składa ofertę, a druga przechodzi do rokowań.

Najpowszechniejsze sposoby zawarcia umowy to tryb ofertowy, negocjacyjny oraz przetargowy i te typy kontraktów opisano w niniejszym opracowaniu. Modele te powszechnie występują zarówno w Polsce, jak i w innych krajach. Spopularyzowanie Internetu w obrocie gospodarczym nie doprowadziło do wykształcenia się nowej dziedziny prawa kontraktów elektronicznych. Dotychczas istniejące regulacje zostały inkorporowane do umów zawieranych w cyberprzestrzeni, którym została przyznana pełna ważność prawna. Fakt ten został potwierdzony w art. 8 ust. 1 modelowej ustawy UNCITRAL o elektronicznym obrocie

[945] G. Bar, *Elektroniczne świadczenie w obrocie profesjonalnym*, Wrocław 2012, s. 47-49.
[946] H. Rowe, *Electronic Commerce and Consumers*, "International Business Lawyer" 1998, nr 4, s. 166.
[947] W.J. Kocot, op. cit., s. 163.
[948] O. Paland, *Bürgerliches Gesetzbuch*, Monachium 1998, s. 139.
[949] Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. z 1964 r., Nr 16, poz. 93).

kontraktowym, w której stwierdzono, że nie można odmówić skuteczności i ważności umowy zawartej w postaci elektronicznej tylko z tej przyczyny, że w procesie jej zawierania użyto danych elektronicznych. Ponadto, w art. 11 ustawy UNCITRAL o handlu elektronicznym uznano, że oferta oraz jej przyjęcie może być również wyrażone w postaci wiadomości elektronicznej. Nie można odmówić skuteczności kontraktu, w którym wymiana oświadczeń woli nastąpiła w sposób elektroniczny[950].

Tryb ofertowy jest najpopularniejszym sposobem zawierania umowy za pomocą przestrzeni wirtualnej. W tym trybie zawierane są transakcje, w których strony korzystają z poczty elektronicznej, komunikatorów internetowych oraz których kontrahenci posługujący się zamieszczonym na stronie www interaktywnym formularzem, służącym do złożenia zamówienia. Negocjacje z kolei są stosowane, gdy strony komunikują się w czasie rzeczywistym bądź zbliżonym do rzeczywistego oraz posiadają dostęp do programu komputerowego pozwalającego wpływać na treść umowy (usługi VoIP, IRC, multimedialne przesłanie obrazu i dźwięku). Prowadzenie „negocjacji może nastąpić za pomocą strony internetowej, na której zalogowani użytkownicy mogą wymieniać swoje propozycje i stanowiska na forum w odpowiedzi na propozycje innych uczestników. Takim systemem posługuje się większość aukcji internetowych na przykład Allegro. Umowa zawierana jest przez aktywne uczestnictwo w aukcji. Oferty są zbierane przez program komputerowy, który wskazuje podbicie oferty przez jednego z uczestników. Wygrywa użytkownik, który zgłosił najkorzystniejszą ofertę"[951]. Popularnym trybem jest również przetarg; jego odmianą jest aukcja internetowa, której uczestnicy stopniowo podbijają ofertę.

Rozwinąć należy wątek umów adhezyjnych, zwanych również umowami o przystąpieniu. Na ich mocy osoba zainteresowana określonym świadczeniem przystępuje do umowy na warunkach, na jakich to świadczenie jest proponowane przez inny podmiot[952]. W przypadku dużych przedsiębiorstw i umów zawieranych z setkami czy tysiącami konsumentów, niemożliwe jest realne negocjowanie warunków każdej pojedynczej umowy zawieranej w przestrzeni cyfrowej. Najbardziej powszechne jest przyjęcie regulaminu czy ogólnego wzorca umowy przedsiębiorcy. Osoba zainteresowania zawarciem umowy musi bezpośrednio (przez specjalną czynność techniczną oraz formalną) lub pośrednio (przy okazji innej czynności) dokonać potwierdzenia, że zapoznała się z odpowiednim wzorcem umowy

[950] W.J. Kocot, op. cit., s. 165-166.
[951] Ibidem, s. 168-169.
[952] R. Golat, *Internet - aspekty prawne*, Warszawa 2003, s. 74-75.

lub regulaminem. Zaznaczenie odpowiedniego pola oznacza akceptację warunków umowy, a zatem zawarcie umowy na zasadach określonych w regulaminie[953]. Umowy adhezyjne w cyberprzestrzeni są zawierane nie tylko pomiędzy przedsiębiorcami a konsumentami, ale również w obrocie dwustronnie profesjonalnym[954]. Przedsiębiorcy mogą zgodzić się na przyjęcie wzorca umownego drugiej strony bądź podjąć negocjacje. Tak jak w przypadku kontraktów tradycyjnych, przedsiębiorcy mają większą możliwość negocjowania szczególnych postanowień umowy.

Jacek Janowski wskazując na powszechne stosowanie wzorców umownych stwierdza, że: „stosunki społeczne, ekonomiczne i prawne nawiązywane w Internecie i za pośrednictwem poszczególnych narzędzi internetowych są więc formalizowane lub faktycznie kształtowane w sposób typowy, przez jednostronnie ustalane ogólne wzorce kontraktowe. Dotyczy to umów o charakterze mieszanym (zawieranych z udziałem konsumentów) oraz umów dwustronnie handlowych (zawieranych pomiędzy przedsiębiorcami). Jednakże w Internecie zachodzi większa swoboda kształtowania treści zawieranych umów, wyboru kontrahenta, z którym zostanie zawarta umowa, oraz samego charakteru Internetu, który jest: rozległy, rozproszony i niezawłaszczalny oraz szeroko dostępny w każdym miejscu i czasie”[955]. Z kolei Damian Klimas stawia trafną tezę, że: „zmienił się klasyczny model umowy oparty na autonomii woli (swobodzie umów), w której obie strony decydowały o treści stosunku. Zastąpił go model masowych umów zawieranych na odległość (często telefonicznych lub elektronicznych, zawieranych *on-line* lub *off-line*)”[956]. Cyberprzestrzeń sprzyja zawieraniu umów adhezyjnych. Po pierwsze, strona ma szeroką możliwość wyboru kontrahenta, a zatem wyboru postanowień umowy, na które będzie się godzić. Oczywiste również jest, iż w przypadku zawierania dużej liczby umów nie jest możliwe każdorazowe negocjowanie ich warunków z każdym kolejnym kontrahentem. Akceptacja ogólnych warunków umowy powoduje przyśpieszenie stosunków kontraktowych, szeroki oraz masowy dostęp do świadczeń odpowiadających potrzebom nabywców.

Zawieranie umów w przestrzeni wirtualnej posiada własną specyfikę związaną z koniecznością spełniania odpowiednich wymogów informatycznych. Udostępnienie umowy następuje w wersji elektronicznej, strony umowy są pozbawione fizycznej możliwości

[953] J. Janowski, *Kontrakty …*, s. 98.
[954] R. Golat, op. cit., s. 75
[955] J. Janowski, *Kontrakty…*, s. 99.
[956] D. Klimas, *Obowiązki informacyjne przedsiębiorców w umowach B2C ecommerce -wybrane aspekty*, [w:] E. Galewska (red.), *Wybrane aspekty prawa nowych technologii. Publikacja studenckiego koła naukowego” Blok prawa komputerowego”,* cz. 3, Wrocław 2015, s. 120.

weryfikacji kontrahenta i złożonej przez niego oferty. By zawrzeć umowę elektroniczną, konieczne jest posiadanie minimalnej wiedzy technicznej i odpowiedniego sprzętu. Kwestią problematyczną może okazać się również płatność za usługę czy towar. Najbardziej rozpowszechnionymi metodami płatności są przelewy oraz płatności kartą[957]. Istnieją jednak alternatywne metody płatności takie, jak pieniądz elektroniczny czy pieniądz wirtualny, które zostaną szczegółowo opisane w dalszej części pracy.

4.2.1.3. Oferta i jej przyjęcie

Oferta i jej przyjęcie jest podstawowym sposobem zawarcia umowy. Zawarcie umowy w drodze ofertowej jest możliwe między innymi w polskim i niemieckim porządku prawnym oraz w systemie anglosaskim. W polskim piśmiennictwie ofertę definiuje się jako: „oświadczenie woli wyrażające stanowczą decyzję zawarcia umowy i określające co najmniej istotne postanowienia tej umowy[958]", czyli *essentialia negotii*. Procedura zawarcia umowy w trybie ofertowym składa się z dwóch kroków: propozycji zawarcia umowy przez jedną stronę oraz przyjęcia oferty przez drugą stronę. Oferta pełni dwie zasadnicze funkcje. Po pierwsze wszczyna procedurę zawarcia umowy, a po drugie ustala jej treść[959]. W artykule 2.2 Zasad Międzynarodowych Kontraktów Handlowych UNIDROIT[960] oferta jest zdefiniowana jako dostatecznie określona propozycja, z której wynika zamiar oferenta do bycia związanym w przypadku jej przyjęcia. Z kolei Konwencja wiedeńska o umowach międzynarodowej sprzedaży towarów z 1980 r. w art. 14 stanowi, że za ofertę uznaje się propozycję zawarcia umowy skierowaną do jednej lub wielu określonych osób, jeżeli jest wystarczająco precyzyjna i wskazuje, że oferent umowy, w razie jej przyjęcia, ma zamiar być nią związany. Kolejny artykuł stanowi, że oferta staje się skuteczna z chwilą dojścia do adresata.

Według artykułu 66 § 1 k.c. oświadczenie drugiej stronie woli zawarcia umowy stanowi ofertę, jeżeli określa ona istotne postanowienia umowy. O tym, czy mamy do

[957] W. Kilian, op. cit., s. 213.
[958] P. Machnikowski, *Komentarz do art. 66 k.c.*, [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks Cywilny Komentarz*, Warszawa 2016, s. 170.
[959] Ibidem, s. 170.
[960] UNIDROIT Principles of International Commercial Contracts, tekst w języku angielskim dostępny na oficjalnej stronie internetowej UNIDROIT: http://www.unidroit.org/publications/513-unidroit-principles-of-international-commercial-contracts [10.06.2016].

czynienia ze stanowczą propozycją oferty rozstrzygać będzie szczegółowość jej treści, ale również ustalone zwyczaje czy praktyka zawierania umów. Pewne wątpliwości prawne mogą budzić propozycje zawarcia umowy, które są składane na stronach internetowych. Można mieć do czynienia z ofertą bądź zaproszeniem do jej złożenia. W polskim oraz zagranicznych systemach prawnych treści zamieszczone na stronach internetowych takie, jak reklamy, cenniki i inne ogłoszenia skierowane do ogółu bądź do poszczególnych osób zazwyczaj traktuje się jak zaproszenie do zawarcia umowy, nawet jeżeli posiadają istotne postanowienia umowy. Podkreśla się, że „rozwiązanie takie jest korzystne zwłaszcza dla tego, kto taką propozycję w Internecie składa choćby z uwagi na liczne zagrożenia, na jakie narażeni są uczestnicy obrotu elektronicznego i znacznie wyższe ryzyko wystąpienia pomyłek lub innych nieprawidłowości w treści danych publikowanych na stronach WWW (...). Ryzyko zawarcia niepożądanych umów leży po stronie operatora strony internetowej. Dlatego też prezentację towaru na witrynie *on-line* wraz z proponowaną ceną uważać należy w razie wątpliwości za zaproszenie do składania ofert lub rozpoczęcia rokowań. Z uwagi na to, że stroną aktywną, inicjującą i nawiązującą kontakt elektroniczny jest zwykle użytkownik sieci (konsument), to od niego należy oczekiwać złożenia oferty. Nie ma zatem potrzeby, aby informację umieszczoną na stronie internetowej z zasady uważać za ofertę, a przedsiębiorcę prezentującego się na takiej stronie za oferenta”[961]. Z kolei wysłanie propozycji zawarcia umowy na wiele adresów e-mail według Wojciecha J. Kocota powinno być uznane za ofertę, ponieważ zostało skierowane do konkretnych odbiorców, których można zidentyfikować. Autor uznaje, że skoro przedsiębiorca zna adresy e-mail adresatów to zostały one poddane wstępnej selekcji i stanowią wybraną grupę zindywidualizowanych odbiorców[962]. Stwierdzenie to jednak jest nietrafne, gdyż współcześnie adresy e-mail będące częścią składową baz danych są sprzedawane pomiędzy różnymi podmiotami i nie zawsze będą stanowiły wyselekcjonowaną grupę odbiorców. Coraz większa część korespondencji elektronicznej zawiera spam, który nie może być uznany za ofertę.

Przyjęcie oferty następuje w drodze oświadczenia woli oblata, aprobującego treść postanowień umowy. Oświadczenie to może być złożone w dowolnej formie i w dowolny sposób. Artykuł 18 ust. 1 Konwencji Wiedeńskiej z 1980 roku stanowi, że akceptacją oferty jest każde oświadczenie lub inne postępowanie, które wyraża zgodę na przyjęcie propozycji. Oświadczenie takie staje się skuteczne z chwilą, gdy doszło do oferenta, chyba że dotarło po

[961] W.J. Kocot, op. cit., s. 177-178.
[962] Ibidem, s. 183.

zastrzeżonym terminie, a jeżeli termin nie został zastrzeżony - w ciągu rozsądnego terminu uzasadnionego okolicznościami danej transakcji. Milczenia czy bezczynności nie można zatem uznać za przyjęcie oferty.

W obrocie elektronicznym przyjęcie oferty może nastąpić przez doręczenie oferentowi oświadczenia woli na nośniku elektronicznym za pomocą przestrzeni wirtualnej w ramach biernego, jak i aktywnego dostępu do sieci. Internet daje szereg form komunikacji, dlatego też przyjmuje się, że oferent ma prawo i obowiązek określić w ofercie w jaki sposób oblat może złożyć oświadczenie o przyjęciu oferty. W sytuacji, gdy brak jest takiego zastrzeżenia istnieje niebezpieczeństwo, iż kontrahent może złożyć oświadczenie o przyjęciu oferty w niespodziewany sposób. Oferent ma również prawo zastrzec pod rygorem nieważności, iż oblat ma obowiązek złożyć oświadczenie o przyjęciu oferty w odpowiedniej formie szczególnej. Gdy takie zastrzeżenie nie zostało uczynione oświadczenie może zostać dokonane w dowolnej postaci[963].

Do polskiego porządku prawnego nowelizacją z dnia 14.02.2003 roku został wprowadzony art. 66^1 Kodeksu cywilnego, który reguluje kwestię związania się ofertą elektroniczną[964]. Zmiana stanowi konsekwencję implementacji art. 10 i 11 dyrektywy o handlu elektronicznym. Podstawowym celem zmian było wprowadzenie odpowiednich regulacji na europejskim rynku handlu i usług internetowych oraz ochrona uczestników tego rynku[965]. Oferta elektroniczna stanowi kwalifikowaną postać oferty, ponieważ ze względu na swoją specyfikę wymaga dodatkowych unormowań. Podstawowym elementem odróżniającym ofertę tradycyjną oraz ofertę elektroniczną jest sposób związania oferenta[966]. Artykuł 66^1 § 1 k.c. stanowi, że oferta złożona w postaci elektronicznej wiąże składającego, jeżeli druga strona niezwłocznie potwierdzi jej otrzymanie. Potwierdzenie może nastąpić przez dowolne zachowanie oblata, jeżeli w sposób dostateczny sposób ujawnia ono przyjęcie oferty.

Ustawodawca paragrafem drugim art. 66^1 k.c. nałożył na przedsiębiorców, którzy składają ofertę w postaci elektronicznej, szereg obowiązków informacyjnych. Przedsiębiorcy

[963] Ibidem, s. 204.
[964] P. Machnikowski, op. cit., s. 175.
[965] A. Brzozowski, *Komentarz do art. 66^1 k.c*, [w:] K. Pietrzykowski (red.), *Kodeks cywilny. Komentarz. Art. 1-449^{10}*, t. 1, Warszawa 2015, s. 337.
[966] J. Janowski, *Kontrakty …*, s. 163.

zostali zobowiązani do informowania przed zawarciem umowy w sposób jednoznaczny i zrozumiały kontrahentów o:

- czynnościach technicznych składających się na procedurę zawarcia umowy (procedura zawarcia umowy, forma w jakiej można złożyć oświadczenie woli),
- skutkach prawnych potwierdzenia przez drugą stronę otrzymania oferty między innymi związanym z udzieleniem informacji o nieodwołalności przyjęcia oferty,
- zasadach i sposobach utrwalania, zabezpieczania i udostępniania przez przedsiębiorcę drugiej stronie treści zawieranej umowy,
- metodach i środkach technicznych służących wykrywaniu i korygowaniu błędów we wprowadzanych danych, które przedsiębiorca jest obowiązany udostępnić drugiej stronie,
- językach, w których umowa może być zawarta,
- kodeksach etycznych, które stosuje oraz o ich dostępności (w postaci elektronicznej).

Zgodnie z art. 66^1 § 3 k.c. §2 stosuje się odpowiednio, jeżeli przedsiębiorca zaprasza drugą stronę do rozpoczęcia negocjacji, składania ofert albo do zawarcia umowy w inny sposób. Podkreślić należy, że regulacje powyższe nie znajdą zastosowania do procedury zawierania umów w ramach poczty elektronicznej ani innych środków indywidualnego porozumiewania się na odległość oraz w stosunkach dwustronnie profesjonalnych, jeżeli strony tak postanowiły. W doktrynie wskazuje się, że „wyłącznie stosowania art. 66^1 § 2 k.c. do zawierania umów w ramach biernego dostępu do Internetu, wzorowane na rozwiązaniu przyjętym w art. 10 ust. 4 i 11 ust 3 Dyrektywy 2000/31/EC, uzasadniane jest najczęściej brakiem potrzeby szczególnej ochrony użytkowników sieci w przypadku posługiwania się przez nich środkami niebezpośredniej komunikacji elektronicznej. Korzystanie z takich środków nie stwarza bowiem zagrożeń większych niż metody porozumiewania się na odległość będące dotychczas w powszechnym użyciu”[967].

Wymienione wyżej obowiązki przedsiębiorcy stanowią konsekwencję implementacji dyrektywy o handlu elektronicznym. Porównanie postanowień dyrektywy oraz przepisów polskiego kodeksu cywilnego prowadzi do przekonania, że katalog obowiązków został w prawie polskim rozszerzony między innymi o kodeksy etyczne, ich dostępność w postaci elektronicznej, obowiązek informowania o skutkach prawnych potwierdzenia oferty oraz

[967] W.J. Kocot, op. cit., s. 200.

objęcie obowiązkiem informacyjnym negocjacji, składania ofert albo do zawarcia umowy w inny sposób[968]. Dyrektywa zakładała wprowadzenie minimalnych standardów, wszelkie zatem dodatkowe obowiązki informacyjne, mają na celu pełniejsze zabezpieczenie słabszej strony stosunku kontraktowego - konsumenta.

Wygaśnięcie oferty nastąpi, jeżeli oblat nie złożył we właściwym czasie oświadczenia o jej przyjęciu lub w czasie przyjętym nie przystąpił do wykonania kontraktu. Ponadto, umowa wygasa w przypadku odrzucenia oferty, złożenia kontroferty przez oblata, śmierci stron, ogłoszenia upadłości oraz utraty zdolności do czynności prawnych. Dopuszczalność odrzucenia oferty znajduje również odzwierciedlenie w międzynarodowych aktach prawnych, między innymi w Konwencji wiedeńskiej z 1980 roku wprowadzono instytucję odrzucenia oferty w art. 17 oraz złożenia nowej oferty w art. 19 ust 1[969].

Dozwolone jest również odwołanie oferty przed zawarciem umowy, jeżeli odwołanie dotarło do adresata przed wysłaniem przez niego oświadczenia o przyjęciu oferty. Rozwiązanie takie zostało przyjęte między innymi w Konwencji wiedeńskiej z 1980 roku, gdzie zastrzeżono jednak, ze oferta nie może zostać odwołana, jeżeli wynika to z jej treści bądź określono w nim termin przyjęcia. Tożsame postanowienia przyjęto również w Polsce jednakże przepis ten znajdzie zastosowanie wyłącznie w odniesieniu do kontraktów zawieranych w kontaktach dwustronnie profesjonalnych, czyli w stosunkach między przedsiębiorcami. W doktrynie przedmiotu podkreśla się, że w obrocie powszechnym obowiązuje zasadna nieodwołalności składanych ofert[970].

4.2.1.4. Negocjacje

W stosunkach pomiędzy przedsiębiorcami zawarcie umowy następuje najczęściej rzez negocjacje, których celem jest zawarcie umowy o złożonej treści, niestandardowym przedmiocie bądź zawierającej postanowienia szczegółowe, które wymagają dokładnego dookreślenia. Negocjacje mogą przebiegać wieloetapowo, brak jest jednak jednego ogólnie

[968] P. Podrecki, *Zawarcie umowy w sieci Internet*, [w:] idem (red.), *Prawo Internetu*, Warszawa 2007 s. 33.
[969] W.J. Kocot, op. cit., s. 276.
[970] Ibidem, s. 291.

przyjętego schematu ich prowadzenia[971]. Wojciech J. Kocot uważa, że cechą wyróżniającą negocjacje jest jednakowa pozycja stron negocjujących, gdzie każdy ma możliwość zgłaszania mniej lub bardziej stanowczych propozycji zawarcia umowy[972].

W polskim porządku prawnym ustawodawca nakłada na strony prowadzące negocjacje obowiązek zachowania tajemnicy informacji udostępnionych z zastrzeżeniem poufności. Naruszenie tego obowiązku będzie skutkować powstaniem roszczenia o naprawienie szkody i wydaniem korzyści uzyskanych przez kontrahenta, który naruszył obowiązek zachowania tajemnicy[973]. Ponadto, wprowadzono obowiązek prowadzenia negocjacji zgodnie z dobrymi obyczajami. Artykuł 72 § 2 k.c. stanowi, że: „strona, która rozpoczęła lub prowadziła negocjacje z naruszeniem dobrych obyczajów, w szczególności bez zamiaru zawarcia umowy, jest obowiązana do naprawienia szkody, jaką druga strona poniosła przez to, że liczyła na zawarcie umowy". Przepis ten wprowadza odpowiedzialność odszkodowawczą za prowadzenie negocjacji w złej wierze, czyli bez zamiaru zawarcia umowy. Podobne postanowienia dotyczące obowiązku prowadzenia negocjacji w dobrej wierze znalazły się w kodeksach cywilnych Włoch (art. 1337 włoskiego k.c.), Izraela (sek. 12(a) ustawy - Prawa Kontraktów (cz. ogólna), 1973 - obowiązek prowadzenia rokowań zgodnie z handlowymi zwyczajami) czy Austrii (§ 914 ABGB zobowiązanie stron negocjujących do wzajemnego uczciwego traktowania się). W innych systemach prawnych odpowiedzialność negocjujących kontrahentów ma charakter deliktowy tak, jak we Francji i w Szwajcarii[974].

Znawcy doktryny, podkreślają, że do przedwczesnego zakończenia negocjacji może dojść w przypadku zastosowania niedozwolonych praktyk negocjacyjnych, za które można uznać chociażby:

- „odmowę dalszego negocjowania albo zerwanie negocjacji, bez podania powodu lub z oczywiście błahego powodu (*refusal to negotiate*),
- obstrukcyjne taktyki negocjacyjne tj. fałszywe przedstawienie okoliczności faktycznych, podstępne wprowadzenie w błąd, celowe opóźnienie negocjacji lub ich prowadzenie ze świadomością, iż zawarcie umowy nie jest możliwe (*improper tactics*),

[971] P. Podrecki, *Zawarcie ...,* s. 36-37.
[972] W.J. Kocot, op. cit., s. 268.
[973] P. Podrecki, *Zawarcie ...,* s. 37.
[974] W.J. Kocot, op. cit., s. 276 - 277.

- zamierzone składanie propozycji niemożliwych do przyjęcia przez drugą stronę (*unreasonable proposals*),
- odmowa ujawnienia informacji istotnych dla prowadzenia rokowań albo wykorzystywanie uzyskanych wiadomości do własnych celów (*nondisclosure, illegal disclosure*),
- równoczesne negocjacje z innymi (*negotiations with others*),
- próby renegocjacji przyjętych już ustaleń (*renegotiating*),
- jednostronne zrywanie negocjacji, które są w impasie lub trwają zbyt długo (*break off negotiations*)"[975].

Możliwość wystąpienia wymienionych przykładowo niedozwolonych praktyk ma szczególne znaczenie w obrocie elektronicznym, w którym nierzetelni kontrahenci starają się wykorzystać anonimowy charakter komunikacji elektronicznej. Postuluje się, aby przedkontraktowa ochrona negocjacji *on-line* została oparta na konstrukcji dobrej wiary. Prezentowany jest pogląd, że najbardziej optymalnym rozwiązaniem w obrocie elektronicznym byłoby zawieranie przedumownego porozumienia negocjacyjnego określającego zasady rozliczeń poniesionych kosztów oraz ustalającego postępowanie w razie niezawarcia umowy. Takie przedumowne porozumienia są zawierane jednakże głównie przez największych przedsiębiorców posiadających profesjonalne zaplecze prawne. Praktyka obrotu gospodarczego pokazuje brak jednolitych i powszechnie akceptowalnych zasad prowadzenia negocjacji w sieci teleinformatycznej. Stąd też postulat wprowadzenia i egzekwowania w negocjacjach kontraktów *on-line* obowiązku prowadzenia negocjacji w dobrej wierze od początku rokowań aż do zawarcia umowy (ang. *fair dealing, good faith, best efforts*, niem. *Treu und Glauben*)[976]. Prowadzenie negocjacji *on-line* winno odbywać się z poszanowaniem dobrych obyczajów i praktyk rynkowych. Uzasadniona jest zatem odpowiedzialność odszkodowawcza w przypadku ujawnienia tajemnic przedsiębiorstwa uzyskanych w czasie negocjacji.

Przeprowadzenie negocjacji za pomocą sieci jest coraz bardziej powszechne. Wciąż powstają nowe narzędzia komunikowania się na odległość, są to połączenia telefoniczne za pomocą Internetu, prowadzenie wideokonferencji czy też najbardziej podstawowa forma poczty elektronicznej. Prowadzenie negocjacji z wykorzystaniem cyberprzestrzeni jest

[975] Ibidem, s. 280-281.
[976] Ibidem, s. 274-281.

rozwiązaniem tańszym, szybszym i łatwiejszym[977]. Udział w wideokonferencji redukuje koszty związane z podróżą pracowników, czyli koszty przejazdu czy zakwaterowania. Przesyłanie danych za pomocą systemów informatycznych znacznie skraca komunikację, przyśpiesza proces wymiany dokumentów, akceptację danych i informacji dodatkowych.

Nie ma jednolitego modelu negocjacji elektronicznych. Zwykle negocjacje służą do przeprowadzenia dużych transakcji gospodarczych takich, jak fuzje, przejęcia spółek, duże inwestycje budowane, sprzedaż sprzętów o dużej wartości. Przeważnie tylko część negocjacji jest prowadzona za pomocą technik informatycznych (za pomocą Internetu następuje wymiana dokumentów, korespondencji, dokumentacji projektowej). Sposobem negocjacji z wykorzystaniem sieci jest również posługiwanie się przez jedną ze stron zautomatyzowanym systemem komputerowym. System ten służy do negocjowania nieskomplikowanych kontraktów, przypominających wzorce umowne[978].

Negocjowanie umów w praktyce przebiega w dwóch zasadniczych formach. Negocjacje w trybie zwykłym są prowadzone aż do ustalenia wszystkich lub istotnych postanowień umowy. Jest to typowy sposób zawierania umów o nieskomplikowanej treści i formie prawnej, nie ma konieczności zatrudniania prawników czy specjalistów do skonsultowania treści umowy. W negocjacjach w trybie złożonym do ustalenia wszystkich (lub istotnych) postanowień umowy następuje przez zaciąganie w trakcie prowadzenia negocjacji zobowiązań przedkontraktowych, które określają sposób prowadzenia rokowań lub treść umowy będącej przedmiotem rokowań. Postanowienia takie nazywane również listami intencyjnymi, deklaracjami z intencją czy punktacją są sporządzane przed zawarciem umowy[979]. Zobowiązania przedkontraktowe potwierdzają zamiar zawarcia umowy przez strony, mają jednak charakter niewiążący. W internetowym obrocie gospodarczym stosowanie wstępnych porozumień negocjacyjnych nie jest powszechnie stosowane z uwagi na fakt wykorzystywania cyberprzestrzeni głównie pomocniczo lub do negocjacji umów o nieskomplikowanej treści. Przewiduje się jednak wzrost znaczenia przestrzeni wirtualnej w

[977] J. Janowski, *Kontrakty …*, s. 233.
[978] W.J. Kocot, op. cit., s. 268-269.
[979] Listy intencyjne można podzielić na materialnoprawne (zawierające już wynegocjowane zapisy przyszłego kontraktu, listę tematów do negocjacji) oraz formalnoprawne (na przykład zobowiązanie stron do prowadzenia rokowań w dobrej wierze, podział kosztów, obowiązek zachowania tajemnicy handlowej). Zob. W.J. Kocot, op. cit., s. 282-290.

obrocie dwustronnie profesjonalnym, a w związku z tym zaistnieje potrzeba ustalania takich postanowień w czasie negocjacji umowy zawieranej w postaci elektronicznej[980].

4.2.1.5. Przetarg i aukcja

Zarówno oferty, jak i negocjacje polegają na zawarciu umowy pomiędzy oznaczonymi stronami umowy. W przypadku aukcji i przetargu dopiero w drodze odpowiednich czynności następuje wyłonienie drugiej strony umowy. Wyłonienie oferenta może nastąpić w drodze ustnej bądź pisemnej. Pierwsza dotyczy zazwyczaj umów o prostym charakterze powszechnie stosowanych w obrocie gospodarczym - w formie aukcji (głównie sprzedaż, dostawa czy najem). W drodze pisemnej w formie przetargu - są zawierane bardziej skomplikowane umowy o złożonym charakterze i treści (na przykład budowa inwestycji), które niejednokrotnie wymagają uzyskania decyzji administracyjnych, zawarcia umów z podwykonawcami czy uzyskania odpowiednich zabezpieczeń. Uczestnictwo w aukcji ma charakter dobrowolny, jest stosowany przez podmioty głównie niepubliczne. Druga często jest stosowana obligatoryjnie przez podmioty publiczne, które przeprowadzą ją zgodnie z odpowiednimi regulacjami prawnymi w sprawach o złożonej tematyce i skomplikowanej treści. Różnicą pomiędzy aukcją i przetargiem jest również to, że organizator przetargu nie jest związany koniecznością wyboru najkorzystniejszej oferty. Odnosząc to do rozważań niniejszej pracy uznać można, że aukcje internetowe uzyskały ogromną popularność, czego nie można z kolei stwierdzić o przetargach internetowych. Nie mniej jednak prognozuje się, że w związku coraz większym postępem technologicznym metoda ta będzie coraz szerzej wykorzystywana[981].

Jacek Jankowski za aukcję internetową uważa aukcję przeprowadzoną w Internecie, charakteryzującą się informowaniem uczestników za pomocą stron internetowych lub e-maila. Autor za przetarg internetowy uznaje przetarg przeprowadzony w pewnym zakresie za pomocą Internetu, w szczególności przez umieszczenie ogłoszeń na stronach www oraz przesyłania ofert za pomocą poczty elektronicznej[982]. Cechą wspólną aukcji i przetargu jest

[980] W.J. Kocot, op. cit., s. 282-290.
[981] J. Janowski, *Kontrakty* ..., s. 240-242.
[982] Ibidem, s. 243.

inicjowanie ich przez organizatorów za pomocą ogłoszeń skierowanych do ograniczonego bądź nieograniczonego kręgu adresatów[983]. Celem obu postępowań jest wybór oferenta, który zaproponuje najkorzystniejsze warunki zawarcia umowy. W toku postępowania uczestnicy mają takie same prawa i obowiązki określone w regulaminie. Tym, co odróżnia aukcję i przetarg jest inny moment składania ofert, w aukcjach są one składane kolejno, a w przetargu równolegle[984]. Aukcję cechuje jednoczesna obecność uczestników, możliwość modyfikacji złożonych ofert oraz jawność składanych ofert[985]. Biorąc pod uwagę praktykę kontraktową oraz niewielką rolę elektronicznego przetargu w obrocie elektronicznym w niniejszym opracowaniu opisano procedurę aukcyjną.

Jacek Janowski stoi na stanowisku, że aukcje *on-line* nie mogą być uznane za aukcje w rozumieniu polskiego kodeksu cywilnego, ponieważ posiadają one znaczne różnice takie, jak brak tego samego miejsca obecności uczestników aukcji, którzy mogą przebywać w dowolnym miejscu na świecie, a ich obecność ma charakter wirtualny. Brak jest również jedności czasu - oferty *on-line,* są one dostępne na witrynach internetowych całą dobę, co oznacza niemal nieograniczony czas trwania aukcji. Wyszczególnia on też brak jawności postępowania, ponieważ oferty innych uczestników aukcji nie są powszechnie znane. Brak jest również konieczności uiszczania wadium. Obowiązek zawarcia umowy pomiędzy sprzedawcą a nabywcą powstaje dopiero w momencie przybicia oferty, a nie jej złożenia. Jako najistotniejszą odrębność aukcji internetowych autor wskazuje możliwość odmowy przybicia przez licytatora najbardziej korzystnej oferty, w sytuacji gdy uzna on, że zaproponowana cena jest niewystarczająca. W prawie polskim internetowe oferty nie są ofertami w rozumieniu kodeksu cywilnego, lecz jedynie zaproszeniami do składania ofert. Oferty winne zawierać wszelkie istotne postanowienia umowy, w tym cenę, która w przypadku aukcji internetowych jest określana przez licytanta, dlatego też nie może być uznana za ofertę w rozumieniu polskiego prawa cywilnego. Nie mniej jednak wobec braku odpowiednich regulacji do aukcji zawieranych w cyberprzestrzeni można stosować odpowiednio przepisy kodeksu cywilnego dotyczącego aukcji tradycyjnych[986].

W innych systemach prawnych z zasady brak jest kodyfikacji procedury przetargowej czy aukcyjnej. Ma ona z reguły charakter wyspecjalizowanej regulacji zwyczajowej, na który

[983] Z. Radwański, *Aukcja i przetarg po nowelizacji*, „Monitor Prawniczy" 2004, nr 8, s. 361.
[984] J. Janowski, *Kontrakty …*, s. 244-245.
[985] S. Kotecka, *Aukcja elektroniczna w polskim prawie zamówień publicznych i nowych unijnych dyrektywach zamówieniowych*, „Monitor Prawniczy" 2005, nr 6 (dodatek), s. 68.
[986] J. Janowski, *Kontrakty …*, s. 252-254.

ogromny wpływ ma zwyczaj oraz praktyka kontraktowa. Chociażby w systemie anglosaskim przetarg jest uważany za rodzaj ofertowego trybu zawarcia umowy. Ogłoszenie aukcji i przetargu uważa się za zaproszenie do złożenia oferty, a nie za ofertę. Na proces ujednolicenia i standaryzacji postępowań aukcyjnych ogromny wpływ mają profesjonalne serwisy aukcyjne takie, jak eBay.com, które stale udoskonalają swoje regulaminy i są wzorem dla mniejszych firm o podobnym profilu[987]. Nie należy również pomijać regulacji organizacji międzynarodowych takich, jak Unia Europejska czy UNCITRAL, które wprowadzają pożądane modele zachowań w przestrzeni wirtualnej, ze szczególnym uwzględnieniem słabszej strony stosunku kontraktowego, czyli konsumenta. Dzięki implementacji norm międzynarodowych konsumentowi przyznano między innymi prawo do odstąpienia od umowy zawartej na odległość.

W doktrynie wskazuje się, że „zawarcie umowy w drodze przetargu nie ma jednolitego charakteru. Wyróżnia go sformalizowany tryb wielostronnego, wieloetapowego i eliminacyjnego postępowania, którego celem jest wybór spośród wielu uczestników przetargu (licytantów, reflektantów) oferenta, który zaproponuje najkorzystniejsze warunki i z którym ogłaszający przetarg zawiera na tych warunkach umowę. Wszyscy uczestnicy przetargu mają zapewnione jednakowe prawa i obowiązki, podlegające tym samym regułom postępowania przetargowego, a relacje prawne nawiązywane pomiędzy nimi, a stroną zainteresowaną zawarciem umowy, nie dają się wyodrębnić. Cechą przetargu świadczącą o jego eliminacyjnym charakterze jest brak zindywidualizowania drugiej strony przyszłej umowy aż do ostatniej chwili, czyli do jego zamknięcia i wyboru oferty najkorzystniejszej”[988]. Biorąc pod uwagę powyższe rozważania należy stwierdzić, że jedynym czynnikiem różnicującym poszczególnych oferentów jest wysokość proponowanej przez nich ceny, wynagrodzenia lub innego świadczenia pieniężnego.

Istnieje wiele rodzajów aukcji, również tych o charakterze *on-line*. Wśród sposobów przeprowadzania aukcji wyróżnić można aukcje:

- klasyczne (angielskie) - polegają na podbijaniu ceny wyjściowej (wywoławczej) przez uczestników aukcji, w określonym przez organizatora czasie; wygrywa uczestnik, który zaoferował najwyższą cenę,

[987] W.J. Kocot, op. cit., s 296-298.
[988] Ibidem, s. 295.

- holenderskie - polegają na licytowaniu w dół, organizator podaje wysoką cenę wywoławczą, która jest stopniowo obniżana, osoby biorące udział w aukcji mogą podać tylko raz cenę, którą są skłonni zapłacić,
- błyskawiczne - ich cechą charakterystyczną jest bardzo krótki okres trwania, zazwyczaj 60 minut, brak jest ceny minimalnej, wygrywa uczestnik, który zaproponował najwyższą ofertę,
- przetargowe - uczestnicy aukcji składają swoją ofertę nie znając ceny minimalnej ani sum zaproponowanych przez innych uczestników aukcji,
- odwrócone - w tym rodzaju aukcji przedmiotem nie są towary do sprzedania lecz kupienia, uczestnicy aukcji są osobami, które mogą dostarczyć/sprzedać licytowany artykuł,
- wielokrotne (równoległe) - mają miejsce, gdy sprzedawca chce sprzedać kilka egzemplarzy tego samego produktu; zwycięzcami aukcji są osoby, które zaproponowały najwyższe ceny za produkt[989].

Przetargi czy też aukcje są jednymi z popularniejszych metod nabywania dóbr w cyberprzestrzeni. W czasie przeprowadzania aukcji organizator i uczestnicy nie są obecni fizycznie w tym samym miejscu i czasie, lecz są obecni w przestrzeni wirtualnej[990]. W klasycznym modelu aukcji, organizowanych przez wyspecjalizowane w internetowych przetargach przedsiębiorstwa, występują trzy podmioty organizator przetargu[991], osoba wystawiająca towar[992] oraz potencjalni nabywcy (którzy muszą przeważnie zarejestrować się wcześniej na stronie organizatora).

Czynnością poprzedzającą wzięcie udziału w aukcji internetowej jest rejestracja uczestnika i zawarcie umowy o korzystanie ze stron aukcyjnych. By aukcja doszła do skutku jej organizator musi zaakceptować udział w aukcji nabywców i zbywców. Następuje to przez rejestrację uczestników, którzy uzyskują w ten sposób prawo do uczestnictwa we wszystkich

[989] B. Gregor, M. Stawiszyński, *e-Commerce*, Bydgoszcz-Łódź 2002, s. 116-121.
[990] J. Janowski, *Kontrakty …*, s. 252.
[991][Por.] A. Stosio, op. cit., s. 115-116. Jest to zazwyczaj wyspecjalizowana firma zapewniająca obsługę aukcji i zamieszczająca towary będące przedmiotem aukcji na swojej stronie www (przykładem takiej firmy są Allegro i eBay). Biorąc pod uwagę dużą liczbę kontrahentów organizator przetargu zajmuje organizacją strony internetowej, grupuje towary w kategorie ułatwiające obejrzenie oferty. Organizator ma za zadanie przekazanie stronom aukcji dokładnych danych umożliwiających wykonanie umowy, czyli dostarczenie towaru czy zapłatę ceny. Za każdą transakcję organizator pobiera prowizję będącą jego przychodem.
[992] Ibidem. Może to być osoba fizyczna, która wystawia używaną rzecz na internetową akcję jak i profesjonalny przedsiębiorca, który chce rozszerzyć swój rynek zbytu i dystrybuować towar nowymi kanałami. Możliwe jest również, że organizatorem i osobą wystawiającą towar będzie ten sam podmiot na przykład producent zamieszczający na swojej stronie www zakładkę z aukcjami internetowymi własnych produktów.

aukcjach internetowych organizowanych na stronie www organizatora. Rejestracja polega na wprowadzeniu do systemu danych osobowych lub rejestrowych użytkownika, który następnie otrzymuje indywidualne konto prowadzenia transakcji w ramach serwisu. By założyć konto należy mieć zdolność do czynności prawnych (wymóg formalny) oraz adres poczty elektronicznej (wymóg techniczny umożliwiający komunikację z serwisem). Kolejnym elementem jest zawarcie umowy o korzystanie z serwisowych stron aukcyjnych, nazywana również umową o przeprowadzenie i uczestnictwo w aukcji internetowej. Umowa ta zawarta jest pomiędzy administratorem portalu aukcyjnego i jego użytkownikami na podstawie regulaminu i stanowi podstawę do uczestnictwa w aukcjach przeprowadzonych na stronie organizatora[993].

W doktrynie wyróżnia się trzy podstawowe fazy aukcji internetowej:

1. Ogłoszenie aukcji *on-line* - organizator ogłasza na swoim portalu aukcyjnym czas, miejsce, przedmiot oraz warunki postępowania aukcyjnego ewentualnie sposób ich udostępnienia. Ogłoszenie jest zazwyczaj publikowane na odpowiednim internetowym formularzu, gdzie po zalogowaniu przez uczestnika, wystawia on przedmiot aukcji wraz z opisem (oraz ewentualnie ze zdjęciami), które to ogłoszenie jest następnie zamieszczane na portalu aukcyjnym. Czas aukcji rozpoczyna się od razu po jej wywołaniu i trwa do precyzyjne oznaczonego momentu. Oznacza to, że w przeciwieństwie do tradycyjnych aukcji brak czasowego odstępu pomiędzy ogłoszeniem a wywołaniem. Co istotne, brak jest również określenia miejsca aukcji internetowej, która odbywa się ona na stronie internetowej opublikowanego ogłoszenia[994].
2. Składanie ofert przez licytantów - w czasie tej fazy licytanci składają oferty w odpowiedzi na zaproszenie do ich składania. Uznaje się, że podanie ceny w toku licytacji oznacza akceptację zasad, na podstawie których prowadzona jest aukcja, złożenie oferty nabycia przedmiotu sprzedaży oraz przyjęciem do wiadomości ogłoszenia aukcyjnego. Postępowanie aukcyjne opiera się w zasadzie na jednym elemencie, jakim jest proponowana cena. Wygrywa oferta najwyższa po upływie oznaczonego w aukcji czasu bądź ta osoba, która skorzystała z opcji „kup teraz”[995]. Pamiętać należy, że złożenie oferty następuje zazwyczaj przez zalogowanie się do

[993] J. Janowski, *Kontrakty …*, s. 259-261.
[994] M. Giaro, *Zawarcie umowy w trybie aukcji internetowej*, Warszawa 2014, s. 109-110.
[995] J. Janowski, *Kontrakty …*, s. 259-265.

systemu aukcyjnego za pomocą przyznanego loginu i hasła. Identyfikacja ta umożliwia przypisanie oferty do konkretnego użytkownika i podanych przez niego danych[996].

3. Wybór oferty - jest to ostatnia faza, w której zostaje zawarta umowa z licytantem, który zaoferował najwyższą cenę. Aukcja internetowa, w odróżnieniu od tradycyjnej nie ma przybicia rozumianego jako publiczne potwierdzenie wyboru oferty, ponieważ „występowanie przybicia w aukcji internetowej jest kwestionowane ze względu na dojście umowy do skutku z upływem oznaczonego terminu. Argumentuje się, że jego upływ nie ma cech oświadczenia woli wyrażającego zamiar wywołania skutków prawnych. Skoro więc upływ terminu nie jest oświadczeniem woli, nie może on być utożsamiany z przybiciem"[997]. Po upływie wyznaczonego terminu trwania aukcji zostaje wybrana oferta najwyższa, zgodnie z postanowieniami regulaminu. Wybór oferty może również nastąpić w sposób zautomatyzowany przez odpowiednie oprogramowanie komputerowe portalu aukcyjnego. O ile postanowienia regulaminu nie stanowią inaczej organizator aukcji nie może jej zamknąć bez wyboru najkorzystniejszej oferty[998]. Z reguły przedwczesne zamknięcie aukcji jest dopuszczalne tylko do chwili złożenia pierwszej oferty bądź wystąpienia szczególnych okoliczności na przykład kradzieży przedmiotu aukcji. Jednakże jeżeli uczestnicy rozpoczęli już licytację to przedwczesne zamknięcie umowy ma ten skutek, że wygrywa licytant, który na daną chwilę złożył najkorzystniejszą ofertę[999].

Ogólne warunki aukcji są zawierane zazwyczaj w regulaminie organizatora. Przeważnie znajdują się tam postanowienia, które mówią między innymi o tym, że organizator przetargu nie ponosi odpowiedzialności za wady fizyczne i prawne przedmiotów będących przedmiotem przetargu, informacje o zakazie wystawiania na aukcję przedmiotów, którymi obrót jest zakazany oraz informacje o danych osobowych uczestników aukcji. Ponadto, regulaminy zawierają ponadto informację o tym czy serwis dopuszcza możliwości wycofania przedmiotu aukcji czy złożonej już oferty, często wprowadza się też zakaz wpływania przez uczestników przetargu na wynik aukcji[1000]. Wojciech J. Kocot odnosząc się do odpowiedzialności organizatorów wskazuje, że: „Zawieranie umów w drodze aukcji internetowej niesie za sobą ryzyko wyłącznie dla bezpośrednich jej uczestników. Internetowe

[996] M. Giaro, op. cit., s. 129.
[997] Ibidem, s. 151.
[998] J. Janowski, *Kontrakty …*, s. 259-265.
[999] M. Giaro, op. cit., s. 157.
[1000] A. Stosio, op. cit., s. 116-117.

serwisy aukcyjne nie ponoszą odpowiedzialności za zachowania ogłaszającego, za jakość, bezpieczeństwo lub prawną dopuszczalność obrotu danymi towarami. Nie odpowiadają również za prawdziwość i rzetelność opisów zawartych w ogłoszeniach, zdolność ogłaszających do zawarcia umowy oraz wypłacalność licytantów uczestniczących w aukcji. Szczegółowo sformułowane zasady wyłączenia odpowiedzialności serwisu aukcyjnego zajmują poczesne miejsce wśród postanowień zdecydowanej większości regulaminów aukcyjnych. Obowiązki serwisu w ramach umowy udostępnienia strony internetowej ograniczone zostają z reguły do podejmowania niezbędnych działań w celu wyeliminowania sprzecznych z prawem lub niezgodnych z regulaminem zachowań użytkowników sieci. Prowadzący strony aukcyjne serwis i jego przedstawiciele lub pracownicy są zwolnieni z jakiejkolwiek odpowiedzialności wynikłej lub związanej z jakąkolwiek aukcją. W związku z faktem, że prowizja staje się należna dopiero po skutecznym sfinalizowaniu transakcji, operator stron aukcyjnych nie odpowiada za ewentualne utrudnienia lub niemożliwość realizacji aukcji, wynikające z przyczyn technicznych”[1001].

Organizatorzy aukcji podejmują zatem wiele kroków, aby zabezpieczyć się przed ewentualnymi roszczeniami uczestników aukcji. Jest to postępowanie jak najbardziej zrozumiałe wobec znacznej liczby przeprowadzanych transakcji oraz braku pewności co do rzetelności oraz autentyczności licytujących i ogłaszającego. W przypadku umów zawieranych w cyberprzestrzeni niebezpieczeństwo niewykonania bądź nienależytego wykonania umowy jest większe niż w obrocie tradycyjnym. O ile sprzedający zazwyczaj czeka z wysyłką towaru do czasu zapłaty ceny, o tyle kupujący nie ma możliwości sprawdzenia stanu i autentyczności towaru przed odebraniem. Również organizator aukcji nie jest w stanie w żaden sposób potwierdzić zgodności towaru z opisem. Niestety, nieuczciwi sprzedawcy wykorzystują potencjalną anonimowość i możliwość ukrycia się pod nic nieznaczącym loginem, sprzedając nieistniejące towary i usługi. Dokonując transakcji *on-line* należy dochować szczególnej ostrożności, sprawdzić opinię o sprzedawcy, dokładnie przeczytać opis przedmiotu i jego parametry techniczne tak, by zminimalizować prawdopodobieństwo zakupu wadliwego przedmiotu. Niestety zachowanie wszystkich możliwych kroków bezpieczeństwa nie jest w stanie uchronić nas przed nieuczciwym kontrahentem.

[1001] W.J. Kocot, op. cit., s. 314.

4.2.1.6 Czas i miejsce zawarcia umowy

Ustawa modelowa UNCITRAL w sprawie handlu elektronicznego z 1996 r. nie porusza wprost kwestii czasu i miejsca zawarcia umowy. W art. 15 znajduje się jednak odniesienie do zagadnienia, gdzie i kiedy doszło do wysłania zbioru danych oraz w gdzie i kiedy przedmiotowy zbiór danych został otrzymany. Uznaje się, że dzięki tym wyznacznikom można ustalić czas i miejsce zawarcia umowy. Artykuł 15 stanowi, że o ile postanowienia stron nie stanowią inaczej to, wysłanie zbioru danych (ang. *dispatch*) następuje wówczas gdy wejdzie (ang. *enters*) on w system informacyjny będący poza zasięgiem kontroli nadawcy. Jeżeli strony nie postanowiły inaczej za czas otrzymania wiadomości (ang. *receipt*) uznaje się (jeżeli adresat wyznaczył system informacyjny w celu odbioru danych) moment, w którym do tego systemu informatycznego został wprowadzony zbiór danych. Jeżeli jednak system informatyczny nie jest przeznaczony do odbioru danych, ale znajduje się pod kontrolą adresata - za moment odbioru danych uważa się chwilę, w której adresat wszedł w posiadanie wiedzy o innym systemie będącym pod jego kontrolą. W sytuacji, gdy adresat nie wyznaczył systemu informacyjnego - za moment odbioru danych uznaje się chwilę, w której zbiór danych wszedł w jakikolwiek system informatyczny adresata. Artykuł 15 ust 4 stanowi, że za miejsce otrzymania zbioru danych uznaje się siedzibę handlową adresata, a nie miejsce lokalizacji systemów informatycznych (o ile strony nie postanowią inaczej).

Brak jest w ustawie modelowej UNCITRAL dokładnego określenia miejsca siedziby handlowej, czyli miejsca prowadzenie działalności. Jeżeli jednak adresat lub nadawca posiadają więcej niż jedną siedzibę handlową, za miejsce prowadzenia działalności należy uznać to miejsce, które ma najściślejszy związek z daną transakcją. Gdy nie można ustalić głównej transakcji, za miejsce prowadzenie działalności należy uznać główną siedzibę. W sytuacji braku miejsca prowadzenia działalności właściwe będzie miejsce zwykłego zamieszkania nadawcy bądź adresata[1002].

Konwencja Organizacji Narodów Zjednoczonych z 2005 r. o korzystaniu z komunikacji elektronicznej w kontraktach międzynarodowych[1003] reguluje kwestię czasu i miejsca wysyłania i doręczania elektronicznych komunikatów w art. 10. Za moment wysłania

[1002] A. Stosio, op. cit., s. 124-126.
[1003] Konwencja ONZ z 2005 r. nie ma szerokiego zastosowania, ponieważ została ratyfikowana zaledwie przez siedem państw, z czego żadne z nich nie jest państwem europejskim.

komunikatu elektronicznego uznaje się chwilę, w której opuszcza on system informacyjny będący pod kontrolą nadawcy, bądź w sytuacji, gdy komunikat nie opuścił systemu informacyjnego nadawcy - moment doręczenia komunikatu. W ust. drugim artykułu za moment doręczenia komunikatu adresatowi określono chwilę, w której możliwe będzie jego odebranie przez adresata pod wskazanym przez niego adresem elektronicznym. W sytuacji gdy komunikat został wysłany pod inny adres, za moment odbioru uznano chwilę, w której możliwe stanie się odebranie komunikatu przez adresata, a adresat dowie się o dostępności komunikatu pod innym adresem. Wprowadzono domniemanie, że komunikat jest możliwy do odebrania w chwili dostarczenia na adres elektroniczny odbiorcy. Miejsce wysłania i doręczenia, podobnie jak w przypadku ustawy modelowej UNCITRAL, ustalono na siedzibę handlową stron.

Wobec powyższych rozważań należy uznać, że w praktyce miejscem zawarcia umowy elektronicznej miejsce zamieszkania albo siedziba oferenta w chwili zawarcia umowy. Zaakcentować trzeba to, co zostało również podkreślone w wyżej wymienionych regulacjach międzynarodowych dla miejsca zawarcia umowy nie ma znaczenia lokalizacja urządzeń, na przykład serwerów przedsiębiorcy. Niejednokrotnie firmy, ze względu na redukcję kosztów lokalizują te urządzenia w różnych rejonach globu, nie mającego związku z prowadzoną działalnością gospodarczą. Miejsce położenia tych urządzeń nie ma wpływu na realizację postanowień umowy, wobec czego nie powinno być brane pod uwagę[1004]. Również w polskim systemie prawa w art. 70 k.c. uznano za moment zawarcia umowy chwilę otrzymania przez oferenta oświadczenia o przyjęciu oferty przez oblata.

4.2.1.7. Wykonanie umowy

Typowym i pożądanym etapem kończącym stosunek zobowiązaniowy jest wygaśnięcie umowy przez jej wykonanie. Wykonanie umowy może nastąpić przez dokonanie transakcji bezpośredniej bądź pośredniej. Pierwsza z nich ma miejsce wówczas, gdy zarówno zawarcie jak i wykonanie umowy następuje w formie elektronicznej wymiany informacji. Jest to wyraz bezpośredniego obrotu handlowego (ang. *direct electronic commerce*), gdzie

[1004] P. Podrecki, *Zawarcie …*, s. 35.

przedmiotem umowy są dobra zapisane w postaci elektronicznej, czyli programy komputerowe, elektroniczne bazy danych[1005]. Przedmiotem tego typu transakcji mogą być zarówno umowy, których przedmiotem jest świadczenie usług, jak i umowy zapewniające korzystanie lub przenoszenie dóbr niematerialnych[1006]. Drugim typem wykonania umowy jest transakcja pośrednia, która jest związana z pośrednim handlem elektronicznym (ang. *indirect electronic commerce*), gdzie zostaje zawarta umowa elektroniczna, lecz jej wykonanie następuje w sposób tradycyjny[1007]. Cechą charakterystyczną tego typu umów jest to, że dotyczą obrotu towarami o charakterze materialnym, niezdygitalizowanym. Wykonanie tej umowy związane jest z fizycznym dostarczeniem rzeczy i wykorzystaniem tradycyjnych środków dostawy takich, jak poczta czy kurier. Przedmiotem umowy może być książka, odzież czy sprzęt elektroniczny, ale również usługi[1008]. Wykonanie umowy w sposób niezdygitalizowany nie budzi większych wątpliwości, ponieważ są wykonywane w tej formie umowy tradycyjne. Więcej problemów może nastręczyć ustalenie, kiedy doszło do wykonania umowy w postaci czysto elektronicznej, gdyż doręczenie usługi bądź innych dóbr cyfrowych może być rozmaite.

W przypadku, gdy przedmiotem umowy jest dostarczenie produktów digitalnych, a strony nie ustaliły inaczej, należyte wykonanie umowy następuje przez dostarczenie towaru w sposób:

- „umożliwiający jego ściągnięcie przez wierzyciela do jego terminala czy telefonu komórkowego,
- kompletny, tj. wraz z ze wszystkimi elementami produktu i właściwą dokumentacją,
- nadający się do uruchomienia na z góry określonym sprzęcie w z góry określonym środowisku,
- zapewniający kompatybilność ze standardowymi programami komputerowymi,
- niewywołujący zmian w systemie, utrudniających korzystanie z innego oprogramowania,
- niepowodujący innych niekorzystnych i niespodziewanych dla wierzyciela konsekwencji,

[1005] A. Stosio, op. cit., s. 214.
[1006] P. Podrecki, *Zawarcie …*, s. 48-49.
[1007] A. Stosio, op. cit., s. 214.
[1008] P. Podrecki, *Zawarcie …*, Warszawa 2007, s. 48.

- zgodny z właściwymi przepisami szczególnymi, np. prawa autorskiego, wynalazczego, znaków towarowych i in."[1009]

W przypadku, gdy dostarczony produkt digitalny wywołuje jeden z wymienionych wyżej negatywnych konsekwencji nie można uznać, iż wykonanie umowy nastąpiło w sposób prawidłowy.

Podstawowym elementem wykonania odpłatnej umowy wzajemnej jest zapłata ceny wyrażonej w sumie pieniężnej. Zapłata stanowi ekwiwalent świadczenia niepieniężnego drugiej strony. W umowach elektronicznych przelew wierzytelności pieniężnej może nastąpić zarówno w formie gotówkowej (zapłata przy odbiorze rzeczy) jak i bezgotówkowej. Do bezgotówkowych transakcji można zaliczyć polecenie przelewu i polecenie zapłaty. Coraz większą popularność uzyskują jednak elektroniczne instrumenty płatnicze, czyli karty płatnicze i pieniądz elektroniczny.

4.2.1.8. Podpis elektroniczny

Złożenie podpisu pod dokumentem jest jedną z podstawowych metod wyrażenia woli oraz zaciągania zobowiązań. Składanie oświadczeń woli w cyberprzestrzeni stworzyło problem bezpieczeństwa zawieranych transakcji i załatwianych spraw. Podpis służy do identyfikacji osoby (imię i nazwisko), deklarowanej przez nią zdolności do czynności prawnych oraz wyrażeniem konkretnej woli. W piśmiennictwie wskazuje się, że podpis „w stosunku do podpisującego jako taki stanowi podstawę domniemania znajomości sygnowanej nim treści oraz dowód akceptacji tej treści. Oznacza to zarazem zgodę podpisującego na ponoszenie konsekwencji, w tym także prawnych, które wynikają z tej znajomości akceptacji. Podpis obejmuje swoim zastosowaniem stan wiedzy, potwierdzając świadomość podpisanej treści oraz stan woli, zaświadczając o akceptacji podpisanej treści"[1010]. Podpis w formie tradycyjnej jest ściśle powiązany z daną osobą, którą można zidentyfikować za pomocą analizy grafologicznej. Dariusz Szostek uważa, że podpis elektroniczny jest bliższy pieczęci, ponieważ każda osoba posiadająca dostęp do urządzenia i danych niezbędnych do złożenia podpisu elektronicznego może wygenerować dokument opatrzony podpisem

[1009] J. Janowski, *Kontrakty …*, s. 300-301.
[1010] J. Janowski, *Podpis …*, s. 25.

elektronicznym[1011]. Również Jerzy Jacyszyn i Sebastian Zakrzewski uznają, że „dokonując identyfikacji, w rzeczywistości weryfikujemy jedynie fakt oznaczenia dokumentu przy użyciu klucza prywatnego, zarejestrowanego na daną osobę, a nie fakt rzeczywistego dokonywania przez nią czynności"[1012]. W świetle tych poglądów należy zwrócić uwagę na niebezpieczeństwo uzyskania nieuprawnionego dostępu do podpisu elektronicznego - czy to przez przypadkowe wejście w posiadanie kodów innej osoby, czy to przez działania hackerskie (łamanie kodów bądź fałszerstwo podpisu elektronicznego). Osoba, która wejdzie w posiadanie odpowiednich dokumentów jest w stanie dokonać wielu czynów niedozwolonych na szkodę ofiary.

Podpisy[1013] można podzielić na:

- manualne - własnoręczne, dokonane przez osobiste naniesienie odpowiednich znaków graficznych,
- biometryczne - tworzone za pomocą zdigitalizowanych cech fizjologicznych lub fizjonomicznych (na przykład skanowanie tęczówki oka),
- cyfrowe - składane za pomocą osobistych kodów (numerów) identyfikacyjnych,
- kryptograficzne - polegające na znajomości tajnego klucza kryptograficznego[1014].

Jeżeli weźmie się pod uwagę rodzaj nośnika wykorzystywanego do utrwalania podpisów złożonych na dokumentach oraz zastosowaną metodę zapisu danych, to podpisy można podzielić na własnoręczne (uwierzytelniające dokumenty tradycyjne) i elektroniczne (uwierzytelniające dokumenty elektroniczne)[1015]. W dysertacji opisano tę drugą formę składania podpisów.

Pierwszy raz instytucja pieniądza elektronicznego została wprowadzona do krajowego porządku prawnego w amerykańskim stanie Utach w 1995 roku ustawą o podpisie cyfrowym (*The Utah Digital Signature Act*)[1016]. W kolejnych latach, w związku z szybkim rozwojem przestrzeni cyfrowej, coraz więcej państw oraz organizacji międzynarodowych zaczęło pracować nad wprowadzeniem unormowań prawnych dotyczących podpisu elektronicznego.

[1011] D. Szostek, *Prawne aspekty podpisu elektronicznego*, [w:] J. Barta, R. Markiewicz, *Handel elektroniczny. Prawne problemy*, Kraków 2005, s. 176.
[1012] J. Jacyszyn, S. Zakrzewski, *Podpis elektroniczny jako element systemu zabezpieczenia danych w sieci*, cz. 2, „Rejent" 2001, nr 11, s. 49.
[1013] Więcej na ten temat w: J. Janowski, *Podpis…* oraz J. Jacyszyn, S. Zakrzewski, op. cit.
[1014] J. Janowski, *Podpis …*, s. 32.
[1015] Ibidem, s. 32-33.
[1016] M. Maciejewska-Szałas, *Podpis elektroniczny w prawie Wielkiej Brytanii*, „Gdańskie Studia Prawnicze" 2011, t. 26, s. 377.

W polskiej ustawie o podpisie elektronicznym z 18 września 2001 r.[1017] za podpis elektroniczny uznano dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny. Unia Europejska w 1999 roku przyjęła dyrektywę Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (dyrektywa o podpisie elektronicznym), która utraciła moc obowiązującą 30 czerwca 2016 roku na skutek wejścia w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS).

Podpis elektroniczny według Jacka Janowskiego to „podpis cyfrowy, będący ciągiem bitów (w jakikolwiek sposób powiązany z innym ciągiem bitów), składających się na podpisywany dokument, pozwalający na identyfikację tego, kto go złożył, oraz zabezpieczenie autentyczności opatrzonego nim dokumentu”[1018]. Bardziej ogólną definicję proponuje Krzysztof Korus: „pod pojęciem podpisu elektronicznego należy rozumieć wszelkie metody identyfikacji osoby, wykorzystujące techniki matematyczne i elektroniczne”[1019]. Ustawa modelowa UNCITRAL o podpisach elektronicznych za podpis elektroniczny (ang. *electronic signature*) uznaje dane w formie elektronicznej dołączone lub logicznie powiązane z przekazem danych, które mogą być użyte do identyfikacji podpisującego w związku z przekazem danych oraz do oznaczenia aprobaty informacji zawartych przekazie danych. Z kolei rozporządzenie nr 910/2014 (eIDAS) w art. 10-12 wprowadza trzy rodzaje podpisu: podpis elektroniczny, zaawansowany podpis elektroniczny oraz kwalifikowany podpis elektroniczny. Pierwszy z nich, definiowany jest jako dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i są użyte przez podpisującego jako podpis.

Artykuł 26 rozporządzenia e-IDAS wprowadza wymagania, które podpis musi spełnić by być uznany za zaawansowany podpis elektroniczny. Przyjmuje się, że jest to podpis, który:

- jest unikalnie podporządkowany podpisującemu,
- umożliwia ustalenie tożsamości podpisującego,

[1017] Dz.U. z 2001 r., Nr 130, poz. 1450.
[1018] J. Janowski, *Podpis…*, s. 38.
[1019] K. Korus, *Oświadczenie woli w postaci elektronicznej i podpis elektroniczny*, [w:] M. Chudzik i in., *Prawo handlu elektronicznego*, Bydgoszcz - Kraków 2005, s. 55.

- jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą,
- jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

W omawianej regulacji unijnej kwalifikowanemu podpisowi elektronicznemu nadano z kolei taki sam skutek prawny, jaki ma podpis własnoręczny. Za kwalifikowany podpis elektroniczny, zgodnie z art. 3 ust. 12 może być uznany zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

Drugi najpopularniejszy obecnie rodzaj podpisu elektronicznego to podpis cyfrowy (ang. *digital signature*, niem. *digitale Unterschrift*, franc. *la signature digitale*). Nie można utożsamiać podpisów elektronicznych i cyfrowych. Podpisy cyfrowe są kategorią niewątpliwie węższą, mieszczącą się w zakresie podpisów elektronicznych, do których można zaliczyć podpisy elektroniczne oparte na kodowaniu symetrycznym czy metodach biometrycznych[1020]. Podpisy cyfrowe oparte są na kryptosystemie asymetrycznym, w którym wiadomość jest szyfrowana i rozszyfrowywana za pomocą asymetrycznych kluczy[1021]. Szyfry asymetryczne wykorzystują dwa rodzaje kluczy: prywatny, tajny służący do zaszyfrowania wiadomości oraz klucz publiczny do jej odszyfrowania. Klucze te są wygenerowane za pomocą odpowiednich algorytmów[1022]. Wiadomość elektroniczna zostaje zaszyfrowana skrótem za pomocą klucza prywatnego. Ten zaszyfrowany skrót jest właśnie podpisem cyfrowym dokumentu[1023]. Klucz prywatny znajduje się w posiadaniu wyłącznie osoby tworzącej dokument, czyli osoby przekazującej informację[1024]. Odszyfrowanie wiadomości następuje za pomocą klucza publicznego, znajdującego się w posiadaniu odbiorcy. Przechwycenie klucza publicznego nie pozwala na odszyfrowanie wiadomości. Nie można także w żaden sposób na jego podstawie odtworzyć klucza prywatnego.

Posługiwanie się przedmiotową parą kluczy w obrocie elektronicznym wymaga stworzenia odpowiedniej infrastruktury bezpieczeństwa, zapewniającej brak możliwości uzyskania kluczy prywatnych przez osoby postronne[1025]. Zabezpieczenia takie gwarantowane

[1020] A. Stosio, op. cit., s. 142.
[1021] Więcej o technicznych aspektach podpisu elektronicznego w: J. Janowski, *Podpis...*
[1022] Internet Law & Policy Forum, Survey of International Electronic and Digital Signature Initiatives, s. 4.
[1023] A. Stosio, op. cit., s. 144.
[1024] K. Kowalik-Bańczyk, op. cit., s. 139.
[1025] W.J. Kocot, op. cit., s. 350-351.

są przez trzeci podmiot (tak zwana zaufana strona trzecia) zarządzający dysponowaniem metodami szyfrowymi, w którego posiadaniu znajduje się klucz publiczny. Podmiotem tym zazwyczaj są centra certyfikacyjne, które potwierdzają wystawienie podpisów elektronicznych z wykorzystaniem określonej metody[1026]. Wystawcy certyfikatów wystawiają je na wniosek osób chcących posługiwać się podpisem elektronicznym. Na wniosek osób trzecich potwierdzają oni również przynależność konkretnego certyfikatu do danej osoby, co jest nazywane weryfikacją podpisów elektronicznych[1027].

Zaufana strona trzecia (ang. *Trusted Third Party* - TTP), zwana też urzędem certyfikacji, podmiotem świadczącym usługi certyfikacyjne, jednostką certyfikacyjną jest instytucją (może to być urząd, jednostka, firma), która zajmuje się wystawianiem, potwierdzaniem, zawieszaniem i unieważnianiem podpisów elektronicznych. Urząd certyfikacji jest instytucją zaufania publicznego, wobec czego winien dysponować niepodważalnym autorytetem, gwarantującym użytkownikom potwierdzenie autentyczności i aktualności podpisów elektronicznych. Urząd certyfikacji każdorazowo na wniosek potwierdza ważność certyfikatu i osoby z nią powiązanej. Jacek Jankowski porównał urząd certyfikacji do „elektronicznego notariusza", gdyż „bierze on odpowiedzialność za poprawność i prawdziwość danych identyfikacyjnych umieszczonych w certyfikacie. W tym też celu opatruje podpisem elektronicznym wystawiane przez siebie certyfikaty. Pełna weryfikacja podpisu elektronicznego obejmuje również weryfikację podpisu złożonego pod certyfikatem. Sprawdzenia więc wymaga nie tylko sam podpis poświadczony certyfikatem, ale też sam certyfikat"[1028].

W ustawie modelowej UNCITRAL o podpisach elektronicznych certyfikat został zdefiniowany jako wiadomość albo inny zapis potwierdzający związek między podpisującym a danymi służącymi do stworzenia popisu. W polskiej doktrynie Andrzej Stosio zdefiniował certyfikat klucza publicznego jako „zapis w postaci elektronicznej, który zawiera potwierdzenie, że wymieniony w nim klucz publiczny należy do określonej w certyfikacje osoby i znajduje się w rejestrze prowadzonym przez wystawcę certyfikatów"[1029]. Certyfikat klucza publicznego potwierdza powiązanie danej osoby z określonym kluczem publicznym.

[1026] K. Kowalik-Bańczyk, op. cit., s. 139-140.
[1027] J. Janowski, *Podpis …*, s. 74.
[1028] Ibidem, s. 75.
[1029] A. Stosio, op. cit., s. 147.

Wystawca certyfikatu składa na nim swój podpis cyfrowy, czym potwierdza autentyczność certyfikatu i zawartych w nim danych[1030].

Według Jacka Janowskiego certyfikatem podpisu elektronicznego jest: „zaświadczenie elektroniczne (elektroniczny dokument) wystawione przez urząd certyfikacji, stwierdzające tożsamość osoby w nim wymienionej oraz wskazujące klucz publiczny służący do potwierdzenia jej podpisu elektronicznego”[1031]. Wskazuje on jednocześnie, że certyfikat może posiadać klasę (ang. *certificate class*) określającą stopień zabezpieczenia i ochrony danych podpisu oraz określających, w jakim stopniu urząd wydający certyfikat ponosi za niego odpowiedzialność. Certyfikat umożliwia identyfikację osoby z nim powiązanej, między innymi dzięki zawartym na nim grupach danych takich, jak dane indywidualizujące podmiot dla którego certyfikat został wydany (imię, nazwisko, klucz publiczny użytkownika podpisu, dodatkowe informacje na przykład siedziba), dane indywidualizujące certyfikat (numer seryjny, okres ważności), dane indywidualizujące wystawcę certyfikatu (nazwę wystawcy, podpis elektroniczny wystawcy) oraz dane dodatkowe (na przykład określające maksymalną wartość transakcji)[1032]. Wprowadzenie odpowiedniego poziomu zabezpieczeń jest konieczne dla zapewnienia pewności obrotu. Powierzenie weryfikacji podpisu elektronicznego zaufanej stronie trzeciej wprowadza bardziej miarodajną i pewną kontrolę nad jego autentycznością i aktualnością.

Podpisy elektroniczne mogą przybrać różnorodne formy. Obok wymienionych wyżej podpisów kryptograficznych (algorytmów asymetrycznych i symetrycznych) i podpisów biometrycznych wyróżnić można też podpisy PIN-owe (numer PIN składany wraz z numerem karty elektronicznej), podpisy manualne (tworzone za pomocą pióra cyfrowego, który przenosi ruchy pióra wprost do pamięci komputera), podpisy hasłowe (jednorazowe hasła wprowadzane na przykład ze zdrapki do systemu informatycznego z użyciem odpowiedniego identyfikatora) czy też podpis skanowany (dokument z własnoręcznym podpisem zostaje zeskanowany i zapisany w formie cyfrowej). Wymienione rodzaje podpisów zapewniają różny poziom bezpieczeństwa. Dlatego też, gdy mówimy o podpisie elektronicznym w szerokim sensie obejmuje on wszelkie środki i techniki elektroniczne, które mogą zastąpić podpis tradycyjny (zwykły podpis elektroniczny). W ujęciu ścisłym o bezpiecznym podpisie

[1030] Ibidem, s. 147.
[1031] J. Janowski, *Podpis …*, s. 80.
[1032] Ibidem, s. 80-81.

elektronicznym, mówimy wówczas, gdy stosowana jest na przykład kryptografia asymetryczna[1033].

Zgodnie z art. 7 ustawy modelowej UNCITRAL o handlu elektronicznym podpis elektroniczny będzie uznany za równoznaczny z podpisem własnoręcznym, jeżeli spełnione zostaną dwie przesłanki:

- istnieje skuteczna metoda, za pomocą której można zidentyfikować nadawcę informacji oraz dokonać autoryzacji przesłanych przez niego danych,
- zastosowana metoda jest niezawodna i w pełni służy celowi, dla którego została wiadomość została wygenerowana lub przekazana, w świetle wszystkich okoliczności, w tym porozumienia zawartego pomiędzy nadawcą a adresatem informacji[1034].

Opisany wyżej art. 7 wymaga zastosowania pewnej i skutecznej metody identyfikacji, nie wskazując jednakże, czym ta metoda miałaby się charakteryzować, czy na czym polegać. Użycie tak ogólnikowych postanowień pozwala na zastosowanie zasady neutralności technologicznej i umożliwia wprowadzenie metod zupełnie innowacyjnych technologicznie.

Tożsama regulacja znalazła się w art. 6 ustawy modelowej UNCITRAL o podpisie elektronicznym, w którym stwierdzono, że w przypadkach, gdy prawo wymaga podpisu osoby, wymaganie to jest spełnione dla przekazu danych, jeśli użyty podpis elektroniczny jest godny zaufania jako odpowiedni do celu, dla którego przekaz danych został stworzony lub przekazany, w świetle wszystkich okoliczności, włączając w to jakiekolwiek stosowne porozumienie stron. Podobne postanowienia znalazły się w rozporządzeniu eIDAS, które stanowi, że nie można odmówić podpisom elektronicznym mocy dowodowej oraz skutku prawnego z powodu, że podpis ma postać elektroniczną.

Jedną z najważniejszych zasad wyrażonych w ustawie modelowej UNCITRAL jest art. 5, który uznając swobodę zawierania umów, daje umowie pierwszeństwo przed przepisami ustawy. Przyjęto, że problemy prawne, które mogą wyniknąć ze stosowania nowych technologii można rozwiązać w samej umowie. Regulacja modelowa opierała się na zasadzie autonomii stron, które mogą zwiększyć lub zmniejszyć reżim wymagań podpisu elektronicznego w drodze postanowienia umownego, o ile nie narusza to bezwzględnie

[1033] Ibidem, s. 39-40.
[1034] Z tym, że w oficjalnym komentarzu do ustawy modelowej UNCITRAL zwracono uwagę na konieczność rozróżnienia pisma (ang. *writing*): od podpisanego oryginału (ang. *signed original*), od pisma uwierzytelnionego podpisem (ang. *signed writing*), od dokumentu poświadczonego (ang. *authenticated legal act*).

obowiązujących przepisów prawa krajowego. Ustawa modelowa przyjmuje szerokie ujęcie podpisów elektronicznych uznając, iż zaliczyć do nich trzeba nie tylko podpisy tworzone na bazie kryptografii asymetrycznej, lecz również te, które powstają na podstawie innych technologii[1035].

Takie neutralne technologicznie podejście zasługuje na aprobatę. Wprowadzanie regulacji ściśle określających parametry techniczne jednej, najlepszej w ocenie ustawodawcy metody nie jest pożądane. Obecny rozwój techniki powoduje, że w szybkim tempie dochodzi do dezaktualizacji dotychczas wykorzystywanych metod i technologii. Postęp technologiczny, zwłaszcza w obszarze bankowości, finansów i innych strefach związanych z obrotem finansowym, wprowadza coraz bardziej zaawansowane ulepszenia mające na celu zabezpieczenie przed nieuprawnionym użyciem. Regulacje neutralne technologicznie zapobiegają konieczności częstych nowelizacji ustawy i wprowadzają pewność obrotu, ponieważ obejmują swoim zakresem nowe technologie. Zasada neutralności technologicznej winna mieć zastosowanie nie tylko do podpisów elektronicznych, ale też do innych regulacji odnoszących się do cyberprzestrzeni.

Można jednak wyróżnić dwie metody regulacji podpisu elektronicznego. Pierwsza z nich, neutralna technologicznie (ang. *technology neutral*), opisuje jedynie funkcje, które podpis ma spełniać i wymagania, którym ma odpowiadać. Druga metoda specyfikacji technologicznej (ang. *technology specific*) wskazuje konkretne rozwiązania technologiczne, po spełnieniu których można by było uznać, że podpis spełnił swoje funkcje[1036].

Obowiązujące do tej pory w Polsce akty prawne są niewystarczające i nie odpowiadają nowym europejskim standardom. Rozporządzenie elDAS nałożyło na Polskę konieczność uchylenia lub zmiany wielu aktów prawnych, gdyż terminologia oraz merytoryka obowiązujących uregulowań wymagała dostosowania do nadrzędnych przepisów unijnego rozporządzenia oraz unijnych aktów delegowanych i implementujących. Wobec powyższych wymogów 5 września 2016 roku została uchwalona nowa ustawa o usługach zaufania oraz identyfikacji elektronicznej[1037]. Do pełnego wdrożenia przepisów unijnych konieczne będzie również dostosowanie systemów informatycznych.

[1035] M. Świerczyński, *Podpis…,* s. 72.
[1036] F. Wejman, *Wprowadzenie do cywilistycznej problematyki ustawy o podpisie elektronicznym*, „Prawo Bankowe" 2002, nr 2, s. 38.
[1037] Dz.U. z 2016 r., poz. 1579.

4.2.2 Elektroniczne środki płatnicze

Od zarania dziejów ludzie wymieniali towary. Początkowo funkcje pieniądza spełniały dobra materialne, kruszce i metale szlachetne, a następnie monety i banknoty. Rewolucja cyfrowa i technologiczna, stworzenie i popularyzacja Internetu była przyczynkiem powstania pieniądza w formie zapisu na elektronicznym nośniku informacji, dzięki któremu możliwe stało się dokonywanie bezgotówkowych form rozliczeń. Pieniądz elektroniczny jest w istocie kolejnym etapem wielowiekowej ewolucji środków płatniczych[1038].

W ujęciu szerokim pieniądzem są wszystkie środki płatnicze, których używa się w obrocie (czyli banknoty, monety, czeki, weksle, obligacje krajowe i zagraniczne). Ujęcie wąskie za pieniądz uznaje tylko takie środki płatnicze, którym państwo nadało moc umarzania zobowiązań pieniężnych, czyli uznania przez państwo danej formy pieniądza za środek zapłaty na określonym obszarze, którego przyjęcie przez stronę stosunku prawnego prowadzi do umorzenia zobowiązania[1039]. Brak jest jednej, ogólnej definicji elektronicznych środków płatniczych. Witold Srokosz wskazuje, że pojęcie to nie jest też używane w doktrynie ani orzecznictwie. Autor postuluje jednak, wprowadzenie tego terminu, uznając, że za użyciem pojęcia elektronicznych środków płatniczych przemawia wygoda i ułatwienie badań nad współczesną postacią środków płatniczych. Wobec powyższego, za elektroniczne środki płatnicze należy uznać: „dokumenty pełniące funkcję środka płatniczego wystawione w złotych polskich lub w walutach obcych, które przybierają postać elektroniczną"[1040]. Zauważyć należy, iż zaproponowana przez Witolda Srokosza definicja nie będzie obejmować walut wirtualnych[*], które nie są wyrażone w walucie żadnego konkretnego państwa, choć mogą być na nie wymieniane.

Do elektronicznych środków płatniczych Witold Srokosz zalicza pieniądz bezgotówkowy (bankowy) o ile przybierze formę elektroniczną, pieniądz elektroniczny, dokumenty wystawione w polskiej lub obcej walucie, które przyjmują postać elektroniczną

[1038] A. Piotrkowska, *Koncepcja i formy pieniądza elektronicznego*, „Acta Universitatis Lodziensis Folia Oeconomica" 2014, nr 1(299), s. 299.
[1039] W. Srokosz, *Istota prawna pieniądza elektronicznego*, „Prawo Bankowe" 2002, nr 12(64), s. 68.
[1040] W. Srokosz, *Prawo a rozwój elektronicznych środków płatniczych w XXI wieku*, [w:] Z. Ofiarski (red.), *XXV lat przeobrażeń w prawie finansowym i prawie podatkowym - ocena dokonań i wnioski na przyszłość*, Szczecin 2014, s. 842-843.
[*] Zostaną omówione w podrozdziale 4.2.2.2 *Pieniądz wirtualny*.

oraz kryptowaluty (ang. *cryptocurrency*). Z pewnym wahaniem autor podchodzi do wirtualnych walut (ang. *virtual currency, virtual money*) stwierdzając, że mogą być one uznane za elektroniczne środki płatnicze tylko w ograniczonym zakresie (zawężonym wyłącznie do świata gier wirtualnych)[1041].

4.2.2.1. Pieniądz elektroniczny

W piśmiennictwie uznaje się, że pieniądzem elektronicznym jest „wartość pieniężna, która jest odpowiednikiem znaków pieniężnych. Wartość ta jest zapisana na odpowiednim instrumencie, urządzeniu bądź w pliku danych (oprogramowaniu) tworząc tak zwaną monetę elektroniczną"[1042]. Europejski Bank Centralny za pieniądz elektroniczny uznał „elektroniczny zasób wartości pieniężnej występujący w urządzeniu technicznym, który może być szeroko wykorzystany do dokonywania płatności na rzecz podmiotów innych niż emitent, bez konieczności angażowania rachunków bankowych, funkcjonujący jako opłacony z góry (przedpłacony) instrument na okaziciela"[1043]. Definicja ta znacząco rozgranicza pieniądz elektroniczny od innych instrumentów płatniczych (karta płatnicza). Trudno jest podać precyzyjną i jednoznaczną definicję pieniądza elektronicznego. Termin ten winien jednak charakteryzować się neutralnością technologiczną tak, by płynnie przystosowywać się do wciąż pojawiających się innowacji technologicznych.

Pierwszy raz definicja legalna pieniądza elektronicznego pojawiła się dyrektywie 2000/46/WE Parlamentu Europejskiego i Rady[1044] z dnia 18 września 2000 r. Pieniądz elektroniczny w jej rozumieniu w żadnej przewidzianej wówczas postaci opartej na rozwiązaniach sprzętowych (karty elektroniczne-chipowe, elektroniczne portmonetki) i rozwiązaniach programowych (cyfrowe monety ang. *digital money*) nie przyjął się w prawdziwym obrocie finansowym[1045]. Wobec takiego stanu rzeczy zaistniała konieczność

[1041] W. Srokosz, *Prawo …*, s. 843.
[1042] T.R. Smus, *Spełnienie świadczeń pieniężnych za pomocą pieniądza elektronicznego*, Warszawa 2010, s. 46.
[1043] *Report on electronic*, European Central Bank 1998, s. 7, tłum. za: B. Frączek, *Pieniądz elektroniczny - próby zdefiniowania i sklasyfikowania*, „Bank i Kredyt" 2004, nr 4, s. 91.
[1044] Dyrektywa Parlamentu Europejskiego i Rady z dnia 18 września 2000 r. nr 2000/46/WE w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością (Dz.Urz. WE L 275 z 27.10.2000 r.).
[1045] W. Srokosz, *Prawo …*, s. 844.

wprowadzenia odpowiednich zmian legislacyjnych. W 2009 roku wymienioną wyżej dyrektywę zmieniono dyrektywą Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE[1046]. W nowej dyrektywie w art. 2 ust. 2 za pieniądz elektroniczny uznano wartość pieniężną przechowywaną elektronicznie, w tym magnetycznie, stanowiącą prawo do roszczenia wobec emitenta, która jest emitowana w zamian za środki pieniężne w celu dokonywania transakcji płatniczych określonych w art. 4 pkt. 5 dyrektywy 2007/64/WE i akceptowana przez osoby fizyczne lub prawne inne niż emitent pieniądza elektronicznego. Zamysłem ustawodawców było powstrzymanie się od wprowadzania ścisłych norm technicznych określających pieniądz elektroniczny tak, by zachował on pewną neutralność technologiczną, to znaczy by obejmował zarówno istniejące już metody przechowywania pieniądza na serwerze czy też na specjalnym urządzeniu płatniczym, ale również, by definicja nie blokowała przyszłych rozwiązań technologicznych.

Do emisji pieniądza elektronicznego, zgodnie z art. dyrektywy 2009/11/WE są uprawnione instytucje kredytowe, instytucje pieniądza elektronicznego, instytucje świadczące żyro pocztowe, Europejski Bank Centralny i krajowe banki centralne oraz państwa członkowskie albo ich organy regionalne lub lokalne, jeżeli nie działają one w charakterze organów publicznych. Unijny akt rozszerza zatem, w porównaniu z poprzednio obowiązującą dyrektywą 2000/46/WE, katalog emitentów pieniądza elektronicznego, co z całą pewnością przyczyni się do upowszechnienia się jego stosowania.

Zgodnie z pkt. 5 i 6 preambuły dyrektywa nie ma zastosowania w stosunku do instrumentów przedpłaconych, które jednak można wykorzystywać w ograniczonym zakresie, to znaczy takim, który pozwala posiadaczowi pieniądza elektronicznego nabywać towary i usługi wyłącznie w określonym sklepie lub sieci sklepów lub nabycia ograniczonego asortymentu towarów i usług. Wynika z tego, że za pieniądz elektroniczny według dyrektywy nie można uznać kart sklepowych, kart członkowskich, kart transportu publicznego czy bonów usługowych. Dyrektywa nie ma również zastosowania do niektórych płatności wykorzystywanych do zakupu towarów i usług cyfrowych, w stosunku do których operator

[1046] Dz.U. L 267 z 10.10.2009.

dodaje do nich wartość nierozerwalnie związaną na przykład narzędzie dostępu czy dystrybucji.

Dyrektywa 2009/110/WE złagodziła nieco reżim prawny przewidziany poprzednim dokumentem wprowadzając odpowiednie zmiany w zakresie wymagań technicznych. Mimo to, wydaje się, że nie nastąpiło jeszcze upowszechnienie się pieniądza elektronicznego w spodziewanym zakresie. Zmian takiego stanu rzeczy można upatrywać w upowszechnieniu się kart elektronicznych oraz coraz większym przejmowaniu przez smartfony funkcji przypisywanych do tej pory wyłącznie komputerom. Z całą pewnością zwiększenie popularności pieniędzy elektronicznych mogłoby nastąpić przez zmniejszenie restrykcyjności norm emisji pieniądza elektronicznego, w tym reżimu ostrożnościowego[1047].

Z powszechnie obowiązującą w Polsce definicją legalną pieniądza elektronicznego możemy zapoznać się w ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych[1048], gdzie za dyrektywą 2009/110/WE uznano go za „wartość pieniężną przechowywaną elektronicznie, w tym magnetycznie, wydawaną, z obowiązkiem jej wykupu, w celu dokonywania transakcji płatniczych, akceptowaną przez podmioty inne niż wyłącznie wydawca pieniądza elektronicznego”[1049]. W definicji tej pieniądz elektroniczny wprost uznany jest za pieniądz, tak, jak inne środki płatnicze, czyli banknoty i monety. Ustawą wprowadzono nowe regulacje dotyczące wykupu, dystrybucji i wytwarzania pieniądza elektronicznego oraz organizacji instytucji nadzoru nad tym pieniądzem.

Tomasz Targosz jest zdania, że pieniądz elektroniczny ma zupełnie innowacyjny charakter, ponieważ różni się od tradycyjnie wykorzystywanych form płatności, również tych dokonywanych w formie bezgotówkowej. Autor twierdzi, że: „innowacyjność pieniądza elektronicznego wynika przede wszystkim z faktu, że wartość pieniężna jest w tym przypadku zapisana na elektronicznym nośniku informacji, który w konsekwencji jest czymś więcej niż tylko narzędziem pozwalającym na identyfikację płacącego i na uzyskanie przez niego dostępu do prowadzonego przez bank tradycyjnego rachunku bankowego. Ta cecha pieniądza elektronicznego pozwala na wyszczególnienie następujących elementów, które uzasadniać mają tezę o jego innowacyjności w procesie zapłaty:

[1047] W. Srokosz, *Prawo…*, s. 846.
[1048] Dz.U. z 2011 r., Nr 199, poz. 1175.
[1049] Ustawa o usługach płatniczych, art. 2 pkt. 21a.

- brak konieczności powiązania z rachunkiem bankowym, co umożliwia dokonywanie płatności bez konieczności udziału osoby trzeciej[1050] (chodzi tu o osobę trzecią wobec stron transakcji, na przykład wydawcę karty płatniczej autoryzującego transakcję),
- możliwość zachowania pełnej anonimowości stron transakcji, a zwłaszcza płacącego, co upodabnia zapłatę pieniądzem elektronicznym do zapłaty gotówką"[1051].

W tradycyjnym ujęciu pieniądz elektroniczny może przyjąć techniczną postać:

- produktu opartego na technologii kart procesowych - nazywanych elektroniczną portmonetką (ang. *multipurpose prepaid card, electronic purse*),
- produktu bazującego na oprogramowaniu umożliwiającemu użytkownikowi dokonywanie płatności w Internecie, czyli tak zwany pieniądz sieciowy (ang. *network based, software based product*)[1052].

W pierwszym z systemów wartość pieniężna jest zapisana na karcie mikroprocesorowej i nazywana kartą *pre-paid*, na którą użytkownik wpłaca określoną sumę, a następnie dokonuje płatności, ale tylko do kwoty zapisanej na karcie, która stopniowo zmniejsza się z każdą kolejną transakcją, aż do wyczerpania środków. Występuje wówczas możliwość „doładowania" karty i uzupełnienia dostępnych na niej środków. „Doładowania" elektronicznej portmonetki można dokonać za pomocą specjalnie do tego dostosowanych bankomatów, komputera wyposażonego w czytnik kart podłączonego do Internetu bądź telefonu[1053]. Możliwość stosowania pieniądza elektronicznego w postaci karty przedpłaconej została ujednolicona ogólnym wprowadzeniem kart z mikroprocesorem zamiast kart z paskiem magnetycznym[1054]. Karta w formie elektronicznej portmonetki ułatwia dokonywanie płatności za zakupy, bilety komunikacji miejskiej czy parking.

Pieniądzem sieciowym jest wartość pieniężna zapisana na dysku komputera. Możliwość uzyskania dostępu do pieniądza elektronicznego przechowywanego w danej formie jest uzależniona od posiadania odpowiedniego oprogramowania umożliwiającego

[1050] D. Hirschson, T. Lewis, *European E-cash rules at the front*,, "ITLR" 2001, nr 5, s. 22.
[1051] T. Targosz, *Pieniądz elektroniczny*, [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007, s. 290-291.
[1052] R. Janowicz, R. Klepacz, *Pieniądz elektroniczny na świecie. Istota i zastosowanie elektronicznej portmonetki*, Warszawa 2002, s. 23.
[1053] R. Janowicz, *Pieniądz elektroniczny w wybranych krajach - charakterystyka, główne funkcje i zastosowanie*, „Bank i Kredyt" 2005, nr 1, s. 87.
[1054] D. Cyman, *Elektroniczne instrumenty płatnicze a bezpieczeństwo uczestników rynku finansowego*, Warszawa 2013, s. 63.

dokonywanie płatności w tej formie[1055]. Płatność z wykorzystaniem pieniądza sieciowego dokonywana jest z zastrzeżeniem, że forma zapłaty następuje zdalnie, czyli elektronicznie z wykorzystaniem łączności komputerowej[1056]. Pamiętać jednak należy, że pieniądz elektroniczny przechowywany zarówno na karcie mikroprocesorowej, jak i w formie pieniądza sieciowego zapisanego w pamięci komputera, ma tą samą cechę; w obu przypadkach istnieje konieczność wpłacenia przez użytkownika środków pieniężnych z góry.

W doktrynie pojawiły się problemy z odróżnieniem pieniądza elektronicznego zapisanego na elektronicznym nośniku informacji od innego rodzaju usług świadczonych za pomocą elektronicznych instrumentów płatniczych, czyli bankowości elektronicznej. Opisując ten problem Tomasz Targosz stwierdził, że: „problemy z właściwym podporządkowaniem powodują w szczególności rozwiązania, w których wartość pieniężna wydawana w zamian za środki pieniężne nie jest zapisana na urządzeniu znajdującym się w fizycznym posiadaniu osoby posługującej się tą formą płatności (na przykład na dysku komputera, karcie z chipem, karcie SIM w telefonie komórkowym), ale na serwerze wydawcy (czyli tak zwany pieniądz serwerowy), przy czym posiadacz ma do niej dostęp za pomocą komputera osobistego lub telefonu komórkowego lub innego urządzenia. Umożliwienie dostępu do rachunku bankowego posiadacza jest przede wszystkim cechą kart płatniczych (w najczystszej formie tak zwanych kart debetowych), podczas gdy charakterystyczne dla pieniądza elektronicznego ma być właśnie to, że nie daje on posiadaczowi jedynie możliwości uzyskania dostępu do środków pieniężnych zgromadzonych na jego rachunku w instytucji finansowej, ale pozwala na posiadanie tej wartości w elektronicznej formie zapisanej na jakimś elektronicznym środku informacji”[1057]. Powyższy problem zrodził się w trakcie implementacji dyrektywy 2000/46/WE w państwach członkowskich. Zróżnicowane podejście do kwestii technicznych i prawnych wyłoniło dwa podejścia: formalne i funkcjonalne. Pierwsze z nich opiera się na założeniu, że pieniądz elektroniczny jest wartością pieniężną zapisaną na urządzeniu elektronicznym znajdującym się w posiadaniu fizycznym osoby, której ten pieniądz został wydany. Znawcy tematu wskazują, że aby stwierdzić, że mamy do czynienia z pieniądzem elektronicznym, konieczne jest by urządzenie, za pomocą którego dokonywana jest transakcja (telefon, karta czy komputer) było tym samym urządzeniem, na którym pieniądz elektroniczny został zapisany. Drugie funkcjonalne skupia się na funkcji jaką

[1055] M. Rybiałek, *Ewolucja środków płatności (zapłaty): od pieniądza gotówkowego do pieniądza elektronicznego*, „Studia Prawnicze” 2012, z. 4 (192), s. 142.
[1056] R. Janowicz, R. Klepacz, op. cit., s. 23.
[1057] T. Targosz, op. cit., s. 297.

ma pełnić pieniądz elektroniczny, a nie aspektach technicznych jego realizacji. Stad też nie wymaga się fizycznego władztwa nad elektronicznym urządzeniem, na którym jest zapisany pieniądz elektroniczny. Wystarczy stwierdzenie, iż środki pieniężne zdeponowane na urządzeniu są pod kontrolą użytkownika, nawet jeżeli posługuje się on nimi „na odległość”[1058].

Zgodnie z ogólnie przyjętym poglądem pieniądz zarówno w formie gotówkowej, jak i bezgotówkowej pełni cztery podstawowe funkcje: miernika wartości, środka cyrkulacji, środka akumulacyjnego oraz środka płatniczego. Zatem, by pieniądz elektroniczny mógł być uznany za substytut pieniądza gotówkowego powinien spełnić wyżej wymienione funkcje[1059]. Mimo cech wspólnych, pieniądz gotówkowy wyróżnia się kilkoma cechami, których pieniądz bezgotówkowy nie posiada. Zaliczyć do nich należy: trwałość, anonimowość, brak możliwości śledzenia zapłaty, łatwość dokonania zapłaty, brak konieczności korzystania z instytucji pośredniczących, brak ograniczeń co do osoby płacącej i tej, która otrzymuje zapłatę. W ujęciu modelowym cechy te winny również być spełnione przez pieniądz elektroniczny[1060].

Wobec tak postawionej analizy należy zidentyfikować, którymi z tych cech charakteryzuje się pieniądz elektroniczny. Część autorów uznaje, że elementami pieniądza elektronicznego, dzięki którym można go uznać za substytut pieniądza gotówkowego są takie cechy, jak: możliwość finansowania bezpośrednich transakcji, akceptowanie go jako środka płatniczego przez inne podmioty niż emitent, dokonywanie głównie płatności detalicznych oraz minimalizację kosztów przy dokonywaniu płatności. Kolejnym podobieństwem jest kryterium trwałości, czyli w obu przypadkach istnieje możliwość fizycznego zniszczenia na przykład przez fizyczne zniszczenie dysku, na którym został zapisany pieniądz elektroniczny. Cechą, której nie posiada pieniądz elektroniczny jest łatwość zapłaty, ponieważ by dokonać transakcji konieczne jest posłużenie się urządzeniami elektronicznymi. Co więcej, płatność pieniądzem elektronicznym nie jest powszechnie akceptowalna. Pieniądz elektroniczny nie jest wydawany przez banki centralne, więc nie musi być akceptowany jako forma zapłaty. Wobec tego płatności można dokonywać tylko w punktach, które przyjmują taką formę rozliczeń. Kolejną cechą wskazującą na odmienności pomiędzy wymienionymi wyżej typami pieniądza jest możliwość wielokrotnego wykorzystania. Nie ulega wątpliwości, iż pieniądz w

[1058] Ibidem, s. 297 -198.
[1059] W. Srokosz, *Istota …*, s. 68.
[1060] Ibidem, s. 68.

formie gotówkowej może być używany nieograniczoną ilość razy. Cechą pieniądza elektronicznego jest jego „jednorazowość" to znaczy niemożność wielokrotnego wydawania przez tę samą osobę tych samych jednostek pieniężnych. Każda jednostka pieniądza elektronicznego ma przypisany numer, który po dokonaniu zapłaty zostaje unieważniony, tak by nie mógł być wykorzystany ponownie[1061].

Inni autorzy wskazują, że pieniądz elektroniczny podobnie jak gotówka nosi cechy anonimowości podczas płatności oraz braku potrzeby angażowania osób trzecich w proces transakcji. Różnicą jest bez wątpienia sposób zabezpieczeń. Gotówka cechuje się zabezpieczeniami fizycznymi w postaci znaków wodnych. Pieniądz elektroniczny jest zabezpieczony kryptograficznie w celu ochrony poufności i integralności danych oraz uwierzytelnienia transakcji[1062]. W świetle powyższych rozważań przychylić należy się do poglądu, że pieniądz elektroniczny stwarza duże trudności klasyfikacyjne, gdyż stale się rozwija i niejednokrotnie występuje w formie modelowej. Autorzy starają się jednakże usystematyzować problem wskazując formy, rodzaje i cech wspólne pieniądza.

Tabela 15. Formy i rodzaje pieniądza gotówkowego, bezgotówkowego i pieniądza elektronicznego oraz niezbędne funkcje (cechy) wspólne pieniądza

Kryteria	**Pieniądz gotówkowy**	**Pieniądz bezgotówkowy**	**Pieniądz elektroniczny**
Forma	Zapisy księgowe - depozyty bankowe na rachunkach	Informacja cyfrowa przechowywana na elektronicznych nośnikach	Funkcje (cechy) wspólne pieniądza, które powinny być spełnione: - miernik wartości - środek płatniczy - środek cyrkulacji - środek akumulacji
Rodzaje	Depozyty na rachunkach banków komercyjnych Depozyty na rachunkach w banku centralnym	Pieniądz bazujący na oprogramowaniu (*software money*) Inteligentne karty przedpłacone (mikroprocesorowe)	

Źródło: T.R. Smus, op. cit., s. 55, opracowanie na podstawie B. Frączek, op. cit., s. 93

[1061] B. Frączek, op. cit., s. 93-94.
[1062] R. Janowicz, op. cit., s. 90.

Zagraniczni znawcy tematu[1063] pod koniec lat dziewięćdziesiątych wskazywali, że idealny system płatności dokonywanej za pomocą sieci wirtualnej winien spełniać następujące cechy:

- być łatwy w użytkowaniu i powszechnie dostępny,
- umożliwiać komunikowanie się na odległość bez konieczności korzystania z jakichkolwiek innych niż Internet środków porozumiewania się,
- mieć stosunkowo niskie koszty transakcji,
- stwarzać możliwość stosowania zarówno do małych, jak i dużych płatności z uwzględnieniem ułamkowych setek części jednostek monetarnych używanych w danym kraju,
- zapewniać bezpieczeństwo dokonywania płatności,
- wprowadzać możliwość rozliczania transakcji międzynarodowych i wzajemnie ich uznawanie w obrocie handlowym,
- mieć szybki okres realizacji przelewu.

Z całą pewnością zmiany w prawie unijnym i ustawodawstwach krajowych innych państw pozwalają na realizację nowych pomysłów ułatwiających dokonywanie płatności oraz wprowadzanie nowych instrumentów pieniądza elektronicznego. Jako przykład podaje się rozpowszechnienie kart zbliżeniowych umożliwiających dokonanie drobnych płatności (do 50 zł) bez konieczności autoryzowania zapłaty, czyli podawania numeru PIN. Od kilku lat można również dokonywać drobnych płatności za pomocą telefonu komórkowego. Instrumenty te ułatwiają obrót, przyśpieszają transakcje i w coraz większym stopniu upodabniają pieniądz elektroniczny do gotówkowego. Coraz więcej osób w codziennym życiu odchodzi od fizycznego posiadania gotówki, coraz chętniej dokonując płatności właśnie pieniądzem elektronicznym.

Wprowadzenie pieniądza elektronicznego nie jest finalnym etapem ewolucji środków płatniczych. Damian Cyman wyszczególnia podstawowe, w jego ocenie, modele pieniądza:

- pieniądz, którego wartość jest zagwarantowana przez państwo, uregulowany jako prawny środek płatniczy (pieniądz gotówkowy),
- pieniądz wymieniany na pieniądz gotówkowy na podstawie ustawy, posiadający reglamentowany w ustawie katalog emitentów (pieniądz elektroniczny),

[1063] G. Smith, *Internet Law and Regulation*, Londyn 1997, s. 225.

- pieniądz będący prawnym środkiem płatniczym, stanowiący roszczenie o wykup tego pieniądza przez emitenta, które jest realizowane na podstawie umowy (na przykład *Linden Dollars*),
- pieniądz nie związany z innymi środkami płatniczymi, w których osoby trzecie nie mogą wysnuwać roszczeń o jego wykup,
- pieniądz będący roszczeniem o wykonanie usług (na przykład *timedollars*)[1064].

Oprócz formy gotówkowej, każda kolejna ma postać wirtualną, która w wybranych aspektach zostanie opisana w dalszych rozważaniach. Dyskutuje się o tym czy wirtualne środki pieniężne winny podlegać regulacji prawnej, a w szczególności przepisom prawa finansowego dotyczącego licencjonowania i nadzoru nad ich wydawcami. Za akceptacją tego stanowiska stoi ochrona uczestników obrotu wirtualnymi środkami pieniężnymi oraz zniwelowanie ryzyka wykorzystywania anonimowości obrotu do celów przestępczych[1065]. Pojawienie się nowych środków płatniczych niepodlegających regulacjom prawa finansowego było związane bezpośrednio z rozwojem technologii informatycznej. Na chwilę obecną w sposób całościowy uregulowane są jedynie pieniądze gotówkowe oraz pieniądze elektroniczne. Nieuregulowanym dotąd zagadnieniem są pieniądze wirtualne.

4.2.2.1. Pieniądz wirtualny

Życie społeczne i ekonomiczne toczy się w cyberprzestrzeni równolegle do tego w świecie rzeczywistym. Cyberprzestrzeń jednakże jako zupełnie inny obszar wymaga nieszablonowych rozwiązań, które niejednokrotnie tworzą się w sposób oddolny. Stworzenie alternatywnych środków płatniczych, wydawanych z inicjatywy użytkowników przestrzeni wirtualnej było zatem wyłącznie w kwestią czasu. Pojawienie się pieniędzy wirtualnych nazywanych też wirtualną walutą alternatywną w dużej mierze jest skorelowane ze światem gier wirtualnych.

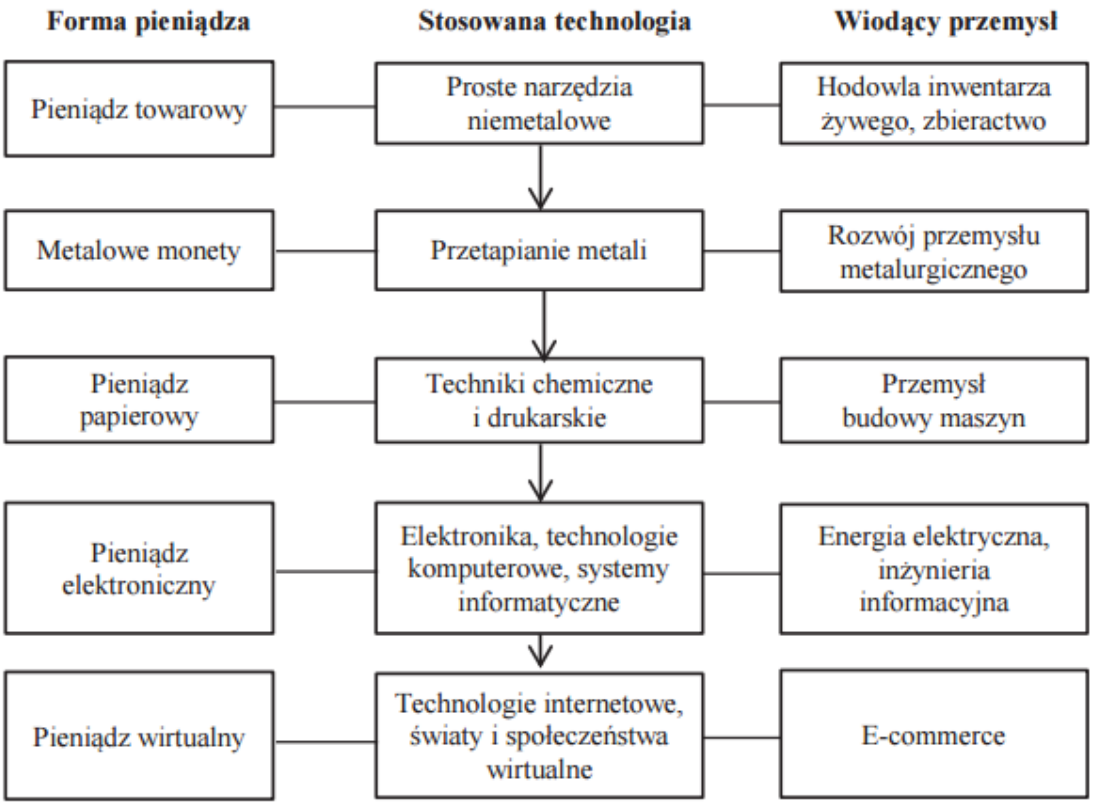
[1064] D. Cyman, *Pojęcie pieniądza i kierunki jego rozwoju*, [w:] Z. Ofiarski (red.), *XXV lat przeobrażeń w prawie finansowym i prawie podatkowym - ocena dokonań i wnioski na przyszłość*, Szczecin 2014, s. 687.
[1065] Ibidem, s. 689.

Intensywny rozwój cyfryzacji wpływający na tradycyjne mechanizmy rynkowe oraz ideę wprowadzenia jednej wspólnej światowej waluty niektórzy autorzy uznają za najwyższy stopień integracji państw w odniesieniu do polityki monetarnej[1066]. Mimo, iż jest to perspektywa bardzo odległa, to z całą pewnością należy obserwować nowy, ciekawy trend posługiwania się alternatywnymi środkami płatniczymi. Omawiana wirtualna waluta jest całkowicie niematerialna i działa tylko wyłącznie dzięki sieciom internetowym, bądź grom wirtualnym. Może jednak spełniać jak najbardziej realną funkcję płatniczą i być alternatywą dla tradycyjnego pieniądza[1067]. Handel walutami elektronicznymi przybiera na sile.

Zmiany oraz przekształcenia środków płatniczych na przestrzeni wieków, dostosowujące się do panujących warunków ekonomicznych i poziomu rozwoju ilustruje rysunek 14. Pojawienie się w cyberprzestrzeni alternatywnych metod płatności jest konsekwencją wzrostu znaczenia nowych technologii w gospodarce. Przedstawiciele piśmiennictwa stoją na stanowisku, że „ewolucja pieniądza jest naturalna i występuje od początku jego istnienia, będąc odpowiedzią na zmieniającą się sytuację gospodarczą. Tak samo naturalne jest, więc pojawienie się nowej kategorii pieniądza, który w świetle zupełnie nowych technologii stanowi odpowiedź liberalnej ekonomii na nową sytuację, jaką jest wykreowanie się gospodarki opartej na całkowitej swobodzie przepływu informacji i kapitału”[1068]. Pojawienie się nowych alternatywnych metod płatności jest już faktem. W cyberprzestrzeni wykształciły się elektroniczne formy wymiany, stworzone przez użytkowników dla użytkowników.

[1066] J. Ryfa, *Waluty wirtualne - problem zdefiniowania i klasyfikacji nowego środka płatniczego*, „Nauki o Finansach Financial Studies” 2014, nr 2(19), s. 138.
[1067] Ibidem, s. 138.
[1068] Ibidem, s. 139.

Rysunek 14. Proces przekształcenia środków płatniczych w pieniądz wirtualny



Źródło: J. Ryfa, op. cit., s. 140, za: Chen L., Wu H., *The Influence of Virtual Money to Real Currency: A Case-based Study*, Beijing University of Posts and Telecommunications, 2009 International Symposium on Information Engineering and Electronic Commerce s. 687.

Pieniądz wirtualny jest zagadnieniem bardzo młodym stąd też nie wypracowano jeszcze ogólno przyjętej definicji. Część autorów uznaje, że jest to: „jednostka będąca jednym z elementów określonego systemu pieniężnego, zapisana wyłącznie w formie elektronicznej, funkcjonująca w oparciu o zdecentralizowane bazy danych połączone ze sobą za pośrednictwem sieci Internet”[1069]. Z kolei Europejski Bank Centralny w 2012 roku, uznał, iż waluta wirtualna jest rodzajem nieregulowanych, cyfrowych pieniędzy, które są używane i akceptowane wśród członków określonej społeczności wirtualnej oraz emitowane przez jego twórców. Autorzy wskazują jednak, że definicja jest dość wąska i konieczna będzie jej zmiana w przyszłości[1070]. Jeszcze inną definicję formułuje Jakub Ryfa: „walutami wirtualnymi określa się specyficzną kategorię pieniądza elektronicznego, posiadającą co

[1069] J. Posyniak, *Bitcoin a aktualne uregulowania prawne środków płatniczych w Polsce*, [w:] Z. Ofiarski (red.), *XXV lat przeobrażeń w prawie finansowym i prawie podatkowym - ocena dokonań i wnioski na przyszłość*, Szczecin 2014, s. 821.
[1070] Europejski Bank Centralny, *Virtual Currency Schames*, Frankfurt am Main 2012, s. 13.

najmniej kilka subkategorii, opartego wyłącznie na zaufaniu użytkowników, przez co nie występuje oficjalna instytucja będąca jego gwarantem, pełniącego rolę środka wymiany i przechowywania wartości. Pieniądz ten jest wysoce elastyczny (podatny na udoskonalenia i modyfikacje), często dostosowany do najnowszych technologii internetowych, zapewniając wysoką mobilność i swobodę przepływu wartości bez pośrednictwa osoby trzeciej (np. bankowości internetowej). W zależności od swojej kategorii działa w obrębie bardzo wąskich granic – zamkniętego systemu (*closed-loop system*) – lub szeroko, w granicach zasięgu Internetu, dając możliwość swobodnej wymiany na inne waluty i zakup dóbr"[1071]. Jeszcze inni lapidarnie wskazują, że waluta wirtualna „nie jest pojęciem prawnym, a jedynie niejednorodnym zbiorem wielu różnych kryptowalut, których cechą wspólną jest przechowywanie za pomocą elektronicznego oprogramowania"[1072]. Inni autorzy wskazują na implikacje prawne waluty wirtualnej, którą można zdefiniować jako „odpowiednik pieniądza posiadający zdematerializowaną postać, będący przedmiotem obrotu wśród użytkowników sieci Internet, który wyróżnia brak krajowych i międzynarodowych aktów normujących jego kreację, obrót i kontrolę nad nim"[1073].

Europejski Bank Centralny wyróżnił dwa zasadnicze sposoby uzyskana walut wirtualnych. Pierwszy, najszybszy, polega na zakupie „prawdziwych" pieniędzy po odgórnie ustanowionym kursie wymiany. Wirtualna waluta nie opiera się zazwyczaj na towarze o realnej wartości. Drugim jest angażowanie czasu przez użytkowników, którzy nabywają walutę wirtualną poprzez reagowanie na akcje promocyjne, reklamowe, wypełnianie ankiet[1074].

Charakteryzując wirtualne pieniądze nie sposób jest nie wymienić ich klasyfikacji ze względu ma możliwość wymienialności na pieniądz realny. Europejski Bank Centralny podzielił tą klasyfikację na trzy kategorie:

> I kategoria - zamknięte systemy walut wirtualnych (ang. *closed virtual currency schemes*) - są to waluty wykorzystywane w masowych grach *on-line*, na przykład sztabki złota w grze World of Warcraft. Systemy te nie mają odniesienia do prawdziwej ekonomii i występują zazwyczaj wyłącznie w grach. Gracz płaci

[1071] J. Ryfa, op. cit. s. 141-142.
[1072] M. Mariański, *Problematyka kwalifikacji prawnej wirtualnej waluty we Francji*, „Państwo i Prawo" 2015, nr 10, s. 92.
[1073] P. Mackiewicz, M. Musiał, *Rozwój wirtualnych systemów monetarnych*, „Nauki o Finansach - Financial Sciences" 2014, nr 1(18), s. 135.
[1074] Europejski Bank Centralny, *Virtual Currency Schames*, Frankfurt am Main 2012, s. 13.

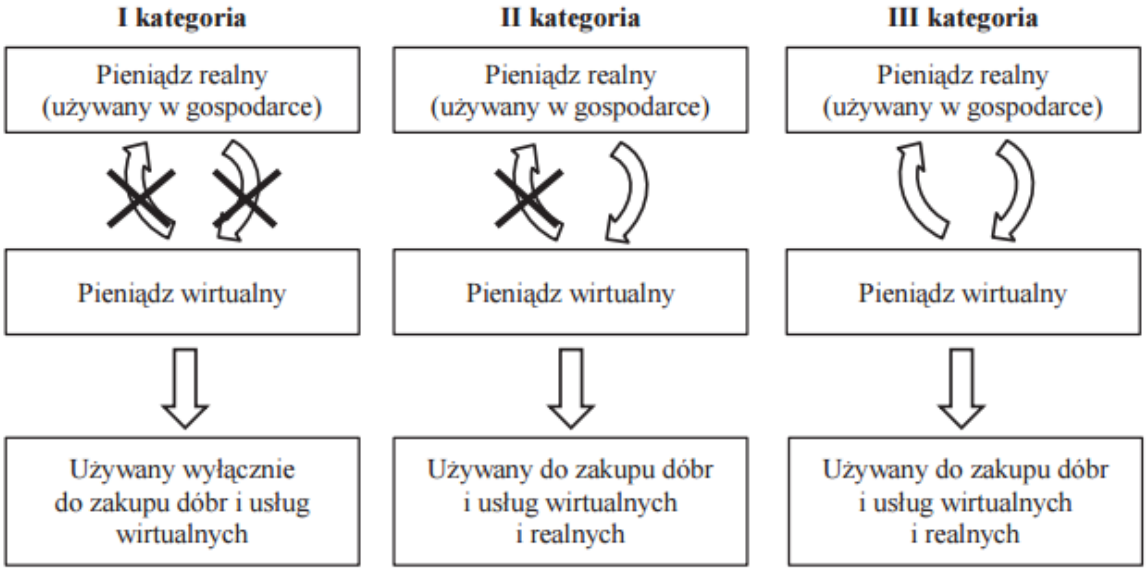
abonament i zarabia wirtualne pieniądze w oparciu o swoje wyniki w grze *on-line*. Waluta wirtualna może być wydawana tylko na zakup towarów i usług oferowanych w ramach społeczności wirtualnych.

II kategoria - systemy wirtualnej waluty z przepływem jednokierunkowym (ang. *virtual currency schemes with unidirectional flow*) - walutę wirtualną można kupić po określonym kursie bezpośrednio za pomocą prawdziwej waluty, jednakże nie może ona być wymieniona z powrotem. Programy umożliwiają zakup wirtualnych towarów i usług, a część z nich - prawdziwych zakupów w świecie realnym.

III kategoria - systemy wirtualnej waluty z przepływem dwukierunkowym (ang. *virtual currency schemes with bidirectional flow*) - użytkownicy mogą kupować i sprzedawać wirtualne pieniądze według kursów zgodnych z ich prawdziwą walutą. Za jej pomocą można nabywać wirtualne i realne dobra i usługi[1075].

Opisany wyżej podział przedstawiono na rysunku 12.

Rysunek 15. Kategorie pieniądza wirtualnego i mechanizm wymiany



Źródło: Europejski Bank Centralny, *Virtual Currency Schames*, Frankfurt am Main 2012, s. 15, tłumaczenie za: J. Ryfa, op. cit., s. 142.

Inny podział walut alternatywnych przyjmuje Robert Kurek. Wyróżnia on dwie kategorie - waluty kryptologiczne (kryptowaluty, kryptony, krypty), czyli *bitcoin*, *peercoin*,

[1075] Ibidem, s. 13 - 14.

goldcoin oraz waluty wykorzystywane w wirtualnych systemach płatności (nabywane za pomocą tradycyjnego pieniądza, a następnie wykorzystywane przy dokonywaniu transakcji w cyberprzestrzeni), tworzone przez platformy internetowe (na przykład *FacebookCredits*) czy używane w grach internetowych (gry typu *FarmVille, Seckond Life*)[1076].

Mimo zaprezentowanych powyżej różnych metod klasyfikacji, można wyróżnić pewne cechy wspólne dla pieniędzy wirtualnych. Są to:

- emitowanie pieniędzy wirtualnych przez społeczności następuje dla użytkowników cyberprzestrzeni, by mogli dokonywać działalności ekonomicznej w świecie wirtualnym,
- kreowanie pieniądza wirtualnego następuje przez popyt oraz ilość wirtualnej pracy wykonywanej przez użytkowników społeczności wirtualnej,
- ważną cechą waluty wirtualnej dla społeczności wirtualnej jest jego suwerenność,
- brak unormowań prawnych
- brak wirtualnego systemu wymiany walut wirtualnych pomiędzy różnymi społecznościami wirtualnymi,
- istnieje możliwości wymiany waluty wirtualnej na pieniądz elektroniczny bądź tradycyjny,
- pieniądz wirtualny jest używany i kreowany przez użytkowników społeczności wirtualnej, których anonimowość nie jest podkreślana[1077].

Pieniądz wirtualny ma nieuregulowany status prawny i nie należy go utożsamiać z pieniądzem elektronicznym. Główną różnicą jest to, że pieniądz elektroniczny ma podstawy prawne oraz zachowany jest związek z pieniądzem tradycyjnym, czyli pieniądze elektroniczne są przechowywane w określonej walucie na przykład euro. W wirtualnych systemach walutowych jednostka rozliczeniowa jest zamieniana na wirtualną (na przykład dolary Linder, Bitcoin'y). Ponadto, pieniądze elektroniczne są regulowane przez odpowiednie instytucje finansowe, które sprawują nad nimi nadzór ostrożnościowy. Zabezpieczeń takich brak jest w odniesieniu do pieniędzy wirtualnych, co znacznie zwiększa ryzyko oszustwa i manipulacji[1078]. Kolejną różnicą jest fakt, że zazwyczaj stosunkowo krótki jest okres

[1076] R. Kurek, *Alternatywne waluty wirtualne*, „Annales Universitatis Mariae Curie - Skłodowska" 2014, t. 48, nr 3, s. 191.
[1077] P. Mackiewicz, M. Musiał, op. cit., s. 137-138.
[1078] Europejski Bank Centralny, *Virtual Currency Schames*, Frankfurt am Main 2012, s. 16-17.

ważności pieniędzy wirtualnych - decyduje o tym emitent[1079]. Czynnikiem, który znacznie utrudnia regulację jest transgraniczny i światowy charakter internetowych usług płatniczych oraz niemal całkowita anonimowość użytkowników[1080]. W czym należy upatrywać wzrostu popularności pieniędzy wirtualnych? Wpływa na to kilka czynników: mniejsze koszty obrotu dla użytkownika (zazwyczaj nie pobiera się opłat transakcyjnych), niezależność od banków centralnych, globalnej gospodarki i wahań na rynkach walutowych. Pojawiają się też tezy, że potencjalnie pieniądz wirtualny może funkcjonować jako międzynarodowa waluta nieograniczona polityką fiskalną państw[1081].

Posługiwanie się wirtualnymi pieniędzmi jest obarczone dużym ryzykiem. Zagrożeniem jest niejasny status prawny, rozbieżności bądź brak jakiejkolwiek regulacji prawnej, możliwość dokonywania cyberprzestępstw (pranie brudnych pieniędzy, piramidy finansowe, nielegalne gry hazardowe, finansowanie cyberterroryzmu) czy też unikanie płacenia podatków. Brak jest odpowiednich form nadzoru nad emitowanymi pieniędzmi wirtualnymi. Dużym zagrożeniem są również waluty *peer - to - peer*, które nie posiadają jednego możliwego do skontrolowania ośrodka. Cecha ta zostaje wykorzystywana przez cyberprzestępców, którzy finansują zakup nielegalnych towarów na czarnym rynku walutami wirtualnymi takimi, jak Bitcoin. Stosowanie walut wirtualnych umożliwia omijanie przepisów prawnych regulujących chociażby kwestię hazardu. W 2007 roku rozgorzała dyskusja o wykorzystaniu pieniędzy wirtualnych w hazardzie po tym, jak FBI zamknęło kasyno, w którym działało w świecie wirtualnym *Second Life*. Wykorzystana w wirtualnej rzeczywistości waluta *Linden Dollar* była wymienialna na amerykańskie dolary, wobec czego wygraną w grze można było łatwo spieniężyć omijając tym samym stanowe i federalne regulacje dotyczące hazardu[1082]. Realnym zagrożeniem systemu pieniędzy wirtualnych jest też niebezpieczeństwo ataku hakerów, którzy włamując się do systemów mogą wytwarzać walutę wirtualną bez żadnych ograniczeń. Ponadto, brak odgórnych ograniczeń dotyczących ilości emisji waluty[1083].

[1079] T. Janyst, *Charakter prawny wirtualnych pieniędzy i formy ich regulacji. Analiza prawnoporównawcza*, [w:] A. Sztoldman (red.), *Prawo wobec innowacji technologicznych*, Warszawa 2013, s. 125.
[1080] D. Cyman, *Pojęcie …*, s. 690.
[1081] T. Janyst, op. cit., s. 126.
[1082] Ibidem, s. 139-141.
[1083] J. Guo, A. Chow, *Virtual Money System: a Phenomenal Analysis*, [w:] *10th IEEE International Conference on E-Commerce Technology (CEC 2008) / 5th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services*, IEEE, Waszyngton 2008, s. 270-271.

Według witryny monitorującej kapitalizację kryptowalut Crypto - Currency Market Capitalizations i danych przyjętych na kwiecień 2016 roku istnieją obecnie na rynku wirtualnym 680 waluty wirtualne, których łączna wartość wynosi ponad 8 miliardów dolarów[1084]. Obrót kryptowalutami zyskuje na popularności. Świadczyć może o tym fakt, iż dwa lata wcześniej walut tych było niemal trzykrotnie mniej, bo 236, a ich wartość szacowana była na 7 miliardów USD[1085]. W ciągu zaledwie dwóch lat obrót kryptowalutami zwiększył się o miliard dolarów.

Bitcoin

Chyba najbardziej znaną kryptowalutą jest bitcoin (skrótowo nazywany BTC), który według różnych źródeł powstał w 2008 roku bądź w 2009 roku. Jego twórcą jest Satoshi Nakamoto, lecz brak jest wiadomości czy jest to jeden podmiot czy może grupa osób[1086]. Bitcoin określany jest jako e-waluta drugiej generacji, kryptowaluta czy waluta wirtualna[1087], jest on „pierwszym cyfrowym, prywatnym pieniądzem, którym dokonuje się rozliczeń bezpośrednio między stronami (ang. *peer to peer*), bez konieczności korzystania z rachunków (bankowych lub niebankowych). Nie jest on wydawany, zarządzany, administrowany, monitorowany ani rozliczany przez jakąkolwiek jednostkę organizacyjną. Podstawowym założeniem funkcjonowania tej kryptowaluty jest to, że została ograniczona ilość wydanych jednostek bitcoin do 21 milionów. Nawiązuje więc do teorii monetarnych, a wartość bitcoin opiera się wyłącznie na popycie i podaży. Pieniądz ten jest niezależny od któregokolwiek z krajów, instytucji czy jakiejkolwiek innej waluty"[1088].

Bitcoinami można dokonywać wszelkiego rodzaju transakcji - płacić zarówno za wirtualne jak i realne dobra i usługi. Co istotne, liczba jednostek bitcoin została ograniczona w algorytmie programu do 21 milionów. Bitcoiny wprowadzane są na rynek stopniowo[1089].

[1084] Oficjalna strona interetowa Crypto- Currency Market Capitalizations https://coinmarketcap.com/all/views/all/ [19.04.2016].
[1085] R. Kurek, op. cit., s. 192.
[1086] J. Posyniak, op. cit., s. 821.
[1087] E. Chrabonszczewska, *Bitcoin - nowa wirtualna globalna waluta?,* „Zeszyty Naukowe Kolegium Gospodarki Światowej SGH" 2013, nr 40, s. 52.
[1088] D. Cyman, *Pojęcie…*, s. 686-687.
[1089] A. Roszyk, *Świat przyjmuje walutę bitcoin*, „Prawo i Podatki" 2015, nr 121, s. 2.

Przyjmuje się, że liczba 21 milionów zostanie osiągnięta około roku 2033[1090]. Każdy bitcoin dzieli się na 100 mln części, a ceny w nim wyrażone mogą mieć 8 miejsc po przecinku, co oznacza, że najmniejszą jednostką jest 0,00000001 BTC[1091].

Wejść w posiadanie bitcoinów można na dwa sposoby. Pierwszy - prostszy z nich - polega na wymianie dowolnej waluty na bitcoiny w jednym z internetowych kantorów bądź internetowych domach aukcyjnych. Działanie to odpowiada zakupowi normalnej waluty na przykład euro czy dolarów. Drugim ze sposobów jest zarabianie bitcoinów w procesie tak zwanego „wydobycia" (ang. *mining*). Grzegorz Rosłan i Marek P. Stolarski szczegółowo przedstawiają techniczny proces wydobycia bitcoinów[1092], który w skrócie można opisać jako poświęcanie mocy obliczeniowej własnego komputera przez użytkownika, który to proces przyczynia się do powstania nowych bitcoinów. W ogólnie dostępnym oprogramowaniu znajduje się cała historia transakcji bitcoinami - od jego powstania do chwili obecnej. Każda nowa transakcja jest autoryzowana przez system, który sprawdza dotychczasową historię transferów. Tak skonstruowany program (tak zwany łańcuch bloków ang. *blockchain*) ma zapobiec fałszerstwom, jeżeli pojawi się nieautoryzowany bitcoin, nie zostanie dopuszczony do transakcji[1093]. System bitcoin w swej pracy wykorzystuje dwa rodzaje kluczy kryptograficznych - publiczny i prywatny. Klucz publiczny ma służyć do identyfikacji właściciela bitcoinów, z kolei klucz prywatny umożliwia mu korzystanie z posiadanych środków.

Bitcoin charakteryzuje się kilkoma cechami: występuje wyłącznie w Internecie, transakcje między użytkownikami są rozproszone i nie są przechowywane w jednym centralnym serwerze, waluta jest całkowicie zdecentralizowana, tworzona przez samych użytkowników bez pośrednictwa jakiegokolwiek banku czy instytucji, nie ma formy

[1090] E. Chrabonszczewska, op. cit., s. 60.
[1091] Ibidem, s. 54.
[1092] „Przygoda w wirtualną walutą rozpoczyna się od pobrania ze strony umieszczonej pod nazwą bitcoin.org standardowego oprogramowania klienckiego, które wydawane jest w wariantach dla popularnych systemów operacyjnych (Windows, GNU/Linux i Mac OS X). Po uruchomieniu program pobiera łańcuch bloków, czyli listę zbiorów wszystkich potwierdzonych transakcji od początku istnienia sieci. Trwa to około 2 dni (zakładając użycie łącza o maksymalnej przepustowości 2 Mbit/s), choć większość czasu nie zajmuje pobieranie, ale sprawdzanie cyfrowych poświadczeń każdego bloku. Równolegle do procesu pobierania bazy można zacząć tworzyć pary kluczy, które staną się adresami Bitcoin, czyli wirtualnymi rachunkami. Gdy łańcuch bloków znajdzie się na dysku, użytkownik może wysyłać i odbierać płatności korzystając z wirtualnego portfela, opcjonalnie zabezpieczanego szyfrem symetrycznym pod postacią hasła. Dla lubiących ryzyko istnieją też portfele utrzymywane w obrębie usług webowych działających w Internecie, jednak za wygodę dostępu do środków z każdego miejsca płaci się obniżonym poziomem bezpieczeństwa". G. Rosłan, M.P. Stolarski, *Cyfrowa waluta Bitcoin - nowe zagrożenie dla systemu finansowego*, cz. 2, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie" 2014, nr 2(27), s. 275-276.
[1093] A. Roszyk, op. cit., s. 2.

materialnej ani prawnego unormowania. Co więcej waluta ta ma ogólnoświatowy zasięg, a część sklepów internetowych i innych podmiotów zaczyna akceptować bitcoin jako formę zapłaty. Koszty użycia waluty są wyjątkowo niskie, ponieważ brak jest opłat transakcyjnych, transakcje są anonimowe i nie pozostawiają za sobą śladu, a fakt, iż środki finansowe nie są przechowywane w instytucji typu bank powoduje, że mamy dostęp do wirtualnych pieniędzy zawsze, gdy tylko uzyskamy dostęp do Internetu[1094]. Oczywiste jednak jest, że bitcoin nie może być uznany za środek płatniczy - nie ma mocy umarzania zobowiązań. Spełnienie świadczenia w tej wirtualnej walucie może nastąpić wyłącznie na mocy porozumienia stron.

Posługiwanie się walutą bitcoin mimo wielu zalet, jak każda nowinka techniczna, determinuje pewne zagrożenia. Wśród zagrożeń technicznych należy wymienić chociażby następujące. Użytkownik przechowuje bitcoiny na dysku twardym swego komputera, co oznacza, iż w przypadku potencjalnego ataku hackera może on utracić zgromadzone środki finansowe albo przez zniszczenie pliku portfela bądź nieautoryzowany przelew środków. Sieć bitcoin, tak jak każda usługa sieciowa, podatna jest na ataki hackerskie związane ze śledzeniem transakcji czy też związanie z ograniczeniem dostępu do sieci, czyli ataki DoS bądź DDoS. Co więcej istnieje możliwość zawarcia w danych transakcji dodatkowych danych (na przykład pliki obrazów, informacje tekstowe). Dokonując przelewu płatności jest możliwe zatem przeprowadzenia „zatrutej" transakcji (zawierającej oprócz samych danych transakcji dodatkowe pliki zakazane przez ustawodawstwo jakiegoś kraju na przykład pornografii dziecięcej) i tym samym zdyskredytowania użytkownika. Wśród zagrożeń o charakterze ekonomicznym wymienia się możliwość spekulowania wartością, brak unormowań prawnych, nieodwracalność transakcji[1095].

Brak jest też międzynarodowych, europejskich czy też polskich uregulowań funkcjonowania bitcoin'ów. W oświadczeniu z 28 czerwca 2013 roku Minister Finansów oświadczył, że funkcjonowanie oraz obrót wirtualnymi walutami nie zostało uregulowane wobec czego nie narusza ani polskiego ani unijnego prawa[1096]. Z kolei Dyrektor Izby Skarbowej w Warszawie wskazał w interpretacji wydanej dla podatnika, że sprzedaż bitcoinów jest usługą i trzeba za nią zapłacić podatek VAT[1097]. Ciężko jest jednoznacznie określić jak będzie wyglądać przyszłość tej wirtualnej waluty - prorokować można wielki

[1094] E. Chrabonszczewska, op. cit., s. 54-55.
[1095] G. Rosłan, M.P. Stolarski, op. cit., s. 276-285.
[1096] Oświadczenie Ministra Finansów http://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/dokumenty/stenogram/oswiadczenia/klima/3001oa.pdf
[1097] Dane z portali Dziennik Internautów Biznes i Prawo: http://di.com.pl/polak-sprzedaje-bitcoiny-swiadczy-usluge-i-ma-zaplacic-vat-50325 [10.03.2017].

sukces jak i wielką klęskę, która ścieżka zostanie zrealizowana zależy do wielu czynników takich, jak wzmocnienie bezpieczeństwa transakcji, wprowadzenie uregulowań prawnych czy zaufania społecznego.

Wskazać trzeba, że nie można zastopować procesu tworzenia się pieniędzy i walut wirtualnych. Proces ten w krótkim czasie stworzył realne ramy obrotu jak najbardziej realnych środków finansowych. Wskazuje się, że dopóki alternatywne środki płatnicze nie staną się ekwiwalentem pieniądza w tradycyjnym znaczeniu będą miały status „umownego środka płatniczego zamkniętej grupy społecznej"[1098]. Prawo nie powinno zostać obojętne tworzącemu się zjawisku, które w obecnej formie podatne jest na zagrożenia. Wydaje się, że państwa winny wprowadzić chociażby minimalne standardy, które będą regulowały kwestie, czyli obowiązek rejestracji walut wirtualnych, określenie sposobu zakupu, standardy bezpieczeństwa, prawa użytkowników czy ograniczenia w możliwości korzystania z walut do określonych portali czy gier.

4.3 Własność intelektualna w cyberprzestrzeni a prawo międzynarodowe

Cyberprzestrzeń prowadzi do powstania nowych wyzwań również w zakresie własności intelektualnej. Nieograniczony dostęp do sieci umożliwia pełne korzystanie z dobrodziejstw kultury i sztuki, więc z utworów chronionych prawami autorskimi. W większości przypadków korzystanie z utworów znajdujących się w przestrzeni wirtualnej nie jest kontrolowane, wobec czego niejednokrotnie prowadzi do nadużyć. Problem ten jest powszechny i występuje w skali globalnej.

Głównymi, lecz nie jedynymi, problemami kwestii własności intelektualnej w przestrzeni jest cyfrowej: ustalenie jurysdykcji właściwej do czynności faktycznych i prawnych, trudności uzyskania ochrony autorskoprawnej, rozpowszechnianie utworów w sieci różniące się od dotychczasowych paradygmatów działalności wydawniczej oraz kwestia zarządzania prawami autorskimi i pokrewnymi. Coraz częściej pojawiają się postulaty

[1098] R. Kurek, op. cit., t. 48, 3, s. 194.

ograniczenia dopuszczalności umownego ograniczenia eksploatacji utworów w zakresie w jakim ma to miejsce w licencjach umownych, czy też zawężaniem dotychczasowych granic dozwolonego użytku osobistego w sieciach komputerowych. Szybki i ciągły rozwój technologii informatycznych powoduje, iż pojawiają się nowe aplikacje czy też narzędzia (chociażby chmura obliczeniowa[1099]), które powodują pytania o charakter czasowy publikacji elektronicznych, czyli o ich dopuszczalność i zasady archiwizacji zapisów[1100].

Magdalena Kowalczuk-Szymańska i Olga Sztejnert-Roszak wśród podstawowych rodzajów naruszeń praw autorskich w Internecie wymieniają: kopiowanie treści stron internetowych (obrazów, tekstu, plików wideo) oraz skanowania publikacji i artykułów, by następnie udostępnić je *on-line* w formacie .pdf. Konieczne jest zawarcie umowy z właścicielem autorskich praw majątkowych, żeby zgodnie z prawem zamieścić i rozpowszechniać takie treści w cyberprzestrzeni[1101]. Jedną z popularniejszych metod naruszenia praw autorskich jest nielegalne ściąganie utworów z sieci. Piractwo muzyki, filmów i gier komputerowych jest zjawiskiem nagminnym, a anonimowość w sieci dodatkowo utrudnia wykrycie i skazanie sprawcy oraz dochodzenie innych praw należnych twórcom[1102].

Problematyka własności intelektualnej w przestrzeni wirtualnej jest zagadnieniem niezwykle szerokim i złożonym, w związku z czym w niniejszej dysertacji zostanie ograniczona jedynie do wskazania podstawowych interesujących zagadnień w tym przedmiocie. W podrozdziale zostaną omówione aktualne problemy związane z własnością intelektualną w cyberprzestrzeni - związane z nowymi metodami naruszeń, chmurą obliczeniową czy samymi stronami internetowymi. Wskazać w tym miejscu należy, iż nie będzie to opracowanie holistyczne, ponieważ temat własności intelektualnej jest na tyle obszerny, że mógłby stanowić podstawę odrębnej rozprawy doktorskiej.

[1099] Chmura obliczeniowa (ang. *cloud computing*) - model przetwarzania danych, opierający się na użytkowaniu usług, programów komputerowych, a także infrastruktury i narzędzi dostarczanych przez usługodawcę.
[1100] J. Barta, R. Markiewicz, *Prawo autorskie,* Warszawa 2016, s. 461- 463.
[1101] M. Kowalczuk-Szymańska, O. Sztejnert-Roszak, *Naruszenia praw autorskich w Internecie*, Warszawa 2011, s. 27-29.
[1102] Ibidem, s. 33.

4.3.1 Przedmiot ochrony

Na początku należy postawić sobie pytanie czym jest własność intelektualna. W znaczeniu węższym są to utwory z zakresu prawa autorskiego, w zakresie szerszym są to utwory prawa autorskiego, prawa pokrewnego i prawa własności intelektualnej[1103]. W Konwencji o ustanowieniu Światowej Organizacji Własności Intelektualnej, sporządzonej w Sztokholmie 14 lipca 1967 roku[1104], za własność intelektualną uznano w art. 2 ust. viii) prawa odnoszące się do: dzieł literackich, artystycznych i naukowych, interpretacji artystów interpratorów oraz do wykonań artystów wykonawców, do fonogramów i do programów radiowych i telewizyjnych, wyznalazków we wszystkich dziedzinach działalności ludzkiej, odkryć naukowych, wzorów przemysłowych, znaków towarowych i usługowych, jak również do nazw handlowych i oznaczeń hanlowych, ochrony przed nieuczciwą konkurencją oraz wszelkie inne prawa dotyczące działalności intelektualej w dziedzinie przemysłowej, naukowej, literackiej i artystycznej. W porozumieniach TRIPS[1105] ogólnie za własność intelektualną uznano: prawa autorskie i pokrewne, programy komputerowe i zbiory danych, ochronę wykonawców, producentów fonogramów (nagrań dźwiękowych) i organizacji nadawczych, znaki towarowe, oznaczenia geograficzne, wzory przemysłowe i patenty, topografie układów scalonych, informacje nieujawnione.

Zgodnie z poglądem Wiesława Kotarby „określenie własność intelektualna należy odnosić (...) do wszelkich dóbr niematerialnych, będących wytworem intelektu chronionych prawem. (...) Pod pojęciem własności intelektualnej będziemy rozumieć własność ustanowioną prawem na dobrach niematerialnych, będących wytworami ludzkiego intelektu, posiadającą określony zakres podmiotowy, czasowy i terytorialny”[1106]. Przedstawiciele doktryny za dobra niematerialne uznali: „wytwory szeroko pojętej twórczości, będące przede wszystkim efektem nagromadzonej wiedzy, umiejętności postrzegania i interpretacji określonych zdarzeń i relacji pomiędzy nimi w otaczającym nas świecie”[1107].

[1103] D.G. Żak, *Wybrane formy naruszeń prawa własności intelektualnej w Internecie*, [w:] D. Żak, *Własność intelektualna w sieci*, Lublin 2014, s. 198.
[1104] Dz. U. z 1975 r., Nr 9, poz. 49.
[1105] Porozumienie w sprawie handlowych aspektów praw własności intelektualnej (ang. *Agreement on Trade-Related Aspects of Intellectual Property Rights*- TRIPS).
[1106] W. Kotarba, *Ochrona własności intelektualnej*, Warszawa 2012, s. 14.
[1107] Ibidem, s. 14.

Janusz Barta i Ryszard Markiewicz podkreślają, iż pojęcie własność intelektualna jest używana w konwencjach międzynarodowych oraz w nazwie Światowej Organizacji Własności Intelektualnej, jako termin nawiązujący do „własności rzeczy", w głównej mierze z powodu przyjętej konstrukcji bezwzględnych praw podmiotowych. Podkreślają, że „dobra niematerialne, ze względu na sposób ich istnienia, są eksploatowane z innymi jednak skutkami niż rzeczy (ze względu na możliwość korzystania z nich równolegle przez nieokreśloną liczbę podmiotów), co przesądza o innym modelu ich ochrony, zbliżonym jednak do ochrony własności"[1108]. Podstawowym zadaniem praw własności intelektualnej jest „zabezpieczenie interesów podmiotów w odniesieniu do charakterystycznej grupy przedmiotów jakimi są wytwory ludzkiego intelektu"[1109]. Inni znawcy tematu podnoszą, że „własność intelektualna jest ściśle związania z procesami tworzenia, rozwijania i wykorzystywania zdobytej wiedzy stanowi wynik ludzkiej twórczości i kreatywności, opiera się na inwencji i pomysłach. Należy tu podkreślić, iż środki służące procesowi twórczości także stanowią przedmiot ochrony. Technologia jako proces prowadzący do powstania określonego dobra jest chroniona jako odrębne dobro. Przykładowo może to być informacja, zastosowane rozwiązanie, wynalazek. Z kolei nowe technologie mogą wpływać na zakres i sposób ochrony danego dobra i przyczynić się do powstania zagrożeń dla tej ochrony, poczynając od trudności interpretacyjnych do dezaktualizacji jej reguł, czego przykładem może być problematyka korzystania z utworów w sieci internetowej. Nowe sposoby korzystania z utworów wymagają nowych regulacji"[1110]. Pogląd ten stanowi znakomity punkt wyjścia do dalszych rozważań na temat.

Przedmiotem ochrony własności intelektualnej w cyberprzestrzeni są utwory cyfrowe (z różnych dziedzin sztuki i kultury) stworzone w wersji cyfrowej lub które przeszły proces konwersji cyfrowej (w przypadku utworów, pierwotnie stworzonych w wersji analogowej) i mogą być rozumiane jako produkty multimedialne[1111]. Utwory udostępnianie w sieci, czyli produkty medialne, łączą elementy z różnych dziedzin sztuki (obraz, film, słowo, muzyka) w formie zapisu cyfrowego. Ich cechą specyficzną jest interaktywność oraz specyficzna relacja zachodząca pomiędzy elementami składowymi dzieła[1112].

[1108] J. Barta, R. Markiewicz, *Prawo autorskie i prawa pokrewne*, Warszawa 2014, s. 17.
[1109] D.G. Żak, op. cit., s.198.
[1110] K. Chałubińska-Jentkiewicz, *Własność intelektualna jako szczególny rodzaj własności w „sieci",* [w:] K. Chałubińska-Jentkiewicz, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 183.
[1111] Ibidem, s.190.
[1112] J. Barta, R. Markiewicz, *Prawo autorskie,…*, s. 464.

Produkty te są udostępniane bezpośrednio w przestrzeni wirtualnej, ale również poza nią, w formie na przykład płyt CD. Odpowiednie ich sklasyfikowanie budzi wątpliwości w polskiej doktrynie - niejasne jest czy należy je uznać za dzieła audiowizualne, bazy danych czy też tworzą odrębny, samodzielny rodzaj utworów. Na przykładzie gier komputerowych Janusz Barta i Ryszard Markiewicz wskazują, że: „gry komputerowe z reguły składają się z dwóch możliwych do wyodrębnienia składników: programu komputerowego i wyznaczonego przez niego interfejsu dla użytkownika, który w przypadku współczesnych gier komputerowych ma najczęściej właściwości utworu audiowizualnego. Uzasadnia to bezpośrednie stosowanie odpowiednich części gier komputerowych i przepisów dotyczących programów komputerowych i utworów audiowizualnych. Mając świadomość wątpliwości wiążących się z taką oceną, uważamy, że gry komputerowe - oceniane całościowo - to hybrydowe, *sui generis* utwory. Stanowisko to potwierdza orzeczenie Sądu Najwyższego we Włoszech, w którym stwierdzono, że gry komputerowe różnią się od programów komputerowych i są bardziej od nich złożone; nie mogą być także porównywalne do mediów, które zawierają ruchome obrazy”[1113]. Rozważania autorów sprowadzają się do stwierdzenia, że w przypadku braku możliwości podporządkowania jednego utworu całkowicie do określonego dzieła multimedialnego, należy stosować te regulacje, które są najbardziej zbliżone do utworu podstawowego w konkretnym dziele multimedialnym. Stanowisko to aprobuje również Katarzyna Chałubińska - Jentkiewicz akcentując, iż pozostaje ono aktualne w obliczu ciągłego rozwoju nowych technologii, które powodują konieczność innowacyjnej interpretacji przyjętych już reguł[1114].

4.3.2. Naruszenie praw autorskich - piractwo komputerowe

Naruszenie praw autorskich za pomocą przestrzeni wirtualnej to nie tylko nielegalne ściąganie muzyki i filmów. Zwiększony obrót e-commerce umożliwił nielegalny handel podrobionymi towarami i piractwo na nieznaną dotąd skalę. Jak podnosi Jerzy Kosiński w cyberprzestrzeni lawinowo rośnie liczba podrabianych leków, wyrobów medycznych, części

[1113] Ibidem, s. 464-466.
[1114] K. Chałubińska-Jentkiewicz, *Własność …*, s.190.

samochodowych niewiadomego pochodzenia. Często dochodzi do podrobienia wyrobów tytoniowych i spirytusowych - a tym samym naruszenia praw własności intelektualnej produkujących je koncernów. Dużym problemem okazuje się również podrabianie produktów, czyli zabawki, które nie spełniają wymogów i norm bezpieczeństwa[1115].

W doktrynie wyróżnia się kilka podstawowych mechanizmów przestępczego naruszania praw własności intelektualnej w cyberprzestrzeni. Jerzy Kosiński uważa, że są to między innymi:

- „Oferty sprzedaży oraz rozpowszechnianie plików chronionych za pośrednictwem stron internetowych.
- Rozpowszechnianie plików za pomocą serwerów ftp[1116]. Znaczącym problemem są tzw. grupy warezowe (zorganizowane grupy, które za pośrednictwem serwerów ftp wymieniają filmy, muzykę, programy komputerowe czy też książki elektroniczne). Często serwery ftp z plikami umieszczane są w sieciach lokalnych tylko dla własnych abonentów.
- Nielegalne rozpowszechnianie utworów za pośrednictwem serwerów tzw. magazynów plików. Coraz większą popularnością cieszą się serwery, na które przesyłane są duże liczby plików, aby następnie mogły być one pobierane przez innych użytkowników.
- Wymianę utworów za pośrednictwem sieci *peer to peer* (p2p). Proceder ten polega na udostępnianiu plików za pomocą programów dedykowanych do sieci zcentralizowanych i zdecentralizowanych, np. kazaa, e-donkey, emule, torent, azeurus. Użytkownik Internetu może wyszukiwać w sieci komputery z udostępnioną zawartością i ściągać stamtąd pirackie kopie, jednocześnie rozpowszechniając zasoby własne.
- Rozpowszechnianie plików za pośrednictwem kont poczty elektronicznej *peer to mail* (p2m), tj. za pomocą odpowiednich programów (plik jest dzielony i przesyłany na konto e-mail). Informacja o tytułach utworów umieszczana jest na zamkniętych forach dyskusyjnych, na których znajduje się informacja o loginach i hasłach do kont, haseł do scalenia oraz rozpakowania plików.

[1115] J. Kosiński, *Wstęp*, [w:] idem (red.), *Internetowe naruszenia własności intelektualnej 2015*, Szczytno 2016, s. 6-7.
[1116] Serwer ftp - serwer umożliwiający wymianę plików z komputerami za pomocą protokołu komunikacyjnego FTP.

- Tak zwany *sharing* platform cyfrowych pozwalających na współdzielenie sygnału telewizyjnego oraz abonenta w sposób bezprawny, często po wpłaceniu określonej kwoty pieniężnej.
- Rozpowszechniania plików umożliwiających kradzież sygnału telewizyjnego przez internetowe downloady z kodami pozwalającymi na podbicie pakiety podstawowego do pełnego"[1117].

Metody oraz rodzaje naruszeń praw własności intelektualnych są liczne. Walka z piractwem internetowym jest niebywale trudna, ponieważ wymiana plików następuje transgranicznie, za pomocą specjalnych programów, a w miejsce jednej zamkniętej strony do wymiany plików po kilku dniach powstaje kilka kolejnych. Z tych też względów Urząd Unii Europejskiej oraz Europol w celu walki z podróbkami oraz piractwem komputerowym *on -line* i *off -line* utworzył koalicję o nazwie Intellectual Property Crime Coordination Centre (IPC3). W ocenie Jerzego Kosińskiego IPC3 zapewni organom ścigania wsparcie techniczne oraz koordynacyjne koordynowaniu dochodzeń transgranicznych, monitorowaniu trendów przestępczości, zwiększanie harmonizacji i standaryzacji unormowań prawnych i organizacyjnych, efektywniejsze egzekwowanie prawa oraz podnoszenie świadomości społeczeństwa w zakresie własności intelektualnej w przestrzeni cyfrowej[1118].

Walka z piractwem komputerowym może być prowadzona przez ściganie użytkowników, którzy nielegalnie ściągają pliki z sieci, bądź też przez walkę z podmiotami, które nielegalnie te treści rozpowszechniają. Ryszard Markiewicz przedstawia trzy alternatywne próby rozwiązania problemu piractwa w cyberprzestrzeni:

- koncepcja pierwsza - rozszerzenie obowiązujących regulacji w taki sposób, by umożliwić wydanie sądowego orzeczenia o zakazie świadczenia usługi dostępu do określonych nielegalnych stron internetowych oraz zakazującego dalszego utrzymywania platformy hostingowej, która jest wykorzystywana głównie do naruszania cudzych praw autorskich, a działanie sprawcy ma charakter zawiniony,
- koncepcja druga - przewiduje legalizację swobodnego rozprzestrzeniania utworów w cyberprzestrzeni; byłoby to możliwe po spełnieniu kilku warunków: dotyczyłoby to tylko uprzednio rozpowszechnionych utworów, osoba rozpowszechniająca nie mogłaby działać w celu osiągnięcia korzyści majątkowej, a osoby korzystające z ochrony praw autorskich miałyby zapewnione odpowiednie wynagrodzenie,

[1117] J. Kosiński, *Wstęp*…, s. 7-8.
[1118] Ibidem, s. 6.

- koncepcja trzecia - utrzymanie *status quo* - które jest argumentowane tym, że właśnie słabe zabezpieczenie praw autorskich wymusza na autorach stworzenie atrakcyjnego dla konsumentów, w miarę taniego systemu udostępniania utworów[1119].

Zwalczanie przestępczości związanej z naruszeniem praw własności intelektualnej jest kluczowym priorytetem w ochronie konsumentów przed niebezpiecznymi produktami oraz elementem eliminacji sieci przestępczych zajmujących się tym procederem. Europol podaje, że podczas międzynarodowej skoordynowanej operacji przeprowadzonej przez ten urząd w 2015 roku ujawniono i zajęto ponad tysiąc stron nielegalnie sprzedających podrobiony towar nieświadomym konsumentom[1120]. Działania operacyjne Europolu ujawniły, jak ogromna jest skala naruszeń znaków towarowych oraz piractwa internetowego w handlu elektronicznym.

4.3.3. Programy komputerowe

Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE w sprawie ochrony prawnej programów komputerowych za program komputerowy uznaje program w jakiejkolwiek formie, w tym program zintegrowany ze sprzętem komputerowym. Ten akt zakresem pojęciowym obejmuje w pkt. 7 również przygotowawcze prace projektowe prowadzące do rozwoju programu komputerowego z tym jednak zastrzeżeniem, że charakter prac przygotowawczych jest taki, że program komputerowy może korzystać z nich na późniejszym etapie. Dyrektywą 2009/24/WE przyznano programom komputerowym taką samą ochronę prawem autorskim, jaką przyznaje się dziełom literackim w rozumieniu konwencji berneńskiej. Ochrona jest przyznana, o ile program komputerowy nosi znamiona oryginalności, w takim rozumieniu, że jest własną intelektualną twórczością jego autora. Autorstwo przysługuje twórcy programu komputerowego, a jeżeli program stworzyło kilka osób - autorstwo przysługuje im wspólnie, chyba że program został stworzony w ramach wykonywania obowiązków służbowych, wówczas prawa do utworu przysługują pracodawcy.

[1119] R. Markiewicz, *Internet i prawo autorskie - wykaz problemów i propozycje ich rozwiązań*, „Prace z Prawa Własności Intelektualnej" 2013, z. 2 (121), s. 13-14.
[1120] Dane z oficjalnej strony internetowej Europolu: https://www.europol.europa.eu/newsroom/news/fighting-intellectual-property-crime [12.12.2016].

Do polskiego porządku prawnego wprowadzono rozwiązania wzorowane na tych postanowieniach. Mimo, że polska ustawa o prawie autorskim i prawach pokrewnych nie zawiera definicji programu komputerowego, to powszechnie uznaje się go za utwór. W doktrynie wyrażany jest pogląd, iż ochronie podlegać będzie też dokumentacja i inne materiały dotyczące programu komputerowego, co zresztą odpowiada przytoczonemu wyżej zapisowi dyrektywy 2009/24/WE o pracach projektowych[1121]. Część autorów proponuje swoje definicje terminu program komputerowy. Aurelia Nowicka uznaje, że jest to: „zestaw instrukcji (rozkazów), przeznaczonych do użycia bezpośrednio lub pośrednio w komputerze w celu osiągnięcia określonego rezultatu"[1122]. Podobnie program komputerowy definiuje Jerzy Szczotka: „zbiór instrukcji (poleceń/ rozkazów) przedstawionych w języku zrozumiałym dla urządzenia technicznego (komputera); ich realizacja przez komputer ma umożliwić osiągnięcie określonych przez twórcę programu celów"[1123]. Najobszerniejszą charakterystykę proponuje Michał Skwarzyński, według którego jest to: „zbiór instrukcji (kod źródłowy), które po umieszczeniu na rozpoznawalnym przez maszynę nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tej maszyny (kod wynikowy) powoduje, że osiąga zdolność do wykonywania danej czynności lub też wykonuje daną czynność; nie stanowi cyfrowego zapisu innego utworu"[1124].

Problemu może nastręczyć kwestia określenia granicy pomiędzy chronionymi i niechronionymi elementami programów komputerowych. Ochrona prawnoautorska nie będzie ograniczać się jedynie do literalnych elementów, czyli kodu źródłowego oraz kodu obiektowego, ale również będzie zawierać inne elementy charakteryzujące się wyrazem twórczości autora. Ochronie z kolei nie podlegają elementy „pozatekstowe" takie, jak algorytm, struktura programu, język programowania czy funkcje[1125].

Janusz Barta oraz Ryszard Markiewicz stoją na stanowisku, że: „treść autorskich praw majątkowych do programu komputerowego jest w istocie szersza niż przewidziana dla innych utworów. Wynika to z omówionego niżej odrębnie zakazu dekompilacji programów, a także z:

[1121] J. Barta, R. Markiewicz, *Prawo autorskie…*, s. 296-297.
[1122] A. Nowicka, *Prawnoautorska i patentowa ochrona programów komputerowych*, Warszawa 1995, s. 11.
[1123] J. Szczotka, *Przepisy szczególne dotyczące niektórych utworów*, [w:] M. Poźniak - Niedzielska (red.), *Prawo autorskie i prawa pokrewne*, Bydgoszcz-Warszawa-Lublin 2007, s. 149.
[1124] M. Skwarzyński, *Przestępstwa uzyskania programu komputerowego - art. 278 § 2 k.k.*, „Palestra" 2010, nr 3, s. 35.
[1125] J. Barta, R. Markiewicz, *Prawo autorskie…*, s. 297.

a) ustanowienia, w ramach praw majątkowych, uprawnienia do wprowadzania zmian do programu, nawet w tych sytuacjach, w których nie wiąże się to ze zwielokrotnianiem programu; można uznać, że osobiste prawo do integralności utworu zostało przy programach komputerowych »przesunięte« do grupy autorskich praw majątkowych oraz »wzmocnione« poprzez objęcie monopolem autorskim także samej czynności dokonywania zmian;
b) całkowitego wyłączenia dozwolonego użytku osobistego względem programów komputerowych, co równocześnie przesądza o tym, że monopolem autorskim objęte zostaje już samo dokonywanie opracowań programu lub wyprowadzanie innych zmian wiążących się ze zwielokrotnieniem;
c) regulacji wyznaczającej dopuszczalne granice dokonywania dekompiliacji i korzystania z jej wyników;
d) niestosowania w odniesieniu do programów części przepisów regulujących dozwolony użytek publiczny"[1126].

Zagadnienie programu komputerowego, jego autorstwa, ograniczeń oraz licencji upoważniających do korzystania z niego jest zagadnieniem szczególnie złożonym[1127]. Prawo staje również w obliczu wyzwań związanych z ciągłym rozwojem techniki komputerowej oraz pojawieniem się wciąż nowych aplikacji i form użytkowania programów komputerowych, jak na przykład za pomocą oprogramowania *open source*[1128], cyfrowych kopii programów komputerowych[1129] czy też postrzegania programu komputerowego jako utworu multimedialnego[1130]. Problemy mogą się również pojawić w przypadku, gdy twórca do stworzenia programu komputerowego używa innych aplikacji, skryptów czy gotowych fragmentów kodu źródłowego[1131]. Jeszcze innym zagadnieniem jest problem środków ochrony przysługujących podmiotowi zamawiającemu program komputerowy[1132] czy też

[1126] Ibidem, s. 299.
[1127] Więcej: J. Barta, R. Markiewicz, *Prawo autorskie…*; J. Sieńczyło - Chlabicz, *Prawo własności intelektualnej*, Warszawa 2011.
[1128] Więcej: J. Barta, R. Markiewicz, *Oprogramowanie open source w świetle prawa. Między własnością a wolnością*, Kraków 2005.
[1129] N. Góreczny, *Wtórny rynek cyfrowych kopii programów komputerowych. Wprowadzenie do obrotu i wyczerpanie prawa w kontekście cyfrowej dystrybucji*, „Zeszyty Naukowe Prawa Własności Intelektualnej Uniwersytetu Śląskiego" 2013, z. 1.
[1130] Więcej: D. Flisak, *Utwór multimedialny w prawie autorskim*, Warszawa 2008.
[1131] Więcej: W. Machała, *Licencja mieszana? Prawnoautorskie aspekty obrotu programami komputerowymi stworzonymi z wykorzystaniem oprogramowania o otwartym kodzie*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej" 2010, z. 1.
[1132] K. Żak, *Środki ochrony zamawiającego program komputerowy. Odpowiedzialność twórcy za usterki utworu*, Warszawa 2015.

kwestia praw związanych z grą komputerową[1133], która przecież działa opierając się na szeregu innych programów[1134].

W kontekście wyżej wymienionych problemów niezwykle trafne jest stanowisko Katarzyny Chałubińskiej - Jentkiewicz, która stwierdza, że: „w przypadku oprogramowania komputerowego mamy do czynienia z nowym przedmiotem ochrony, której zasady ewoluują wraz z postępującym stanem techniki. Dlatego tak skomplikowane wydaje się ustalenie zasad przyszłej ochrony, zwłaszcza w sytuacjach, kiedy mamy do czynienia z tworzeniem oprogramowania na zamówienie, także wtedy, gdy nie jesteśmy w stanie przewidzieć koniecznych zabezpieczeń czy nawet sposobów przyszłego korzystania”[1135]. Przychylić należy się do wyrażonego powyżej poglądu. Stały rozwój techniki oraz coraz powszechniejsze wykorzystanie programów komputerowych stanowi wyzwanie dla teoretyków i praktyków prawa oraz mogłoby stanowić temat odrębnych, rozległych rozważań.

4.3.4. Bazy danych

W powszechnym rozumieniu pojęcie bazy danych to zbiór informacji bądź zbiór danych. W przeszłości, za bazy danych były uważane głównie biblioteki, rejestry i kartoteki. Obecnie bazy danych są tworzone przez nieograniczoną liczbę podmiotów: instytucje państwowe, banki, policję oraz przede wszystkim podmioty prywatne - przedsiębiorstwa. Bazy te są tworzone zazwyczaj w formie elektronicznej i dzięki temu mogą mieścić w sobie niemal nieograniczoną liczbę rekordów. Bazy elektroniczne mają przewagę nad tymi tradycyjnym ze względu na kilka czynników: możliwość przeprowadzania bieżącej aktualizacji, szybkość oraz łatwość odnalezienia informacji i materiałów. Baza danych ma szczególną wartość zarówno komercyjną, jak i strategiczną, dlatego też podmiot

[1133] Więcej: S. Wiśniewski, *Prawnoautorska kwalifikacja gier komputerowych - program komputerowy czy utwór audiowizualny?* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej” 2012, z. 1.
[1134] E. Traple (red.), *Ochrona gry komputerowej. Aktualne wyzwania prawne*, Warszawa 2015 oraz K. Sztobryn, *Ochrona programów komputerowych w prawie własności intelektualnej w Unii Europejskiej*, Warszawa 2015.
[1135] K. Chałubińska-Jentkiewicz, *Własność…*, Warszawa 2015, s. 222.

administrujący bazą winien podjąć wszelkie możliwe kroki celem zapewnienia jak najlepszej ochrony[1136].

Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony baz danych ujednoliciła europejskie przepisy w omawianym zakresie. W art. 1 definiuje bazy danych jako zbiór niezależnych utworów, danych lub innych materiałów uporządkowanych w sposób systematyczny lub metodyczny, indywidualnie dostępnych środkami elektronicznymi lub innymi sposobami. Co istotne, akt ten nie ma zastosowania do programów komputerowych użytych do sporządzenia lub funkcjonowania baz danych dostępnych środkami elektronicznymi. Artykuł 2 stanowi, że dyrektywę stosuje się do ochrony prawnej programów komputerowych, prawa najmu i prawa wypożyczania oraz niektórych praw pokrewnych do prawa autorskiego w dziedzinie własności intelektualnej oraz okresu ochrony prawa autorskiego i niektórych praw pokrewnych.

Omawiany akt prawa unijnego wprowadza zasadę *sui generis* ochrony baz danych, który ma na celu ochronę inwestycji poniesionej przez producenta (wówczas podmiotem prawa jest producent). Ma to szczególne znacznie w przypadku elektronicznych baz danych, które można z łatwością kopiować i rozpowszechniać, co z kolei jest niezwykle istotne dla ekonomicznych interesów właściciela bazy[1137]. Autorem bazy danych jest osoba fizyczna lub grupa osób fizycznych, które sporządziły bazę lub, jeżeli pozwalają na to przepisy wewnętrzne państw - osoba prawna. Wyjątki od prawa *sui generis* wymienione w art. 9 zachodzą wówczas, gdy, legalni użytkownicy bazy danych (publicznie udostępnionej w jakikolwiek sposób) mogą, bez upoważnienia producenta, pobierać dane lub wtórnie je wykorzystywać w istotnej części. Ma to miejsce w przypadku:

- pobierania nieelektronicznych baz danych do użytku osobistego,
- pobierania w charakterze ilustracji w celach dydaktycznych lub badawczych, tak długo jak wskazane jest źródło i o ile odbywa się to w zakresie uzasadnionym przez niehandlowy cel, który ma być osiągnięty,
- pobierania danych i/lub wtórnego ich wykorzystania do celów bezpieczeństwa publicznego, postępowania administracyjnego lub sądowego.

[1136] E. Kurzępa, *Ochrona baz danych*, [w:] B. Kurzępa, E. Kurzępa, *Ochrona własności intelektualnej. Zarys problematyki*, Toruń 2010, s. 254.
[1137] K. Chałubińska - Jentkiewicz, *Własność…*, s. 245.

W doktrynie wskazuje się, że „prawo *sui generis* do baz danych stanowi składnik praw własności intelektualnej i poszerza zamknięty katalog praw tego rodzaju. Przedmiotem regulacji nie są usytuowane w bazie materialne nośniki (»tradycyjne« lub elektroniczne), na których zawartość bazy jest utrwalona, lecz całość informacji zebranych, uporządkowanych i udostępnionych w toku istotnych nakładów inwestycyjnych, łącznie z elementami potrzebnymi do funkcjonowania i korzystania z bazy na przykład tezaurus, indeks, system wyszukiwaczy”[1138]. Prawo *sui generis* do baz danych ma określone cechy: jest prawem podmiotowym bezwzględnym, skutecznym *erga omnes* i może ono być przedmiotem obrotu prawnego (może być zbyte, przeniesione)[1139].

4.3.5. Usługi *peer - to - peer*

Usługi *peer - to - peer* (P2P - odnoszące się do angielskiego sformułowania „każdy z każdym”) są formą wymiany plików i innych danych cyfrowych pomiędzy użytkownikami. Aplikacje te budzą szereg wątpliwości pod względem naruszeń praw autorskich na ogromną skalę. Wymiana danych następuje za pomocą aplikacji czy też programu, który powoduje, że urządzenie staje się hostem, który nie tylko pobiera, ale również udostępnia dane innym użytkownikom. Programy P2P wykorzystywane są głównie do ściągania muzyki, filmów i seriali. Usługi te stały się przedmiotem międzynarodowej dyskusji, amerykańskie sądy próbowały ustalić zakres odpowiedzialności pośredniej i bezpośredniej w przypadku stosowania tego programu. Z kolei parlament francuski rozważa możliwość wprowadzenia licencji generalnej, która uznałaby legalność usług P2P przy zastosowaniu ogólnego systemu uiszczenia opłaty z tytułu korzystania za pomocą tego programu w zawartych w nim treści[1140]. Na gruncie Konwencji Berneńskiej uznano, że udostępnienie utworu w sieci komputerowej, tak by był dostępny na każde żądanie użytkownika, stanowi rozpowszechnienie utworu.

Znawcy doktryny podkreślają, że „działania *peer - to - peer* charakteryzują sytuację, która odnosi się do dwóch rodzajów odpowiedzialności: pośredniej odpowiedzialności

[1138] J. Barta, R. Markiewicz, *Prawo autorskie...*, s. 426.
[1139] Ibidem, s. 431.
[1140] K. Chałubińska - Jentkiewicz, *Własność ...*, s. 203.

dostawców oprogramowania (usługi), którzy dostarczają aplikację stanowiącą narzędzie służące naruszeniem prawa autorskiego oraz odpowiedzialności bezpośredniej, która dotyczy użytkowników końcowych, którzy poprzez korzystanie z utworów w ramach usługi *peer - to - peer* naruszają prawo autorskie ich twórców"[1141]. Zaakcentować wypada, że ochronie podlega nie tylko cały utwór, ale nawet jako fragment. Pogląd taki został wyrażony między innymi przez Europejski Trybunał Sprawiedliwości w sprawie Infopaq[1142], w którym Trybunał uznał, iż nawet ciąg 11 słów wyciętych z artykułu prasowego jest chronionych prawem autorskim zgodnie z dyrektywą 2001/29/WE Parlamentu Europejskiego w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych. ETS uznał, że przechowywanie fragmentu utworu, czyli ciągu 11 słów może być uznane za „zwielokrotnianie", jeżeli fragment ten nosi elementy własnej twórczości intelektualnej ich autora (kwestia ta winna być jednak zbadana przez sąd krajowy). W konkluzji „rozpowszechnianie" winno być interpretowane szeroko, a ochronna winna obejmować cały utwór jak i jego fragmenty[1143].

Innym jeszcze problemem jest *streaming* (nadawanie internetowe), które polega na nielegalnym udostępnieniu utworów. W czasie *streamingu* użytkownik nie pobiera pliku na własny komputer, lecz za pośrednictwem odpowiedniego portalu internetowego może oglądać filmy, serialne i inne pliki multimedialne *on-line*. Zaznaczyć w tym miejscu należy, iż samo oglądanie czy czytanie utworu za pomocą *steamingu* nie jest naruszeniem prawa autorskiego. Problem sprowadza się do określenia zasad i granic odpowiedzialności osób świadczących usługi (ang. *service providers*), gdyż to właśnie one mogą w sposób pośredni bądź bezpośredni naruszyć prawo autorskie[1144] .

[1141] Ibidem, s. 203.
[1142] Wyrok Europejskiego Trybunały Sprawiedliwości z dnia 16 lipca 2009 r., w sprawie *Infopaq International A/S przeciwko Danske Degblades Forening*, sygn. akt C-5/08.
[1143] A. Gajda, S. Gajda, *Prawne aspekty ścigania użytkowników sieci P2P w Polsce*, [w:] J. Kosiński (red.), *Internetowe naruszenia własności intelektualnej*, Szczytno 2015, s, 39.
[1144] R. Markiewicz, op. cit., s. 6-7.

4.3.6. Strona internetowa a prawo własności intelektualnej

Na świecie istnieje blisko pięć miliardów[1145] stron internatowych o najróżniejszej tematyce i przeznaczeniu. Służą one do komunikacji z organami władzy, umożliwiają pracę, naukę, rozrywkę, łączenie ludzi o wspólnych zainteresowaniach. Możliwość wykorzystania stron www jest niemal nieograniczona. Również sam wygląd stron oraz ich funkcje z roku na rok są coraz bardziej zaawansowane. W związku z tym należałoby zadać sobie pytanie jak wygląda status stron internetowych w świetle prawa własności intelektualnej. Pominięto w pracy kwestię zlecenia wykonania witryny internetowej oraz związane z tym zagadnienie poprawnego skonstruowania umowy o stworzenie takiej strony.

Strony internetowe można podzielić na dynamiczne i statyczne. Witryny statyczne są przedstawione w Internecie w takim samym kształcie w jakim widnieje ona na serwerze. Z kolei strony dynamiczne są każdorazowo tworzone za pomocą specjalnego programu komputerowego tak zwanych aplikacji webowych. Rozróżnienie to ma ogromne znaczenie do klasyfikacji stron na gruncie prawa autorskiego[1146].

W polskiej literaturze przedmiotu brak jest szerszej analizy strony internetowej jako przedmiotu prawa autorskiego. Trudności może nastręczyć pytanie czy można uznać stronę www za utwór w rozumieniu polskiej ustawy o prawie autorskim i prawach pokrewnych. Kolejny problem nasuwa się przy ustaleniu, czy witryna nosi cechy oryginalności, nowości utworu oraz jego indywidualnego charakteru. Mimo wielu wątpliwości, uznaje się jednak, iż strona internetowa może uzyskać ochronę autorskoprawną, lecz może nastąpić problem z jego klasyfikacją[1147].

Utwory cyfrowe, z którymi można się spotkać w cyberprzestrzeni, w tym strony internetowe, z związku z różnorodnością form należy uznać za utwory multimedialne. Nawet podstawowe strony www zostały uznane za utwory multimedialne między innymi przez Damiana Flisaka[1148] oraz Arkadiusza Michalaka[1149]. Z kolei Łukasz Draszczyk wskazuje że:

[1145] Dane z oficjalnej strony internetowej World Wide Web Size http://www.worldwidewebsize.com/ [10.12.2016].
[1146] Ł. Draczyk, *Strona internetowa w świetle prawa autorskiego*, „Prace z Prawa Własności Intelektualnej" 2015, z. 2 (128), s. 80.
[1147] Ibidem, s. 77-79.
[1148] D. Flisak, op. cit., s. 95.

„strukturę strony internetowej, jak każdego utworu multimedialnego, możemy podzielić na dwie części: programistyczną, zapisaną w odpowiednim kodzie (w przypadku stron internetowych będzie to np. język HTML, PHP, Java) - tzw. *back end*, oraz część graficzną - czyli to, co widzimy na ekranie monitora po otworzeniu adresu strony www w przeglądarce internetowej (czyli tzw. *front end*). To właśnie w tych dwóch warstwach należy poszukiwać cech oryginalności i indywidualności wymaganych do uznania danej strony internetowej za utwór w rozumieniu prawa autorskiego"[1150].

Należy zatem rozważyć, czy warstwa programistyczna, kod programu, zapisany w języku HTML może być uznany za program komputerowy i podlegać pod ochronę prawa autorskiego. Problem ten nie był szerzej poruszany w polskiej doktrynie, lecz zagadnienie to było rozpatrywane w innych porządkach prawnych. W niemieckim prawie o ochronie praw autorskich i prawach pokrewnych[1151] brak jest legalnej definicji programu komputerowego, wobec czego należy uznać, że jest to program komputerowy w jakiejkolwiek formie. Wobec braku jednoznacznych uregulowań niemiecka doktryna wykształciła dwa przeciwstawne stanowiska. Pierwsze z nich odwołuje się do Traktatu WIPO o prawach autorskich, który interpretuje programy komputerowe szeroko - niezależnie od sposobu lub formy wyrażania. Przedstawiciele drugiego - przeważającego w niemieckim piśmiennictwie - stanowiska, uznali jednak, że stron internetowych stworzonych w języku HTML nie można uznać za program komputerowy[1152].

Rozbieżności takie nie występują w prawie USA. Amerykański Urząd Ochrony Praw Autorskich (ang. *The Copyright Office*) w dokumencie wyjaśniającym procedurę rejestracji „dzieł internetowych" (ang. *on-line works*) w sposób bezpośredni stwierdza, że kod HTLM może podlegać ochronie jako program komputerowy. Również warstwa graficzna strony (rysunki, materiały audiowizualne, fotografie) będzie podlegała ochronie na gruncie amerykańskich przepisów o prawach autorskich[1153]. Podobne rozwiązania przyjęto też w Wielkiej Brytanii. W polskim piśmiennictwie Łukasz Draszczyk przychyla się do

---

[1149] A. Michalak, *Przegląd cywilnoprawnych instrumentów ochrony portali internetowych*, „Przegląd Prawa Handlowego" 2010, nr 4, s. 19.
[1150] Ł. Draczyk, op. cit., s. 80.
[1151] Gesetz über Urheberrecht und verwandte Schutzrechte von 09.09.1965.
[1152] Ł. Draczyk, op. cit., s. 80-81.
[1153] Por. Wyrok *Apple Computer Inc. przeciwko Microsoft Corp*.709 F.Supp. 925, 10 U.S.P.Q.2d (BNA) 1677 (N.D. Cal. 1989), oraz wyrok *Lotus Develompment Corporation przeciwko Borland International Inc*., sygn. akt 516 U.S. 233 (1996).

stwierdzenia, że witryny internetowe stworzone w języku HTLM nie będą stanowiły programu komputerowego[1154].

Coraz popularniejsze jest tworzenie stron internetowych w bardziej skomplikowanych, nowocześniejszych programach (PHP, Java, Java Script). By ustalić, że program ten będzie podlegał ochronie autorskoprawnej konieczne jest zbadanie, czy posiada on cechy indywidualne i twórcze. Zupełnie niezależnie należy też rozważać warstwę graficzną strony internetowej tak zwany interfejs użytkownika, utwory plastyczne czy audiowizualne[1155]. Warstwa graficzna może zatem być, pod pewnymi warunkami[1156], rozumiana jako inny utwór podlegający ochronie praw autorskich[1157]. Utwory multimedialne, do których można zaliczyć strony internetowe mają skomplikowaną strukturę i niejednorodny, złożony charakter. Mimo braku jednoznacznych rozwiązań i różnic pomiędzy polskim porządkiem prawnym i praktyką zagraniczną dyskusja nad problemem własności intelektualnej w odniesieniu do stron internetowych pozostaje otwarta. Wydaje się, iż w przyszłości - ze względu na rozwój innowacyjność wprowadzanych rozwiązań - zaistnieje konieczność podjęcia głębszych rozważań nad tym tematem.

4.3.7. Chmura obliczeniowa a własność intelektualna

Coraz większą popularność i powszechność stosowania zyskuje tzw. „chmura", czyli chmura obliczeniowa (ang. *cloud computing*) rozumiana jako model przetwarzania i przechowywania danych. Chmura obliczeniowa „bazuje na współdzieleniu i korzystaniu z zewnętrznych zasobów infrastruktury informatycznej (na przykład sprzęt komputerowy, serwery, urządzenia do przechowywania danych) niezależnie od geograficznej lokalizacji poszczególnych jej elementów oraz wykorzystywanych kanałów i narzędzi komunikacyjnych. Takie oddzielenie warstwy logicznej od warstwy fizycznej systemu komputerowego umożliwia użytkownikowi między innymi korzystanie z różnego rodzaju oprogramowania niezależnie od miejsca jego instalacji, tworzenie dzieła z innymi współtwórcami niezależnie

[1154] Ł. Draczyk, op. cit., s. 81-82.
[1155] Ibidem, s. 80.
[1156] Jeżeli szata graficzna będzie spełniać cechy indywidualnego charakteru, co może przejawiać się przez połączenie różnych elementów: wybór czcionki, kolorów, układ graficzny strony, sposób prezentacji treści, kompozycja menu i linków.
[1157] Zob.: Wyrok Trybunału Sprawiedliwości z dnia 22 grudnia 2010 r. *Bezpečnostní softwarová asociace - Svaz softwarové ochrany przeciwko Ministerstwo Kultury*, sygn. akt C-393/09.

od odległości, która ich dzieli, jak i łatwiejsze rozpowszechnianie utworów przez ich udostępnianie w wielu miejscach jednocześnie”[1158]. Termin i technologia chmury obliczeniowej jest zagadnieniem nowym, niejednolitym, a jej zakres obejmuje szereg usług o różnej charakterystyce.

Według Krajowego Instytutu Standaryzacji i Technologii w Stanach Zjednoczonych chmura obliczeniowa to „model umożliwiający wszechstronny, wygodny, sieciowy dostęp na żądanie do wspólnej puli konfigurowalnych zasobów obliczeniowych (...), które można szybko zapewniać i udostępniać przy minimalnym wysiłku w zakresie zarządzania czy też przy minimalnej interakcji z dostawcą usługi”[1159]. Chmura jest narzędziem, które przyśpiesza wymianę danych, mobilność oraz zwiększa efektywność całej gospodarki[1160]. Ewa Molenda - Kropielnica staje na stanowisku, że *cloud computing* jest modelem „świadczenia usług IT, który daje użytkownikowi możliwość korzystania z zasobów obliczeniowych w dowolnym miejscu i czasie. Klient ma tu dostęp zarówno do aplikacji bez konieczności ich instalacji, jak i do infrastruktury, na którą dokonuje transferu gotowych lub stworzonych przez siebie programów. Co jednak najbardziej istotne, płaci jedynie za tyle, ile rzeczywiście używa (ang. *pay as you go*), zazwyczaj w modelu abonamentowym (subskrypcyjnym). Usługi w chmurze obliczeniowej, dzięki możliwościom jakie daje skalowanie i wielodzierżawa, są elastyczne i dostosowane do zmieniających się potrzeb klientów”[1161]. Z tych względów chmury obliczeniowe zdobywają coraz większą popularność. Rozwiązania techniczne połączone z elastycznym modelem biznesowym powodują, że z chmury korzystają nie tylko osoby prawne, ale również fizyczne.

Chmura obliczeniowa oferuje kilka rodzajów usług polegających na zapewnieniu usługobiorcy na żądanie dostępu do zasobów IT. Możemy się spotkać z trzema podstawowymi modelami usług: infrastruktura jako usługa (ang. *Infrastructure as a Service* - IaS - polegający na dostarczaniu usługobiorcy zasobów obliczeniowych, systemów operacyjnych), platforma jako usługa (ang. *Platform as a Service* - PaS - gdzie usługobiorcy

[1158] M. Siwicki, *Jurysdykcja krajowa w sprawach z zakresu prawa autorskiego w „chmurach obliczeniowych” w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1215/2012*, „Europejski Przegląd Sądowy” 2016 nr 1, s. 21.

[1159] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Wykorzystanie potencjału chmury obliczeniowej w Europie”, http://eur–lex.europa.eu/ LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:PL:PDF [10.12.2016].

[1160] Więcej o architekturze chmur obliczeniowych w: M. Siwicki, *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajemnicy telekomunikacyjnej w chmurach obliczeniowych*, „Prokuratura i Prawo” 2015, nr 5.

[1161] E. Molenda-Kropielnicka, *Cloud Computing - zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej” 2013, z. 1 (119), s. 112.

dostarczona jest gotowa infrastruktura, na której może on budować aplikacje i programy) oraz oprogramowanie jako usługa (ang. *Software as a Service* - SaS - rozumianej jako umożliwienie użytkownikowi korzystania z aplikacji działających w chmurze)[1162]. Do wszystkich tych modeli usług zbiorczo używa się nazwy SPI (ang. *Software - Platform - Infrastructure*)[1163].

Używanie chmury obliczeniowej w kontekście prawa autorskiego rodzi pytania o to, czy z utworu korzysta tylko użytkownik końcowy oraz czy dochodzi do ograniczenia praw legalnego użytkownika, gdy korzysta on z chmury, a nie z własnego egzemplarza programu. Prawnoautorski problem ochrony praw w chmurze obliczeniowej jest wielowymiarowy. Przede wszystkim podstawową kwestią jest zakres korzystania z programów komputerowych udostępnionych przez dostawcę bądź transferowanych do chmury przez użytkownika. Za pomocą chmury można również magazynować dane oraz wymieniać pliki metodą *peer-to-peer*, zagadnienie zostało już opisane we wcześniejszych podrozdziałach. Szczególnie problematyczne jest miejsce wykonania zobowiązania w przypadku eksploracji utworów w chmurze obliczeniowej - ciężko jest ustalić miejsce położenia nośnika, na którym zostały zapisane dane. Maciej Siwicki uznaje, że „w przypadku chmury do zapisu utworu w zdigitalizowanej wersji może dojść na: a) pojedynczym serwerze służącym do przechowywania (gromadzenia) danych, b) kilku serwerach, na których zapisane będą poszczególne fragmenty utworów, c) urządzeniu końcowym użytkownika, gdzie utwór został w całości lub w części przesłany będąc zapisanym czasowo (np. *streaming*), lub w sposób trwały (ang. *download*), d) egzemplarzu utworu przesyłanym na żądanie użytkownika (np. CD-ROM, DVD-ROM z wersją instalacji oprogramowania)"[1164].

Krytycy chmury obliczeniowej podkreślają, iż ten model dostarczania usług w IT wiąże się z dużym niebezpieczeństwem w zakresie prywatności i bezpieczeństwa danych osobowych. Szczególnie niebezpieczny wydaje się scenariusz, w którym na skutek nieprawidłowego zarządzania systemem dochodzi do niekontrolowanego wycieku danych bądź ataku hackerów. Podmioty dostarczające usługi chmury obliczeniowej muszą zapewnić

[1162] M. Hałuszczak, *Wybrane problemy cloud computing z perspektywy polskiej regulacji ochrony danych osobowych*, „Zeszyty Naukowe Prawa Własności Intelektualnej Uniwersytetu Śląskiego" 2013, z. 1, s. 52.
[1163] E. Molenda - Kropielnicka, op. cit., s. 113.
[1164] M. Siwicki, *Jurysdykcja…*, s. 22.

bezpieczeństwo fizyczne, bezpieczeństwo serwerów, odpowiedni sposób gromadzenia i przechowywania danych oraz ich szyfrowania[1165].

Poruszyć, chociażby pokrótce, należy również kwestię stosowania licencji w chmurze obliczeniowej. W świadczeniu usług *cloud computing* mamy do czynienia z programem komputerowym- czy to w przypadku aplikacji, do których użytkownik uzyskuje dostęp, czy to przez oprogramowanie wykorzystane w ramach infrastruktury chmury. W praktyce pojawiają się poglądy, że chmura wymaga nowego podejścia do kwestii licencjonowania[1166]. Maciej Siwicki podkreśla, iż stosowanie chmury obliczeniowej łączy się z jeszcze jednym dylematem, często spotykanego automatyzmu działania, który może spowodować automatyczne zwielokrotnianie przechowywanych w niej danych (na przykład przez utworzenie kopii zapasowej). Może również dojść do sytuacji, że umieszczony w chmurze obliczeniowej utwór zostaje podzielony, ze względów ekonomicznych lub technicznych, na mniejsze kawałki i rozmieszczony na kilku serwerach położonych w zupełnie różnych miejscach[1167].

Analiza tego problemu prowadzi do wniosku, że w przypadku eksploatacji utworów w chmurze obliczeniowej możliwe jest wniesienie pozwu we wszystkich państwach, w których doszło do realizacji umowy nawet, jeżeli była to realizacja częściowa. Ten stan prawny może doprowadzić do ustalenia właściwości wielu państw. Uzasadnione zatem wydaje się zawieranie w umowach o świadczenie usług w chmurze obliczeniowej zapisu ustanawiającego sąd właściwy do rozstrzygania sporów wynikłych z umowy. Innym rozwiązaniem jest przyjęcie przez dostawcę chmury takich rozwiązań technologicznych, które wyeliminują możliwość zwielokrotniania lub dzielenia programu bądź utworu[1168].

Chmura obliczeniowa jest stosunkowo nowym rozwiązaniem technicznym, ale nie ulega wątpliwości, iż będzie ono coraz częściej spotykane. Wpłynie na to kilka czynników: rozwój szerokopasmowego Internetu, wielkie korzyści dla przedsiębiorców, czyli chęć częściowego *outsorcingu* danych, oszczędność miejsca i pieniędzy (nie trzeba utrzymywać drogich serwerowni). Używanie chmury obliczeniowej to nie tylko wskazane wyżej kwestie ochrony praw własności intelektualnej. Nie mniej istotne są kwestie bezpieczeństwa przetwarzania danych osobowych, zarządzania infrastrukturą krytyczną czy też tajemnicy

[1165] R. Marchini, *Cloud computing: A Practical Introduction to the Legal Issues*, Londyn 2010, s. 24-25.
[1166] Więcej na temat licencji w chmurze: E. Molenda-Kropielnicka, op. cit.
[1167] M. Siwicki, *Jurysdykcja …*, s. 22-23.
[1168] Ibidem, s. 24-26.

komunikacyjnej. W niniejszej pracy jedynie zasygnalizowano pojawiające się problemy prawne związane z chmurą obliczeniową, jednakże nawet tak krótka analiza daje podstawy do uznania, że są to problemy na tyle interesujące i istotne, że powinny stać się przedmiotem większej uwagi ze strony praktyków i teoretyków prawa, także w Polsce.

4.4 Inne obszary cyberprzestrzeni

4.4.1 Cyberprzestrzeń a prawa człowieka

We wstępie do Powszechnej Deklaracji Praw Człowieka z dnia 10 grudnia 1948 r. stwierdzono, że: „uznanie przyrodzonej godności oraz równych i niezbywalnych praw wszystkich członków rodziny ludzkiej jest fundamentem wolności, sprawiedliwości oraz pokoju na świecie”[1169]. Prawa człowieka są powszechne, przyrodzone, przynależne każdemu człowiekowi, niezależnie od sytuacji i pozycji społecznej. Praw tych nie można pozbawić, ani dobrowolnie się ich zrzec. Prawa człowieka mają charakter podmiotowy i podlegają ochronie.

Prawami człowieka są „doniosłe prawa, które służą jednostce według jakiejś koncepcji filozoficznej, odnoszącej się do jej pozycji w państwie (płaszczyzna filozoficzna), czy też służą jej w świetle norm prawa międzynarodowego, wewnątrzkrajowego lub ponadpaństwowego (płaszczyzna prawna)”[1170]. Małgorzata Kun - Buczo i Małgorzata Wenclik wobec braku powszechnej definicji praw człowieka wyróżniają trzy główne grupy definicyjne. Pierwsza z nich odnosi się wyłącznie do norm prawa traktatowego. Jej zwolennicy uznają, że „prawami człowieka nazwiemy pewien zbiór uprawnień przysługujących jednostce zawartych w konkretnym akcie prawnym oraz podmiot zobowiązany do ich zapewnienia”. Druga grupa istnienie praw człowieka upatruje w godności ludzkiej, twierdząc, że „prawami człowieka są uprawnienia wypływające wyłącznie z godności ludzkiej oraz faktu, że jest człowiekiem. Wszyscy ludzie nabywają je w jednakowym zakresie”. Trzecia, ostatnia grupa łączy dwa wymienione wyżej poglądy,

[1169] Powszechna Deklaracja Praw Człowieka.
[1170] Z. Hołda, *Prawa człowieka. Wiadomości wstępne,* [w:] J. Hołda, Z. Hołda, D. Ostrowska, J.A. Rybczyńska, *Prawa człowieka. Zarys wykładu*, Warszawa 2014, s. 11.

uznając że „prawami człowieka nazwiemy prawa wypływające z godności ludzkiej wraz z korelatywnymi obowiązkami. Znajdują one potwierdzenie w normach prawa krajowego i międzynarodowego. Są niezbywalne, powszechne i nienaruszalne”[1171].

Koncepcje praw człowieka współcześnie wyróżniają trzy kategorie takich praw:

- wolności i prawa osobiste - związane z najistotniejszymi prawami jednostki, czyli ochrona życia, bezpieczeństwo czy nietykalność,
- wolności i prawa polityczne - dotyczą aktywnego udziału jednostki w społeczeństwie i życiu społeczno – politycznym; prawa te odnoszą się do wolności zgromadzeń, zrzeszania się w organizacje, możliwość ekspresji poglądów, biernego i czynnego prawa wyborczego, prawa do rzetelnego procesu sądowego,
- wolności i prawa społeczne, ekonomiczne i kulturalne - mają związek z prawem do zabezpieczeń społecznych, dostępem do edukacji, dóbr kultury, opieki medycznej, zabezpieczenia życia rodzinnego[1172].

Dwie pierwsze kategorie są nazywane prawami człowieka pierwszej generacji. Wolności i prawa społeczne, ekonomiczne i kulturalne uzyskały miano praw drugiej generacji. W ostatnich latach proponuje się wyszczególnienie kolejnej, trzeciej kategorii praw człowieka. Miałyby być one związane na przykład z prawem do pokoju, środowiska czy też rozwoju[1173].

Międzynarodowe i regionalne systemy ochrony praw człowieka w gruncie rzeczy zawierają tożsame postanowienia gwarantujące ochronę jednostki. Jednakże w procesie rewolucji cyfrowej ochrona praw człowieka wkracza w zupełnie inny wymiar. Nie oznacza to jednak, że istnieje konieczność budowy zupełnie nowych norm prawnych, które usankcjonowałyby status człowieka w cyberprzestrzeni. Człowiek jest częścią nowego społeczeństwa informacyjnego opartego na wiedzy. Jedną z jego podstawowych cech jest dostęp do szeroko rozumianej informacji, możliwość jej przekształcania oraz autonomia informacyjna. Te elementy według Mariusza Jabłońskiego i Krzysztofa Wygoda stanowią o statusie informacyjnym jednostki w państwie, na który składa się między innymi wolność wyrażenia swoich poglądów, pozyskiwania i rozpowszechniania informacji (czyli wolność

[1171] M. Kun-Buczko, M. Wenclik, *Międzynarodowa ochrona praw człowieka*, [w:] M. Kun-Buczko, *Prawo międzynarodowe publiczne. Zarys problematyki*, Białystok 2011, s. 212.
[1172] Ibidem, s. 217.
[1173] Z. Hołda, op. cit., s. 11.

słowa i wypowiedzi, wolność prasy, zakaz cenzury prewencyjnej), wolność sumienia i religii (wolność wyznania, wyrażania i uzewnętrzniania religii), wolność twórczości artystycznej, badań naukowych, ogłaszanie ich wyników, prawo do nauki, wolność korzystania z dóbr kultury, prawo do informacji o działalności organów władzy publicznej, wolność i ochrona korespondencji, prawo do ochrony prawnej życia prywatnego, prawo do nieujawniania informacji dotyczących siebie samego oraz prawo dostępu do dotyczących nas urzędowych dokumentów i zbiorów danych[1174]. Ze względu na przedmiot niniejszej pracy należy skupić się na wybranych zagadnieniach, które mają największe znaczenie dla ochrony praw jednostki w przestrzeni cyfrowej, bądź są rozbieżnie interpretowane w różnych porządkach prawnych.

Wolność wypowiedzi

Wolność wypowiedzi ma fundamentalne znaczenie dla funkcjonowania demokratycznego państwa prawa. Przysługuje ona jednostkom, ale może, ze względu na swoją specyfikę, być wykonywana zbiorowo, ponieważ jest jednym z podstawowych elementów innych swobód takich, jak wolność zgromadzeń, prawo do uzewnętrzniania religii czy prawo do wolnych wyborów. Leszek Garlicki podkreśla, że jest to prawo fundamentalne w krajowych i międzynarodowych systemach ochrony praw człowieka określane mianem „superprawa"[1175]. Wolność wypowiedzi została uregulowana między innymi w art. 19 MPPOiP[1176], art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka (EKPC)[1177] oraz w art. 54 polskiej Konstytucji[1178]. Na wolność wypowiedzi składa się: wolność posiadania poglądów, wolność poszukiwania i otrzymywania informacji i idei oraz wolność ich przekazywania. Wolność posiadania poglądów jest prawem, które przysługuje indywidualnie jednostce. Pozostałe z wymienionych elementów może z kolei przysługiwać zarówno osobom fizycznym jak i podmiotom grupowym. Wolność do otrzymywania informacji jest z kolei

[1174] M. Jabłoński, K. Wygoda, *Prawa człowieka w komunikacji elektronicznej*, [w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003, s. 29-30.
[1175] L. Garlicki, *Polskie prawo konstytucyjne*, Warszawa 2003, s. 584-585.
[1176] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku 19 grudnia 1966 r., Dz.U. z 1977 r., Nr 38, poz. 167.
[1177] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2., Dz.U. z 1993 r., Nr 61, poz. 284.
[1178] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r., Nr 78, poz. 483.

prawem, które przysługuje głównie odbiorcom wypowiedzi: słuchaczom, widzom, internautom, czyli ogólnie opinii publicznej[1179].

Orzecznictwo strasburskie wyszczególnia trzy płaszczyzny wolności ekspresji: środek (medium), podmiot (autora) i materię, treść i formę wyrażania opinii[1180]. Pierwsza płaszczyzna poruszająca problem środka wypowiedzi dotyczy formy przekazu, pisemnego, ustnego, czy też tworzonego za pomocą środków technicznych: telewizji, radia, Internetu. Płaszczyzna podmiotowa dotyczy otwartego katalogu osób, którym wolność wypowiedzi przysługuje[1181]. Ostatni aspekt dotyczy treści i formy wyrażania opinii. W wyroku Europejskiego Trybunału Praw Człowieka (ETPCz) z dnia 23 września 1994 r.[1182] stwierdzono, iż swoboda wypowiedzi nie ogranicza się jedynie do poglądów oraz informacji, które są uważane za przychylne, nie obraźliwe czy też neutralne. Wolność słowa odnosi się również do tej formy wypowiedzi, która ma charakter obraźliwy, oburzający, wywołujący niepokój czy też nie akceptowalny przez większą część społeczeństwa. Nie można jednak domniemywać, że swoboda wypowiedzi ma charakter bezwzględny, absolutny i nie podlega żadnym ograniczeniom[1183]. Bez wątpienia przestrzeń cyfrowa umożliwiła, na nieznaną do tej pory skalę, wymianę poglądów. Pozorna anonimowość w sieci potęguje jednak treści o pejoratywnym charakterze. Europejski Trybunał Praw Człowieka kilkukrotnie poruszył kwestię wolności wypowiedzi internetowej między innymi w sprawie dotyczącej publikowania w Internecie nieprawdziwych informacji o osobie fizycznej przez osobę trzecią[1184], w sprawie dotyczącej publikowania w cyberprzestrzeni materiałów obscenicznych[1185] czy też kwestii zasad publikacji internetowych[1186].

W tym miejscu krótko należy wspomnieć, że pewnym kategoriom wypowiedzi jest przyznana większa ochrona wolności wyrażania poglądów. Dotyczy to mianowicie kwestii politycznych, uznano, iż debata polityczna jest jądrem koncepcji społeczeństwa

[1179] M. Jastrzębski, *Międzynarodowe i polskie standardy wolności wypowiedzi a postanowienia umowy ACTA*, [w:] M. Jastrzębski, T. Kuczur (red.), *Bezpieczeństwo państwa a wolność jednostki. Wybrane aspekty prawne i polityczne*, Toruń 2013, s. 82 -84.
[1180] L. Garlicki, op. cit., s. 587.
[1181] M. Jastrzębski, op. cit., s. 85.
[1182] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 23 września1994 r., w sprawie *Jersild przeciwko Danii*, skarga nr 15890/89.
[1183] Ł. Goździaszek, *Cywilnoprawne granice swobody wypowiedzi w Internecie*, Warszawa 2015, s. 5-6.
[1184] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 grudnia 2008 r., w sprawie *K.U. przeciwko Finlandii*, skarga nr 2872/02.
[1185] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 18 października 2005 r., w sprawie *Laurent Perrin przeciwko Wielkiej Brytanii*, skarga nr 5446/03.
[1186] Wyrok Europejskiego Trybunału Praw Człowieka z dnia dnia 10 marca 2009 r., w sprawie *TIMES przeciwko Wielkiej Brytanii*, skarga nr 3002/03 i 23676/03.

demokratycznego[1187]. Również media pełnią szczególną rolę, ponieważ dzięki nim realizowana jest wolność otrzymywania i przekazywania informacji, pełnią one rolę obrońcy interesu publicznego[1188]. Publikowanie satyrycznych czy też prześmiewczych materiałów w ramach debaty politycznej nie może być zatem uznane za działanie niezgodne z prawem[1189].

Wolność wypowiedzi nie ma jednak charakteru absolutnego, podlega ono uregulowanym ustawowo ograniczeniom, związanym z prawami innych osób bądź ochroną bezpieczeństwa, porządku publicznego bądź zdrowia czy moralności. W USA wolność słowa jest rozumiana nieco inaczej niż na gruncie europejskim. Wolność słowa została zagwarantowana w Pierwszej Poprawce do Konstytucji. Zgodnie z amerykańskim porządkiem prawnym rozpowszechnianie informacji za pomocą Internetu jest traktowane, jak komunikacja telefoniczna, wobec czego, dopuszczalna jest daleko idąca wolność słowa do momentu, gdy nie dochodzi do szykanowania odbiorcy. Jeżeli jednak wypowiedź będzie grozić konkretnej osobie, to może być zakwalifikowana jako zbrodnia nienawiści tak zwana *hate crime*. W regulacjach europejskich często spotyka się przepisy zabraniające propagowaniu niektórych treści, czyli chociażby nazizm. Jednakże w systemie amerykańskim treści o charakterze rasistowskim, ksenofobicznym czy faszystowskim w dalszym ciągu będą korzystały z Pierwszej Poprawki do Konstytucji USA[1190].

Demokratyczne państwa z europejskiego i amerykańskiego kręgu kulturowego przyznają szeroki katalog ochrony praw człowieka, w tym w zakresie swobody wypowiedzi w cyberprzestrzeni. Sytuacja wygląda zgoła odmiennie w krajach takich, jak Chiny, w których dochodzi do cenzury Internetu za pomocą skomplikowanej i nowoczesnej infrastruktury technologicznej[*]. Przyczyną odmiennego podejścia są między innymi różnice kulturowe. W Chinach wartością nadrzędną jest dobro ogółu, nawet kosztem jednostki[1191]. Podobne

[1187] Wyrok Europejskiego Trybunału Praw Człowieka z dnia z 08 lipca 1986 r., w sprawie *Lingens przeciwko Austrii*, skarga nr. 9815/82.
[1188] B. Gronkowska, T. Jasudowicz, *Prawa człowieka i ich ochrona*, Toruń 2005, s. 336.
[1189] Tak jak to miało miejsce w sprawie bloga AntyKomor.pl, na którym były publikowane satyryczne zdjęcia i gry przedstawiającego byłego Prezydenta Rzeczpospolitej Polskiej Bronisława Komorowskiego. Sąd Apelacyjny w Łodzi umorzył postępowanie w sprawie znieważenia prezydenta.
[1190] J. Przyjemska, *Granice wolności słowa w Internecie w wybranych systemach prawnych*, [w:] A. Biłgoraski (red.), *Wolność wypowiedzi i jej granice. Analiza wybranych zagadnień*. Katowice 2014, s. 115.
[*] Zagadnienie to było szerzej poruszane w podrozdziale 3.2.2. *Porządki prawne krajów o silnie zarysowanej polityce dotyczącej cyberprzestrzeni.*
[1191] J. Przyjemska, op. cit., s. 116.

ograniczenia w swobodnym dostępie do informacji zawartych w przestrzeni cyfrowej można spotkać w krajach takich jak Egipt, Birma czy Malezja[1192].

Charakterystyczną cechą wypowiedzi dokonywanych za pomocą sieci teleinformatycznych jest ich szeroki zasięg i potencjalna możliwość odbioru przez niemal nieograniczoną liczbę osób. W doktrynie pojawiło się zatem pytanie czy znaczna ilość odbiorców w przypadku publicznych wypowiedzi w Internecie będzie stanowić kryterium miarkowania odpowiedzialności? Specyfika cyberprzestrzeni powoduje, że zamieszczona na portalu internetowym wypowiedź może dotrzeć do szerokiego audytorium, ale również ze względu na ogromną ilość informacji udostępnianych codziennie w Internecie, równie prawdopodobny jest również całkowity brak odbiorców. Przy rozpatrywaniu niniejszego zagadnienia należy wziąć pod uwagę, że treści, które pojawiają się w cyberprzestrzeni często bywają kopiowane i udostępniane na innych stronach internatowych. Zgodzić należy się z Łukaszem Goździaszkiem, który zauważył, że „wypowiedź jako taka nie jest powiązana jedynie z jednym nośnikiem, czyli stroną internetową, ale jest informacją, która może krążyć po Internecie. Obieg informacji w Internecie jest z kolei bardzo dynamiczny i trudny do monitorowania. Szeroki krąg odbiorców w Internecie najczęściej jest pochodną viralowego (niekontrolowanego) rozprzestrzeniania informacji, czyli udostępniania i polecania w swoim środowisku internetowym konkretnych stron internetowych”[1193]. Również praktyka orzecznicza mniejszą wagę przykłada do kryterium rzeczywistego zasięgu takiej wypowiedzi. Istnieje oczywiście możliwość zbadania liczby „wejść” na konkretną stronę internetową jednakże znacznie utrudnionym będzie ustalenie czy dana treść nie została skopiowana i udostępniona w innym serwisie internetowym.

Istotnym zagadnieniem jest swoboda wypowiedzi prasowej. Systemy normatywne z zasady nie różnicują prasy tradycyjnej i internetowej. W rzeczywistym obrocie możemy jednak napotkać problemy ze zdefiniowaniem współczesnego obrotu informacyjnego. O tyle o ile elektroniczne odpowiedniki prasy tradycyjnej bez wątpienia możemy nazwać prasą, to blogi, vlogi i podcasty redagowane w pierwszej osobie mogą być kwalifikowane nie jako prasa, lecz jako twórczość literacka. Problem kwalifikacji prawnej różnego typu witryn internetowych pojawia się również w kontekście wymogu rejestracji działalności prasowej[1194].

[1192] J. Kulesza, *Międzynarodowe …*, s. 256-259.
[1193] Ł. Goździaszek, op. cit., s. 11-12.
[1194] Ibidem, s. 59-61.

Prawo prasowe nakłada na dziennikarzy obowiązek prawdziwego przedstawiania omawianych zjawisk, zachowania szczególnej staranności i rzetelności przy gromadzeniu i wykorzystywaniu zebranych materiałów. Czytelnik prasy tradycyjnej ma zagwarantowaną większą pewność, iż zamieszczone w nim informacje są prawdziwe. Dziennikarska rzetelność w odniesieniu do doniesień internetowych niejednokrotnie może jednak budzić poważne wątpliwości. Zgodzić należy się z poglądem Łukasza Goździaszeka, który stwierdza, że: „wypowiedzi internetowe, pomimo że hipotetycznie mogłyby zostać zamieszczone również w ramach prasy, powinny wiązać się z surowszą odpowiedzialnością związaną z publikacją nieprawdy, ponieważ nie ma w takich przypadkach gwarancji, również o charakterze pozaprawnym, co do rzetelności i staranności dziennikarskiej. Odrębnym zagadnieniem jest jednak kwestia wskazania, że dana wypowiedź jest lub nie jest prasą (...) Funkcjonowanie wypowiedzi internetowych w ramach prasy, pod warunkiem zachowania rzetelności i staranności, przesuwa granicę odpowiedzialności za przekroczenie granic swobody wypowiedzi, niezbędnym jednak warunkiem w tym zakresie, jest kwalifikacja tej działalności jako prasowej”[1195]. Anonimowość oraz ogólnodostępność Internetu powoduje, iż zamieszczane tam treści i wypowiedzi często mają na celu wyrażenie prywatnych opinii autora, a nie przekazanie prawdziwych informacji. Walor wiarygodności danej publikacji może zostać przyznany wówczas, gdy dany użytkownik sieci obdarzy nadawcę treści zaufaniem, ponieważ „korzystanie z Internetu zmusza użytkownika do dokonywania ciągłych i świadomych wyborów. Nie ograniczają się one do selekcjonowania treści już opublikowanych, ale mogą prowadzić także do tworzenia własnych materiałów i ich publicznego udostępniania. Wybory, których dokonuje użytkownik, dotyczą zatem także jego statusu w Internecie. Użytkownik decyduje, czy pozostanie tylko odbiorcą, czy wybierze także rolę nadawcy. Multimedialność Internetu umożliwia mu wybór najbardziej właściwej, w jego odczuciu, formy prezentacji”[1196]. Z rozważań tych wynika, iż publikacja wypowiedzi w cyberprzestrzeni nie jest w zasadzie unormowania prawnie. Skutkiem takiego stanu rzeczy jest brak regulacji, które zapewniałyby treściom zamieszczanym w Internecie ich dosłowność i prawdziwość. Osoby publikujące w przestrzeni wirtualnej nie są obwarowane wymogami, prawnymi czy etycznymi, a ich celem może być jedynie wyrażanie poglądów o populistycznym charakterze.

[1195] Ibidem, s. 73.
[1196] J. Taczkowska, *Kategorie wypowiedzi i ich ochrona*, Warszawa-Poznań 2008, s. 239 - 340.

Prawo do prywatności

Temat prawa do prywatności oraz powiązana z tym zagadnieniem kwestia ochrony praw osobowych został poruszony w wielu regulacjach międzynarodowych i ponadnarodowych, między innymi w art. 17 MPPOiP czy też w art. 8 EKPCz. Prawo do prywatności zostało również zagwarantowane w art. 47 i 51 polskiej Konstytucji. W polskim prawie prywatność można rozpatrywać w kategorii dóbr osobistych, uznanych za dobra doniosłe i zasługujące na ochronę. Artykuł 23 k.c. zawiera katalog dóbr osobistych, do których zaliczono: zdrowie, wolność, cześć swobodę sumienia, nazwisko lub pseudonim, wizerunek, tajemnicę korespondencji, nietykalność mieszkania, twórczość naukową, artystyczną, wynalazczą i racjonalizatorską. Generalnie prywatność może być rozumiana przez prawo jednostki do decydowania we wszystkich istotnych sprawach życia fizycznego i duchowego, prawo do własnej tożsamości i życia zgodnie z własnym życzeniem. Pojęcie to jest niezwykle ciężkie do zdefiniowania ze względu na niejednorodność sytuacji, w których może być zastosowane[1197].

Normy prawa międzynarodowego oraz prawa krajowego przyznają każdemu człowiekowi prawo do poszanowania swego życia prywatnego, rodzinnego, mieszkania oraz tajemnicy korespondencji. Wynika z tego, że jest niedopuszczalna nieuprawniona ingerencja w te prawa, nawet przez władze państwowe - oczywiście z wyłączeniem przypadków dopuszczanych przez prawo. Jednak gdy dojdzie do takiej ingerencji przez państwo musi zostać zachowana proporcjonalność, tak by nie przekreślić istoty prawa do prywatności i nie zagrozić godności człowieka. W przypadku konfliktu dwóch ważkich interesów, prawa do prywatności i na przykład względów bezpieczeństwa publicznego, władza państwowa powinna zachować czytelną równowagę pomiędzy tymi dwoma interesami[1198].

Problematyka prawa do prywatności w przestrzeni wirtualnej może być rozpatrywana w trzech głównych aspektach: politycznych (działalność państwa), ekonomicznych (działalność podmiotów prywatnych takich, jak przedsiębiorstwa) oraz w skali mikro (indywidualny podmiot tych praw)[1199]. Pierwszym z problemów, który należy poruszyć jest

[1197] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 322.
[1198] M. Karpiuk, *Prawo do prywatności w warunkach nowych technologii,* [w:] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia,* Warszawa 2015, s. 335-336.
[1199] P. Siuda, *Prywatność w Internecie - zarys perspektywy krytycznej*, „Kultura - Media - Teologia" 2015, nr 20, s. 40.

kwestia ochrony prywatności człowieka w cyberprzestrzeni w kontekście działań państw. Rozwój przestrzeni cyfrowej dał państwom niemalże nieograniczoną możliwość monitorowania naszych ruchów w sieci. Każda działalność w przestrzeni wirtualnej zostawia cyfrowy ślad. Dzięki Internetowi można sprawdzić z kim dana osoba się przyjaźni, jakie są jej poglądy, co kupuje *on-line* oraz jakie strony internetowe odwiedza. Wielkie „cyberkorporacje" często współpracują z organami państwa, i na ich żądanie dostarczają newralgicznych informacji o swoich użytkownikach[1200]. Możliwość cyfrowej inwigilacji jest zatem ogromna. Należy postawić sobie pytanie, jak daleko może posłużyć się władza w monitorowaniu naszych cyfrowych działań. Organy ścigania przeszukują sieć w celu ujawnienia nielegalnych zachowań takich, jak chociażby pornografia dziecięca. Cyberprzestrzeń jest również wykorzystywana do monitorowania i wykrywania cyberprzestępców i terrorystów, badania przepływu gotówki i informacji. Część władz krajowych stoi na stanowisku, iż współczesne zagrożenia są tak groźne, że musimy zrzec się części prywatności by zapewnić bezpieczeństwo państwa i jego obywateli. O ile duża część społeczeństwa wyraziłaby zgodę na przyznanie rozszerzonych kompetencji do monitorowania (i tym samym pewnego zakresu inwigilowania) przez własne państwo to zgody takiej z całą pewnością nie udzieliliby innemu państwu. Tymczasem cyberprzestrzeń znajduje się poza jakimikolwiek granicami, wobec czego inne państwa są w stanie, pod byle pretekstem (chociażby walki z terroryzmem), szpiegować obywateli innych krajów.

Innym jeszcze zagadnieniem jest zagrożenie naszej prywatności przez podmioty prywatne, czyli przedsiębiorstwa typu Facebook czy Google. Podmioty te zbierają ogromne ilości danych o swoich użytkownikach, pozycjonują treści, a za pomocą odpowiedniego zapisu w umowie monitorują nasze działania w przestrzeni cyfrowej[1201]. Zagrożenia prywatności w skali mikro wiążą się z małymi instytucjami (szkoły, placówki zdrowia), sąsiadami, kolegami oraz zupełnie obcymi osobami. Za pomocą programu szpiegowskiego, niechcianego oprogramowania czy też przez monitorowanie naszych działań w portalach społecznościowych podmioty te są w stanie uzyskać ogromne ilości informacji na nasz temat. Jest to o tyle niebezpieczne, że może to prowadzić do działań przestępczych, *cyberstalkingu,* kradzieży tożsamości, uzyskania nieuprawnionego dostępu do naszych rachunków bankowych oraz innych prywatnych informacji.

[1200] Ibidem, s. 46.
[1201] Przy zakładaniu konta na Facebooku można wyrazić zgodę na udostępnienie korporacji hasła oraz loginu do konta e-mail w celu znalezienia wspólnych znajomych. Wyrażenie zgody na tę czynność oznacza, że do każdego e-maila dostarczonego lub wysłanego z naszej poczty elektronicznej będzie miał również dostęp Facebook.

Ochrona korespondencji

Gromadzenie, przechowywanie oraz transmisja danych i informacji wiąże się z ich ochroną przed nieuprawnionym dostępem. Prawo międzynarodowe oraz prawo krajowe jako jedno z podstawowych praw człowieka wymienia ochronę korespondencji. W związku z pojawieniem się komputerów osobistych prawo to musiało zostać rozszerzone na informacje i dane zawarte w systemach informatycznych i komputerowych. Ochronie podlegać będą zatem wiadomości przesłane za pomocą komunikatorów, e-maili oraz innych elektronicznych form przesyłania informacji, które są przeznaczone do ściśle określonego adresata. Za naruszenie tajemnicy korespondencji należy uznać nieuprawnione uzyskanie dostępu do informacji, nieprzeznaczonej dla sprawcy oprzez działanie polegające na otwarciu zamkniętego pisma, ale również podłączenie się do sieci komputerowej bądź też przełamanie lub też ominięcie elektronicznego, magnetycznego, informatycznego oraz każdego innego szczegółowego zabezpieczenia sieci telekomunikacyjnej[1202].

Do uzyskania nieuprawnionego dostępu do informacji z całą pewnością może dojść na skutek włamania się do sieci, komputera, systemu użytkownika, czyli przez hacking. Kontrola korespondencji i informacji może być również dokonywana przez państwo w sposób prawnie regulowany. W polskim porządku prawnym podsłuch jest dopuszczalny jedynie w przypadku uzasadnionego przypuszczenia popełnienia poważnego przestępstwa wymienionego w art. 237 k.k. W Polsce uznaje się, że podsłuchem jest utrwalanie rozmowy telefonicznej oraz innych informacji przekazywanych za pomocą fal akustycznych, radiowych oraz elektromagnetycznych (czyli na przykład za pomocą smsa lub e-maila)[1203].

Nie sposób jest szczegółowo opisać wszystkie przysługujące prawa człowieka w kontekście działalności człowieka w przestrzeni cyfrowej. Temat ten coraz częściej jest przedmiotem orzecznictwa sądów krajowych i międzynarodowych. Jedynie przykładowo wskazać należy, że ETPCz wypowiadał się w następujących kwestiach:

[1202] P. Siejka, *Naruszenie tajemnicy korespondencji zagrożeniem bezpieczeństwa informacji*, [w:] M. Sitek, I. Niedziółka, A. Ukleja, *Wymiary ochrony informacji i polityki bezpieczeństwa. Państwo - Prawo - Społeczeństwo*, Józefów 2014, s. 123-124.
[1203] S. Kowalska, *Prawa człowieka a terror i terroryzm*, Kalisz 2008, s. 137.

- archiwów gazet internetowych na których przetrzymywane są informacje, które stanowią naruszenie dóbr osobistych bądź zniesławienie[1204],
- ochronę wizerunku w mediach internetowych[1205],
- odpowiedzialności pośredników za obraźliwe i nieodpowiednie komentarze publikowane na ich serwisach internetowych[1206].

4.4.2 Cyberprzestrzeń a ochrona danych osobowych

Z problematyką praw człowieka wiąże się również problem ochrony danych osobowych i baz danych. Przepisy obowiązujące w Unii Europejskiej okazały się niewystarczające w obliczu nowych technologicznych wyzwań. Konieczne okazało się opracowanie zupełnie nowych regulacji, dostosowanych do zmian, które nastąpiły w ostatnich latach. Ochrona osób fizycznych w zakresie przetwarzania danych osobowych jest jednym z praw podstawowych Unii Europejskiej zagwarantowanych w Karcie Praw Podstawowych[1207] oraz w Traktacie o funkcjonowaniu Unii Europejskiej[1208].

Przez cztery lata trwały prace nad wprowadzeniem nowych regulacji dotyczących ochrony dany osobowych w coraz bardziej cyfrowym świecie. 27 kwietnia 2016 roku przyjęto rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Rozporządzenie ma wejść w życie w 25 maja 2018 roku i zapewnić wysoki, ujednolicony poziom ochrony danych w całej Unii Europejskiej, przyczyniając się również do wzrostu poczucia pewności prawnej w tym zakresie. Omawiany dokument ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych - w związku z działalnością prowadzoną przez jednostkę

[1204] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10 marca 2009 r., w sprawie *Times Newspapers Ltd przeciwko Wielkiej Brytanii,* skarga nr 3002/03 oraz 233676/03 oraz Wyrok Europejskiego Trybunału Praw Człowieka z dnia 16 lipca 2013 r. w sprawie *Smolczewski i Węgrzynowski przeciwko Polsce*, skarga nr 33846/07.
[1205] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10 maja 2011 r., w sprawie *Mosley przeciwko Wielkiej Brytanii,* skarga nr 48009/08.
[1206] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10 października 2013 r., w sprawie *Delfi przeciwko Estonii* skarga nr 64569/09.
[1207] Dz. Urz. UE C 83 z 30.03.2010.
[1208] Dz.U. C 326 z 26.10.2012.

organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii. Terytorialny zakres zastosowania obejmuje również przetwarzanie danych osobowych osób przebywających w UE bądź, jeżeli przetwarzanie danych jest związane z oferowaniem towarów i usług tym osobom bądź monitorowania ich zachowań (o ile do zachowania tego dochodzi na terytorium UE).

Tego samego dnia wydana została również dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[1209]. Państwa członkowskie winny implementować dyrektywę do 6 maja 2018 roku. Przyczyną wprowadzenia nowych regulacji jest konieczność zapewnienia równorzędnego stopnia ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych przez organy sprawiedliwości, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania tym zagrożeniom. Dyrektywa ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do wymienionych celów. We wskazanych aktach prawnych UE dane osobowe zostały zdefiniowane w taki sam sposób, jako: wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego, jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[1210]. Definicja w sposób bezpośredni odnosi się, więc do identyfikacji cyfrowej osoby fizycznej przez dane o lokalizacji (na przykład GPS telefonu) bądź identyfikator internetowy.

Wobec zbliżających się dużych zmian legislacyjnych w niniejszym opracowaniu jedynie pokrótce zostanie opisane zagadnienie danych osobowych, ponieważ nowe regulacje znacznie zrewolucjonizują opisywane zagadnienie i trudno jest na razie określić, jak w praktyce będą one stosowane i interpretowane. Dane osobowe są przedmiotem

[1209] Dz.U. L 119 z 4.5.2016,
[1210] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680, art. 3 pkt 1 oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679, art. 4 pkt 1.

zainteresowania ogromnej rzeszy podmiotów, zarówno publicznych jak i prywatnych. Elektroniczny obrót danymi osobowymi niesie wiele korzyści, czyli obniżenie kosztów, zwiększenie efektywności i szybkości prowadzonych działań. Regulacje międzynarodowe i krajowe spełniają w tym przedmiocie dwie funkcje. Z jednej strony zapewniają swobodę przepływu danych, z drugiej minimalizują zagrożenia i zapewniają szeroką ochronę praw osób, których dane są przetwarzane[1211]. Przetwarzanie danych osobowych musi być prowadzone z poszanowaniem praw człowieka, ale jednocześnie przyczyniać się do postępu gospodarczego i społecznego[1212].

Za dane osobowe należy uznać te, które umożliwiają identyfikację danej osoby fizycznej. W doktrynie wskazuje się, że zupełnie obojętny jest sposób, w jaki zostaną wyrażone informacje umożliwiające identyfikację. Może to nastąpić zarówno słownie. jak i przez dźwięk, obraz, zapis informatyczny czy też w inny sposób. Za dane osobowe nie można jednak uznać informacji anonimowych, których nie da się powiązać z konkretną osobą (na przykład dane statystyczne) oraz dane osób prawnych nieposiadających osobowości prawnej[1213]. W praktyce do danych osobowych możemy zaliczyć: imię, nazwisko, adres i kod pocztowy, dzielnicę miasta, numer dokumentu w tym numer licencji uprawniającej do wykonywania zawodu, numer PESEL, NIP, numer telefonu, wizerunek czy też zdjęcie. Bezpośrednio w przestrzeni cyfrowej do danych osobowych, w niektórych przypadkach można zaliczyć loginy, nicki (nazwy użytkownika), adres e-mail, adres strony internetowej numer IP (numer identyfikujący urządzenie w sieci Internet) czy też geolokalizację (lokalizujące osobę chociażby przez odbiornik GPS w telefonie komórkowym)[1214].

Zarówno w aktach prawnych Unii Europejskiej, jak i Rady Europy podkreśla się konieczność kompetentnego przetwarzania danych osobowych. Muszą one być pozyskiwane i przetwarzane rzetelnie i zgodnie z prawem, winny być gromadzone legalnie, w określonych, usprawiedliwionych celach. Regulacje międzynarodowe kładą nacisk na możliwość aktualizacji danych osobowych, również przez zapewnienie możliwości usunięcia lub poprawienia danych nieprawidłowych lub niekompletnych. Nie mniej ważny jest również

[1211] B. Fischer, *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich*, Warszawa 2010, s. 56.
[1212] M. Karpiuk, *Ochrona danych osobowych na gruncie regulacji Unii Europejskiej*, [w:] M. Karpiuk, K. Chałubińska - Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015, s. 14.
[1213] B. Fischer, *Transgraniczność…*, s. 57-58.
[1214] L. Kępa, *Ochrona danych osobowych w praktyce*, Warszawa 2014, s. 42-63.

aspekt przechowywania danych w formie umożliwiającej identyfikację osób, których dotyczą[1215].

Przetwarzanie danych osobowych w wyszukiwarkach internetowych stało się przedmiotem głośno komentowanego wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r.[1216]. W orzeczeniu TS UE przyznał każdej osobie prawo do bycia zapomnianym, czyli prawo do żądania usunięcia jej imienia i nazwiska z wyszukiwarki internetowej. Sprawa dotyczyła obywatela Hiszpanii, którego nieruchomość została zlicytowana za długi. W wyszukiwarce Google, po wpisaniu jego danych osobowych, wciąż można było uzyskać link do ogłoszenia licytacji. Hiszpan argumentował, że spłacił zadłużenie i nie chce by jego nazwisko było łączone z dawną sprawą. Trybunał Sprawiedliwości po rozpoznaniu sprawy uznał, że operator wyszukiwarki internetowej ponosi odpowiedzialność za przetwarzanie danych osobowych, ponieważ jest również ich administratorem, czyli podmiotem, który określa cele i środki przetwarzania danych[1217]. W wyroku podkreślono, że prawo do bycia zapomnianym będzie przedstawiać się inaczej w stosunku do osób publicznych i prywatnych. Wyrok ten nie ma charakteru bezwzględnego, w żaden sposób nie ogranicza dostępu do informacji publicznej. Na podstawie wyroku nie można przyjąć, że będziemy uprawnieni do usunięcia każdej informacji o swojej osobie z cyberprzestrzeni. Możemy to uczynić jedynie w stosunku do danych niepełnych, nieistotnych lub nieaktualnych. Zaaprobować należy zaprezentowany wyrok TS UE. Prawo do bycia zapomnianym jest trafnym rozwiązaniem. Wyszukiwarki internetowe przechowują ogromne ilości danych, w tym dane osobowe oraz informacje, które mogą naruszyć nasze dobra osobiste. Skoro mamy prawo do prywatności, ochrony naszego wizerunku i dobrego imienia, to powinno nam przysługiwać realne prawo do decydowania o losie naszych danych osobowych. Jest to szczególnie istotne w dobie Internetu, który przechowuje w swych zasobach dane, które po pierwsze nie zawsze są prawdziwe, a po drugie dotyczą naszej przeszłości, a mogą negatywnie wpłynąć na nasz wizerunek. Nawet w przypadku przestępców istnieje instytucja zatarcia skazania, cyberprzestrzeń jednak „nie zapomina", w jej zasobach dane są przechowywane bez ograniczenia czasowego.

[1215] M. Karpiuk, *Ochrona…*, s. 16-34.
[1216] Wyrok Trybunału Sprawiedliwości Unii Europejskiej, z dnia 13 maja 2014 r., w sprawie *Google Spain SL i Google* Inc, sygn. akt C-131/12.
[1217] Więcej: I.C. Kamiński, Z. Warso, *Czy można zniknąć z Google'a? Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos i Mario Costeja González* (C-131/12), [w:] D. Bychawska - Sinarska, D. Głowacka, *Wirtualne media - realne problemy*, Warszawa 2014. M. Krzysztofek, *Prawo do bycia zapomnianym* i inne aspekty prywatności w epoce Internetu w prawie UE, „Europejski Przegląd Sądowy" 2012, nr 9.

Na niwie opisanego wyżej wyroku Google udostępniła formularz stanowiący wniosek o usunięcie wyników danych osobowych dotyczących naszej osoby. Każda sprawa rozstrzygana jest indywidualne. Google zastrzega sobie prawo odmowy usunięcia linku w określonych sytuacjach na przykład, gdy dotyczy on informacji o nadużyciach finansowych, postępowaniach karnych, nieprawidłowościach w wykonywanej pracy zawodowej czy też o zachowaniu przedstawicieli władz[1218].

4.4.3 Adekwatność dotychczasowych rozwiązań prawnych wobec problemów przedmiotowych cyberprzestrzeni - próba oceny

Wyniki analizy aktualnych problemów dotyczących działalności człowieka w cyberprzestrzeni oraz istniejących rozwiązań prawnych będą odmienne w zależności od przedmiotu rozważań. Zauważyć można jednak kilka cech wspólnych. Przede wszystkim podstawowym problemem w regulacji cyberprzestrzeni jest brak jednolitej, spójnej terminologii. Rozważania niniejszego rozdziału jasno ukazały, że zdefiniowanie jakiegokolwiek nowego pojęcia - chmury obliczeniowej, pieniądza wirtualnego bądź elektronicznego, czy też ustalenie definicji legalnej poszczególnych cyberprzestępstw prowadzi do wielkich rozbieżności interpretacyjnych. Brak wspólnego nazewnictwa może szczególnie utrudnić pracę organów sprawiedliwości, w tym w ramach prowadzonej pomocy prawnej oraz wprowadzić trudności w interpretacji tekstów umów zawartych za pomocą przestrzeni wirtualnej.

W pierwszej kolejności należy odnieść się do problemu zwalczania cyberprzestępczości na gruncie prawa międzynarodowego. Najważniejszym aktem prawnym o najdonioślejszym znaczeniu jest Konwencja o cyberprzestępczości. O trafności regulacji świadczy chociażby fakt, iż do konwencji przystąpiło szereg państw spoza Rady Europy, czyli Australia, Japonia, Kanada i USA. Wagę traktatu podkreśla również Unia Europejska zachęcając państwa członkowskie do natychmiastowej ratyfikacji jej postanowień.

[1218] Dane z oficjalnej strony internetowej Google https://support.google.com/legal/contact/lr_eudpa?product=websearch# [02.01.2017].

Konwencję RE implementowało do swojego porządku prawnego kilkadziesiąt państw, dziesiątki innych wprawdzie nie związały się omawianą umową międzynarodową, lecz na jej podstawie wprowadziły penalizację niektórych cyberprzestępstw do własnych porządków prawnych.

Konwencja o cyberprzestępczości jest w zasadzie jedyną wielostronną umową międzynarodową, która w jednym akcie prawnym podejmuję próbę regulacji cyberprzestępczości. Konwencja Rady Europy jest istotnym krokiem w kierunku przyjęcia uniwersalnych standardów dotyczących problematyki przestępstw popełnianych przy zastosowaniu technologii informatycznych między innymi przez zawarcie w swych postanowieniach przepisów materialnoprawnych oraz procesowych określających znamiona przestępstw oraz zasady zbierania dowodów w formie elektronicznej, ustalenia jurysdykcji karnej, ekstradycji oraz współpracy międzynarodowej, wzajemnej pomocy prawnej i wymiany informacji. Mimo ogromnego, pozytywnego wpływu konwencji o cyberprzestępczości na międzynarodową unifikację zagadnienia działań przestępczych w sieci wirtualnej nie można być obojętnym na jej niedoskonałości. Konwencja nie ujęła w swych postanowieniach wszystkich ważkich tematów, a postęp technologiczny doprowadził do pojawienia się nowych metod działania cyberprzestępców, które nie zostały ujęte w traktacie. Dorobek prawny innych organizacji międzynarodowych w przedmiocie cyberprzestępczości jest niestety rozproszony. Wydaje się, że podejmowane próby ograniczają się do uregulowania szczególnie określonych kwestii, to jest seksualnego wykorzystywania dzieci, przestępczości zorganizowanej czy też oszustw związanych z bezgotówkowymi środkami płatniczymi.

Tymczasem istotnym problemem jest ustalenie zasad bezpieczeństwa w cyberprzestrzeni. Z roku na rok zwiększa liczba incydentów komputerowych, zorganizowanych cyberataków i nowych zagrożeń, w tym związanych z cyberterroryzmem. Przestrzeń wirtualna jest środowiskiem szalenie dynamicznym, co generuje potrzebę wprowadzania zmian w zakresie prawno-organizacyjnym i systemowym. Duża część państw (w tym w ocenie Autorki Polska) jest zupełnie nieprzygotowana do możliwości wystąpienia zmasowanego ataku cybernetycznego. Wprawdzie na ostatnim szczycie NATO stwierdzono, że cyberatak może zostać uznany za naruszenie art. 5 Traktatu Północnoatlantyckiego, jednakże prawdziwym pytaniem jest to, jakie środki i działania mogą być wówczas zastosowane w przestrzeni wirtualnej oraz jakie podmioty staną w walce informacyjnej.

Najistotniejszą funkcją i zaletą przestrzeni cyfrowej dla większości przedsiębiorstw, instytucji i osób prywatnych jest możliwość szybkiej, łatwej oraz taniej wymiany towarów i usług. W obecnym stanie prawnym na gruncie międzynarodowym istnieje szereg międzynarodowych umów międzynarodowych, aktów prawnych oraz dokumentów organizacji międzynarodowych, które bezpośrednio bądź pośrednio poruszają tematykę handlu elektronicznego. Kwestie jurysdykcji mogą, w zależności od stanu faktycznego, być ustalone na podstawie nowej konwencji lugańskiej oraz rozporządzeń nr 1215/2012 bądź Rzym I i Rzym II. Ustalenie jurysdykcji właściwej wiąże się jednakże z koniecznością ustalenia właściwego łącznika jurysdykcyjnego takiego, jak „ściślejszy związek" z krajem właściwym, ustaleniem siedziby kontrahentów oraz określenia czy mamy do czynienia z zobowiązaniem pozaumownym, dwustronnie profesjonalnym czy też umową zawartą z konsumentem. Ponadto, wskazane akty prawa międzynarodowego zawierają szereg postanowień dotyczących jurysdykcji przemiennej. W tak skomplikowanym stanie prawnym najodpowiedniejszym rozwiązaniem dla stron stosunku kontraktowego jest związanie się w umowie klauzulą jurysdykcyjną. Postanowienia tego typu dość powszechnie są wprowadzane w internetowych umowach adhezyjnych. Z jednej strony można im zarzucić jednostronne narzucanie rozwiązań jednakże wydaje się, że cyberprzestrzeń oferuje tak ogromną liczbę potencjalnych kontrahentów, że jeżeli nie godzimy się na określone postanowienia wzorca umowy to z łatwością możemy wybrać innego, odpowiedniejszego dostawcę czy usługodawcę. Rozstrzygnięcie takie jest zgodne ze swobodą kontraktowania oraz zasadą autonomii stron. Brak klauzuli jurysdykcyjnej prowadzi do niepewności prawnej oraz większego problemu w dochodzeniu należnych praw. Jeżeli umowa została zawarta z kontrahentem posiadającym siedzibę w Unii Europejskiej to dochodzenie roszczeń będzie stosunkowo łatwe, więcej problemów może nastręczyć obrót pozaunijny. Kluczowe znacznie w UE ma dyrektywa o handlu elektronicznym, wprowadzająca harmonizację w obszarze przejrzystości, wymogów informacyjnych dla dostawców usług oraz kontraktów zawieranych drogą elektroniczną. Istotny wpływ na ujednolicenie przepisów dotyczących obrotu elektronicznego miały również ustawy modelowe UNCITRAL, które mimo niewiążącego charakteru stanowiły wzorzec dla wielu państw.

Wyzwaniem dla prawa międzynarodowego okazuje się ustalenie zakresu i poziomu ochrony własności intelektualnej w przestrzeni wirtualnej. Prawo międzynarodowe nie jest należycie przygotowane do wyzwań stawianych przez nowe technologie. Wydaje się, że w chwili obecnej, w zakresie prawa własności intelektualnej w cyberprzestrzeni, mamy do

czynienia z większą liczba pytań niż odpowiedzi. Brak jest zarówno na poziomie globalnym, jak i regionalnym, europejskim norm prawnych, które w sposób kompleksowy w jednym akcie uregulowałyby omawiane zagadnienie. Tymczasem w praktyce nasuwają się pytania o jurysdykcję, status prawny chmury obliczeniowej, programów i gier komputerowych, baz danych czy też usług *peer-to-peer*. Konieczne jest przyjęcie nowego paradygmatu w stosunku do korzystania z utworów w cyberprzestrzeni, zarówno w kontekście lawinowego wzrostu piractwa internetowego, jak i w odniesieniu do nowych reguł społeczeństwa informacyjnego, w których dostęp do informacji i dóbr kultury jest dobrem o szczególnym znaczeniu[1219]. Analiza międzynarodowych i europejskich aktów prawnych prowadzi do wniosku, iż istnieje pilna potrzeba opracowania jednolitego holistycznego dokumentu, który zmierzyłby się z problemem własności intelektualnej w cyberprzestrzeni. Akt taki mógłby przede wszystkim ujednolicić terminologię oraz zharmonizować najważniejsze kwestie prawnoautorskiej ochrony dzieł.

Analiza aktualnego stanu prawnego prowadzi do przekonania, iż szczególną rolę w modelowaniu i unifikacji prawa cyberprzestrzeni odgrywa *soft law*. Mimo, że prawo miękkie nie ma charakteru prawnie wiążącego to nie można go bagatelizować. Model tworzenia *soft law* odpowiada wolnościowej i oddolnej strukturze cyberprzestrzeni. Dopuszczenie do dyskusji podmiotów prywatnych oraz nowych aktorów, którym tradycyjnie nie przypisuje się atrybutu podmiotu prawa międzynarodowego, powoduje zapewnienie równowagi i proporcjonalności pomiędzy dążeniami rządów a zabezpieczeniem interesu użytkowników przestrzeni wirtualnej. Ogromne znaczenie należy przyznać rezolucjom Zgromadzenia Ogólnego ONZ oraz niewiążącym aktom unijnym. Mogą one szybko reagować na zmieniającą się sytuację technologiczno - społeczną. Następnie, *soft law* może być pewnym drogowskazem dla państw, wskazaniem pożądanego kierunku rozwoju cyberprzestrzeni. Co więcej akty o charakterze prawa miękkiego mogą być doskonałą podstawą do stworzenia konwencji wielostronnych. Jeśli zaproponowany przez rezolucję, postanowienie czy też zalecenie tryb postępowania będzie ogólnie stosowany może również doprowadzić do wykształcenia się normy zwyczajowej.

Dotychczasowe regulacje prawa międzynarodowego dotyczące cyberprzestrzeni są z zasady niewystarczające i nieadekwatne. Międzynarodowe regulacje są fragmentaryczne i rozproszone, nie kompleksowe, nie oferują jednolitej terminologii oraz co najmniej

[1219] J. Barta, R. Markiewicz. *Prawo autorskie*…, s. 647.

minimalnych norm prawnych. Na gruncie prawa karnego konwencja o cyberprzestępczości pełni rolę pewnego wzoru, zbioru minimalnych standardów w zakresie walki z działaniami przestępczymi w sieciach cyfrowych. Podobnych rozwiązań brak jednak w innych dziedzinach prawa. Przestrzeń cyfrowa szczególnie skomplikowała tematykę regulacji w obrębie praw własności intelektualnych oraz obrotu gospodarczego. Cyberprzestrzeń jest obszarem, na który w sposób naturalny wpływa technologia i nowe innowacyjne rozwiązania. Przestrzeń ta szybko inkorporuje nowości techniczne, pozostawiając prawo w tyle. Dlatego też wciąż brak jest międzynarodowych dokumentów regulujących status prawny chmury obliczeniowej, walut wirtualnych, usług cyfrowych czy też innych form działalności człowieka w cyberprzestrzeni. Wydaje się, że w chwili obecnej mamy do czynienia z *law in action*, prawem w działaniu, rozumianym jako stopniowe formułowanie się dziedziny prawa cyberprzestrzeni. Państwa i organizacje międzynarodowe mają świadomość niedoskonałości przyjętych rozwiązań i stale pracują nad nowymi regulacjami. Z tych też względów można przypuszczać, iż w kolejnych latach wydane zostanie wiele nowych propozycji legislacyjnych w zakresie prawa cyberprzestrzeni. Winny one być elastyczne, przejrzyste, efektywne, adekwatne i neutralne technologicznie.

CZĘŚĆ III

KONCEPCJA REKONSTRUKCJI STATUSU PRAWNEGO CYBERPRZESTRZENI (Z WYKORZYSTANIEM PRAWA MIĘDZYNARODOWEGO)

Rozdział 5

Identyfikacja obszarów regulacji prawnomiędzynarodowych możliwych do wykorzystania rekonstrukcyjnego wobec cyberprzestrzeni

Rozważając problemy prawa w odniesieniu do nowych technologii, w tym technologii informacyjnych nie sposób jest nie odnieść się do prawa międzynarodowego**.** Postępująca globalizacja, międzynarodowa wymiana towarów i usług, większa współzależność państw przyczynia się do unifikacji prawa, ale też zmusza do wspólnego mierzenia się z wyzwaniami współczesności, w tym w stosunku do cyberprzestrzeni. W związku z nowością zjawiska są podejmowane próby przestrzeni cyfrowej do istniejących już reżimów prawnych i przyjętych w nich rozwiązań.

W niniejszym rozdziale zostanie opisana specyfika prawa międzynarodowego oraz uniwersalizmu jego norm prawnych. Prawo to nie jest homogenicznym systemem, a w ostatnich latach nasila się jego fragmentaryzacja. Prawo międzynarodowe publiczne ze względu swoją naturalną tendencję do tworzenia uniwersalnych terminów, norm i standardów predysponuje do jego stosowania również w odniesieniu do nowych dziedzin działalności człowieka, zwłaszcza, jeżeli mają one transgraniczny i transnarodowy charakter. Historia ukazuje, iż prawo międzynarodowe nie po raz pierwszy staje w obliczu zupełnie nowego obszaru prawa oraz problemu stosowania norm właściwych. Wobec tego nasuwa się pytanie, czy prawo międzynarodowe może mieć rekonstrukcyjne zastosowanie w odniesieniu do

nowego obszaru przestrzeni wirtualnej oraz jakie normy obowiązują w przestrzeniach, które nie podlegają jurysdykcji żadnego z państw.

5.1 Specyfika prawa międzynarodowego

Prawo jest elementem, który wiąże członków wspólnoty wyznaczając normy i standardy zachowań. Prawo międzynarodowe reguluje stosunki pomiędzy różnymi podmiotami prawa międzynarodowego. Jednakże dopiero w XX wieku nastąpił niespotykany rozwój tej dziedziny prawa. Wyodrębniono zupełnie nowe gałęzie prawa międzynarodowego związane ze wzrostem stosunków społecznych (międzynarodowe prawa człowieka), doświadczeniami II wojny światowej (międzynarodowe prawo humanitarne) czy też nowymi obszarami działalności (prawo kosmiczne). Z zasady prawo związane jest ściśle z terytorium i na nim właśnie obowiązuje. W przypadku prawa międzynarodowego jest inaczej. Reglamentuje ono działania i zdarzenia o charakterze transnarodowym, przekraczające granice państw[1220]. Prawo międzynarodowe obowiązuje w przestrzeni społeczności międzynarodowej, rozumianej jako wspólnota międzynarodowa. Społecznością tą w znaczeniu węższym są państwa, a w znaczeniu szerszym również organizacje międzynarodowe i inne podmioty prawa międzynarodowego. Społeczność międzynarodowa charakteryzuje się stosunkowo małą liczbą członków, niskim stopniem zorganizowania oraz równością wobec prawa[1221]. Co więcej, społeczność ta ma charakter zmienny, ulega nieustannym przekształceniom, wciąż pojawiają się nowe państwa i znikają stare, a coraz to nowi aktorzy pretendują do bycia podmiotem prawa międzynarodowego.

Cechą charakterystyczną prawa narodów jest brak obowiązkowego sądownictwa oraz zorganizowanego aparatu przymusu. Jednakże tym, co odróżnia prawo międzynarodowe od innych gałęzi prawa jest sposób kreacji norm oraz ich moc wiążąca. Prawo międzynarodowe publiczne nie jest uporządkowanym i zamkniętym zbiorem norm. W przeciwieństwie do krajowych systemów prawa cechuje się brakiem hierarchiczności i tym samym nadrzędności norm (z wyjątkiem zapisu o pierwszeństwie stosowania Karty NZ oraz norm peremptoryjnych, norm *ius cogens*). Specyficzna jest również metoda kreacji norm

[1220] J. Pieńkos, *Prawo międzynarodowe publiczne*, Kraków 2004, s. 26.
[1221] J. Barcik, *Zagadnienia ogólne*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2014, s. 3.

prawnomiędzynarodowych. Przede wszystkim brak ustawodawcy czy rządu nadrzędnego powoduje, iż prawo jest tworzone przez podmioty prawa międzynarodowego. Normy międzynarodowe wiążą wyłącznie te państwa, które wyraziły na to zgodę wedle zasady, że umowa obowiązuje wyłącznie między stronami, które ją zawarły (*ius facit inter partes*) oraz nie ma wpływu na prawa i obowiązki państw trzecich (*pacta tertiis nec prosunt nec nocent*)[1222].

W skład źródeł prawa międzynarodowego wchodzą umowy międzynarodowe, zwyczaj, ogólne zasady prawa, orzecznictwo sądów międzynarodowych, opinie doktryny, akty jednostronne oraz uchwały organizacji międzynarodowych. Wszystkie normy prawa międzynarodowego (oprócz wskazanych wyjątków) mają jednakową moc obowiązującą i moc prawną. Pojawiają się jednak poglądy, iż tradycyjny podział nie spełnia wymogów współczesnego, globalnego świata. Zauważalna jest tendencja do nowej kreacji norm prawa międzynarodowego za pomocą środków niewiążących. *Soft law*, czyli tak zwane prawo miękkie jest rozumiane jako niewiążące zasady postępowania. Tego typu regulacje są przyjmowane w stosunkach wielostronnych, często na forum ONZ (w formie rezolucji) oraz w ramach innych organizacjach międzynarodowych. *Soft law* jest wydawane również przy współudziale organizacji pozarządowych i innych jednostek. W ostatnich latach można zaobserwować znaczny wzrost tego typu regulacji, co może być spowodowane między innymi wolnym kształtowaniem się międzynarodowego konsensusu koniecznego do zawarcia wielostronnej umowy międzynarodowej.

Należy przytoczyć pogląd Władysława Czaplińskiego i Anny Wyrozumskiej, którzy uznali, że „nie ulega wątpliwości, że podmioty prawa międzynarodowego w coraz większym stopniu posługują się instrumentami o charakterze niewiążącym, jak różnego rodzaju zasady, normy, standardy czy też innego rodzaju reguły zachowania. Pomimo tego niewiążącego charakteru twórcy ich oczekują, że będą one przestrzegane w praktyce. To polityczne i moralne zobowiązane musi być siłą rzeczy ograniczone do podmiotów współuczestniczących w ich kształtowaniu. Status prawny aktów organizacji międzynarodowych, składających się z *soft law* jest niejednolity i zależy od statusu tej organizacji. W każdym razie zasady »miękkie« mogą stanowić podstawę dla wykształcenia się norm prawnych, element pomocniczy przy ich stosowaniu, mogą być także traktowane jako składnik późniejszej praktyki państw przy dokonywaniu wykładni traktatów zgodnie z Konwencją o prawie

[1222] Ibidem, s. 5-6.

traktatów. W niektórych przypadkach rozróżnienie konsekwencji naruszenia norm »twardych« i »miękkich« może być utrudnione, zwłaszcza, jeśli w grę wchodzi zastosowanie represaliów lub retorsji. Szczególne znaczenie zyskały akty niewiążące w dziedzinach ochrony praw człowieka i ochrony środowiska, gdzie poprzedzały one niejednokrotnie zawarcie konwencji wielostronnych. Ta praktyka ułatwiła zresztą negocjowanie tekstów umów. Wspomnieć należy również o odrębnej kategorii aktów niewiążących, które z założenia nie są powiązane z jakimikolwiek umowami międzynarodowymi, ale mają wskazywać, w jakim kierunku powinny iść działania społeczności międzynarodowej (tego typu instrumenty zostały wypracowane m.in. w dziedzinie kontroli eksportu broni oraz zapobiegania finansowaniu terroryzmu)"[1223]. Z tych też względów, mimo niewiążącego charakteru, nie należy zupełnie bagatelizować norm prawa miękkiego, zwłaszcza w dziedzinach, które nie są ugruntowane w prawie międzynarodowym (bądź są uregulowane niewystarczająco). Cyberprzestrzeń jest nowym zagadnieniem, w którym niezwykle trudno jest wyodrębnić wiążące reguły międzynarodowe. *Soft law* może być znakomitym punktem wyjścia do rozmów, a następnie przyczynkiem do stworzenia umów wielostronnych w tym przedmiocie. Szczególną zaletą prawa miękkiego jest łatwość tworzenia norm i ich modyfikacji, odgórne proponowanie pewnych rozwiązań i szybkość dostosowywania nowych norm do zmieniających się stosunków społecznych, gospodarczych i technologicznych.

Prawo międzynarodowe reguluje stosunki między podmiotami prawa międzynarodowego, oprócz państw do jednostek tych można zaliczyć też inne podmioty: organizacje międzynarodowe, osoby fizyczne czy też chociażby Stolicę Apostolską. Prawo międzynarodowe w ostatnich dziesięcioleciach ulega przekształceniom. Maciej Perkowski stwierdza, że: „podmiotem prawa międzynarodowego jest ten, komu ów porządek normatywny nadaje prawa i/lub obowiązku oraz skazuje mechanizm(-y) ich kształtowania, niezależnie od formalnego rodowodu i przedmiotowego zakresu atrybutów (...). W nauce stosunków międzynarodowych spotkać możemy pojęcie »aktorów międzynarodowych« lub »aktorów stosunków międzynarodowych«. Wydaje się, że dla podmiotowości prawa międzynarodowego zakres podmiotowy owych pojęć stanowi swoisty rezerwuar potencjału. Oznacza to, że - o ile wszystkie podmioty prawa międzynarodowego są jednocześnie aktorami stosunków międzynarodowych - o tyle wśród aktorów stosunków międzynarodowych podmiotowość prawnomiędzynarodową posiada jedynie ta część, której

[1223] W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2014, s. 15-16.

bezpośrednio dotyczą konkretne prawa i obowiązki prawnomiędzynarodowe oraz towarzyszące im mechanizmy aktywności".[1224] Tradycyjnie podmiotami prawa międzynarodowego były wyłącznie państwa, obecnie coraz więcej aktorów międzynarodowych pretenduje do tego miana.

Część znawców przedmiotu uważa, że za szczególne podmioty prawa międzynarodowego można uznać międzynarodowe spółki publiczne nazywane również przedsiębiorstwami wielonarodowymi czy też spółkami międzynarodowymi. Jako przykład korporacji ponadnarodowych są wymieniane przedsiębiorstwa takie, jak Exxon Mobil, General Motors czy Simens[1225]. Korporacje te są „prywatnymi przedsiębiorstwami, obejmującymi po kilka wzajemnie powiązanych nadrzędną strukturą podmiotów jawnych. Klasyfikowane są w zależności od wielkości i rozmieszczenia. (...) Podejmowane są próby określenia zbioru zasad, jakie cechują tego rodzaju podmioty na arenie międzynarodowej"[1226]. Cechą, która przesądza o ich podmiotowości, jest istnienie międzynarodowych ustaleń zapewniających współpracę pomiędzy prywatnymi oraz międzynarodowymi przedsiębiorstwami. Wskazuje się, że: „kwestia ich podmiotowości prawnej zależeć będzie od zróżnicowania istoty podmiotu prawa krajowego i podmiotu prawa międzynarodowego. Jeśli danemu podmiotowi zostanie przypisane wiele uprawień przy równoczesnym dostatecznym wyłączeniu go spod prawa krajowego, możemy mówić o podmiocie prawa międzynarodowego, jednak wymagane jest przy tym wnikliwe rozpatrzenie okoliczności"[1227]. Jako przykład międzynarodowej spółki publicznej wymienić można INTELSAT - największego na świecie komercyjnego dostawcę usług telekomunikacyjnych i operatora satelitarnego, który powstał jako struktura międzyrządowa.

Zmiana w zakresie postrzegania podmiotowości prawnomiędzynarodowej jako wyłącznego atrybutu państw została zapoczątkowana „rewolucyjną" opinią doradczą MTS w sprawie Reparacji[1228], w której przyznano podmiotowość również innym, pozapaństwowym

[1224] M. Perkowski, *Kształtowanie się podmiotowości prawa międzynarodowego*, [w:] J. Menkes (red.), *Prawo międzynarodowe. Księga pamiątkowa prof. Renaty Szafarz*, Warszawa 2007, s. 457-458.
[1225] Więcej na temat korporacji ponadnarodowych w: K. Karski, *Problem statutu korporacji ponadnarodowych w prawie międzynarodowym (globalizacja a podmiotowość prawa międzynarodowego),* [w:] E. Dynia (red.), *Nauka prawa międzynarodowego u progu XX wieku. Materiały pokonferencyjne*, Rzeszów 2003.
[1226] M.N. Shaw, *Prawo ...*, 2006, s. 164.
[1227] Ibidem, s. 164-165.
[1228] Opinia doradcza Międzynarodowego Trybunału Sprawiedliwości (ICJ Reports 1949, s. 187 i 189), opinia dostępna na oficjalnej stronie internetowej Międzynarodowego Trybunału Sprawiedliwości: na: http://www.icj-cij.org/docket/index.php?p1=3&p2=4&case=4&p3=4 [10.02.2017].

podmiotom[1229]. Inni autorzy odnosząc się do zagadnienia podmiotowości stwierdzili, że: „pojęcie podmiotowości prawnej pociąga za sobą konieczność przeanalizowania określonych koncepcji prawnych, takich jak jej status i zdolność, a także istota i zakres poszczególnych praw i obowiązków. Status danego podmiotu może być zdeterminowany pewnymi prawami i obowiązkami, podczas gdy pojęcie zdolności wiąże jego status z poszczególnymi prawami i obowiązkami. Wszystko to obowiązuje w granicach wyznaczonych przez dany system prawny, który stanowi o podmiotowości, jej istocie i definicji. Dotyczy to w szczególności prawa międzynarodowego. Odpowiednie spojrzenie na dany system niezmiennie wykaże jego wpływ na podejmowanie zagadnień tożsamości i istoty międzynarodowych osób prawnych"[1230]. Zakres uprawnień do kształtowania prawa będzie, zatem wynikał z zakresu podmiotowości prawnomiędzynarodowej tego podmiotu. Jest to szczególnie istotne w zakresie prawa tworzonego przez organizacje międzynarodowe, ponieważ ich uprawnienia będą wynikały z kompetencji nadanych im przez państwa. Jedynie część z nich będzie miała realny wpływ na kształt prawa międzynarodowego[1231].

Niezwykle cenne są rozważania Malcolma N. Shaw dotyczące kreowania prawa przez podmioty prawa międzynarodowego. Autor stoi na stanowisku, że „jednym ze znaczących wyróżników współczesnego prawa międzynarodowego jest istnienie wielu uczestników działań na scenie międzynarodowej. Odnosi się to do państw, organizacji międzynarodowych, regionalnych, pozarządowych, spółek prawa publicznego i prywatnego oraz osób fizycznych. Nie wszystkie z wymienionych podmiotów są podmiotami prawa, chociaż mogą w pewnym stopniu wywierać jakiś wpływ na sprawy międzynarodowe. Na podmiotowość międzynarodową składa się uczestnictwo w życiu społeczności międzynarodowej w połączeniu z pewną formą akceptacji ze strony tej społeczności. Ten ostatni element zależeć będzie od bardzo wielu czynników, w tym również od rodzaju danej podmiotowości. Może się on przejawiać w wielu formach i niektórych przypadkach może wynikać z praktyki. Jest on też odzwierciedleniem konkretnych potrzeb. Podstawowymi tego wyznacznikami są w konkretnych przypadkach poszczególne dziedziny prawa międzynarodowego. Szczególnie istotne w kreowaniu i odzwierciedlaniu uczestnictwa oraz podmiotowości w prawie międzynarodowym są prawa człowieka, prawo dotyczące konfliktów zbrojnych oraz

[1229] M. Perkowski, *Koncepcja „non-state actors" a umiędzynarodowienie regionów*, „Białostockie Studia Prawnicze" 2012, z. 12, s. 97.
[1230] M.N. Shaw, Prawo…,2006, s. 134-135.
[1231] K. Bagdan - Kurluta, *Podmioty prawa międzynarodowego*, [w:] B. Wierzbicki (red.), *Prawo międzynarodowe publiczne*, Białystok 2001, s. 69-70

międzynarodowe prawo gospodarcze”[1232]. W ostatnich latach w tworzeniu prawa coraz częściej w charakterze konsultacyjnym czy doradczym biorą udział najróżniejsze podmioty i instytucje. Trend ten jest również zauważalny w przypadku kreowania norm prawa międzynarodowego w cyberprzestrzeni. Największe korporacje międzynarodowe w dziedzinie IT, przedstawiciele dostawców usług i użytkowników czynnie uczestniczą w dyskusji na temat pożądanego kształtu norm zgłaszając jednocześnie problemy i zastrzeżenia.

Przedmiot, czyli funkcje prawa międzynarodowego zmieniają się na przestrzeni wieków. Po II wojnie światowej najważniejszym zadaniem prawa międzynarodowego było przede wszystkim zapewnienie pokoju i bezpieczeństwa, przyśpieszenie rozwoju gospodarczego państw, a więc wyrównanie dysproporcji w stosunkach społeczno--gospodarczych na świecie[1233]. W ostatnich latach przed prawem międzynarodowym stoją zupełnie nowe wyzwania takie, jak szeroko rozumiana ochrona praw człowieka oraz ochrona środowiska naturalnego. Wojciech Góralczyk i Stefan Sawicki jako podstawowy przedmiot prawa międzynarodowego wskazują dwa zasadnicze rodzaje spraw:

1. Regulowanie stosunków wewnętrznych państw - autorzy wskazują, że jest to tradycyjna i główna funkcja prawa międzynarodowego, które:
    - określa sytuację państwa w społeczności międzynarodowej (w stosunku do innych państw) wskazując na przykład na prawa zasadnicze państw,
    - określa ogólne zasady postępowania państw we wzajemnych stosunkach na przykład ustalając zasadę pokojowego rozstrzygania sporów międzynarodowych,
    - determinuje zindywidualizowane, konkretne stosunki pomiędzy podmiotami międzynarodowymi na przykład udzielenie pomocy humanitarnej,
    - ustala formy stosunków wzajemnych pomiędzy państwami na przykład przez regulację prawa dyplomatycznego i konsularnego,
    - normuje kwestię zasięgu władzy terytorialnej poszczególnych państw na przykład przez ustalanie granic państwowych,
    - reguluje normy postępowania na obszarach niepodlegających suwerenności żadnego państwa, czyli na morzu pełnym i w przestrzeni kosmicznej.

[1232] M.N. Shaw, *Prawo…*,2006, s. 134-135.
[1233] M. Kun - Buczko, *Zagadnienia wstępne*, [w:] M. Kun - Buczko (red.), *Prawo międzynarodowe publiczne. Zarys problematyki*, Białystok 2011, s. 19.

2. Oddziaływanie na stosunki wewnętrzne państw - w zakresie niezbędnym dla zapewnienia skuteczności norm prawa międzynarodowego[1234].

Na uwagę zasługuje występujący w doktrynie pogląd na temat znacznej ewolucji prawa międzynarodowego w XX wieku, związanej z postępem naukowym i technologicznym. W ostatnich dziesięcioleciach nastąpił wzrost działalności społecznej i gospodarczej wymagającej współpracy na szczeblu międzynarodowym. Rozwój nauki spowodował, iż powstały zupełnie nowe działy prawa takie, jak prawo kosmiczne, prawo atomowe czy prawo regulujące status prawny szelfu kontynentalnego oraz dna mórz i oceanów. Uległy też zmianie istniejące działy prawa, które ewoluowały z powodu szybkiego i znacznego postępu techniki. Ponadto, akcentuje się, iż powstanie międzynarodowych i regionalnych organizacji międzynarodowych przyczyniło się do wyodrębnienia nowego obszernego zespołu norm prawnych rozumianych jako prawo organizacji międzynarodowych[1235]. W obliczu wyzwań współczesności tradycyjne funkcje pozostają wciąż aktualne. To właśnie prawo międzynarodowe jest odpowiednie do wyznaczenia granic jurysdykcyjnych państw, ustalenia norm w obszarach niepodlegających suwerenności żadnego z państw oraz ustalenia norm postępowania w najbardziej istotnych kwestiach.

Podzielić należy stanowisko Remigiusza Bierzanka, że: „ukształtowany w dobie przechodzenia od średniowiecza do epoki nowożytnej międzynarodowy porządek prawnopolityczny, polegający na istnieniu państw suwerennych sprawujących władzę i wyłącznie kompetentnych do regulowania stosunków w granicach terytorium państwowego, podlega obecnie istotnym przeobrażeniom. Wprawdzie nadal istnieją i działają państwa, których rządy z różnych powodów często podkreślają suwerenność i niezawisłość państwową, to jednak pod naporem rosnącej współzależności międzynarodowej we wszystkich dziedzinach treść suwerenności - jako wyłącznego prawa do reglamentacji stosunków na obszarze swego terytorium i w odniesieniu do własnych obywateli - ulega stopniowej erozji. Coraz więcej zagadnień uważanych dotychczas za należące do wyłącznej wewnętrznej kompetencji państwa staje się przedmiotem reglamentacji międzynarodowej; przykładem tego trendu rozwojowego są liczne umowy międzynarodowe dotyczące ochrony praw człowieka. Następuje ewolucja od prawa państw do prawa na rzecz człowieka i do prawa mającego zaspokoić potrzeby ludzkości (ochrona praw człowieka, rozwój gospodarczy i społeczny,

[1234] W. Góralczyk, S. Sawicki .*Prawo międzynarodowe publiczne w zarysie,* Warszawa 2015, s. 20 - 21.
[1235] R. Bierzanek, *Zarys historii prawa międzynarodowego,* [w:] R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Warszawa 2005, s. 68-69.

ochrona środowiska naturalnego, ochrona planety). Proces internacjonalizacji stosunków regulowanych dotychczas przez prawo wewnętrzne odbywa się również w drodze dostosowania ustawodawstwa wewnętrznego do zasad i reguł zawartych w umowach międzynarodowych i uchwałach organizacji międzynarodowych; występuje ten rozwojowy trend wyraźnie w prawie komunikacyjnym zwłaszcza w prawie morskim i lotniczym. Istotnym przeobrażeniom ulega struktura prawa międzynarodowego. Obok zasad i reguł określających prawa i obowiązki państw, głównie w zakresie rozgraniczenia między kompetencjami przysługującymi państwom, prawo międzynarodowe staje się w coraz większym stopniu prawem organizującym wielostronną współpracę państw w różnych dziedzinach o żywotnym znaczeniu dla społeczności międzynarodowej, która z tradycyjnego luźnego zrzeszenia przekształca się w bardziej zintegrowaną społeczność"[1236]. Prawo międzynarodowe coraz częściej musi mierzyć się z nowymi problemami. Konieczna stała się regulacja nie tylko stosunków międzypaństwowych, ale powstałych też na przestrzeni ostatnich dekad abstrakcyjnych obszarów (w teorii). Społeczność międzynarodowa coraz częściej domaga się zmian w regulacjach, próbując nawet oddolnie normować ważne dla niej kwestie.

Po II wojnie światowej można było zaobserwować pewne nowe trendy i cechy współczesnego prawa międzynarodowego. Do najważniejszych z nich należą: wprowadzenie zakazu użycia siły i groźby jej użycia, konieczność zapewnienia pokojowego współistnienia państw, przewartościowanie pojęcia suwerenności, ogromny wzrost liczby organizacji międzynarodowych oraz jakościowy i ilościowy rozrost prawa międzynarodowego. Nie powinno się również pominąć postępującego procesu wertykalizacji systemu prawa międzynarodowego, który jest związany nie tylko z koncepcją norm *iuris cogentis* oraz z wymogiem z art. 103 Karty NZ, lecz przede wszystkim występującą złożonością problemów prawnych współczesnego świata. Przede wszystkim w zglobalizowanym świecie, państwa napotkały trudności w samodzielnym rozwiązywaniu problemów. Efektywniejsze okazało się przekazanie części kompetencji organizacjom międzynarodowym. Wywnioskować z tego można, że coraz większe znaczenie przypisuje się pozapaństwowym podmiotom prawa międzynarodowego. Co więcej na arenie międzynarodowej pojawiają się nowi aktorzy

[1236] Ibidem, s. 69.

aspirujący do statusu podmiotów prawa międzynarodowe (wielonarodowe korporacje, globalne partnerstwa publiczno - prywatne)[1237].

Rozwój prawa międzynarodowego przypada na XX i XXI wiek, a w obliczu postępu cywilizacji i postępujących procesów globalizacyjnych tendencja ta będzie się nasilać. Zaobserwować można trend do zacieśniania współpracy międzynarodowej oraz rosnącą współzależność państw. Systematyczne rozszerzanie prawa międzynarodowego zmusza do redefiniowania niektórych pojęć oraz zmierzenia się z wyzwaniami współczesności. Postęp technologiczny wymusza wprowadzenie nowych regulacji, ponieważ działalność człowieka wkracza nowe obszary legislacyjne, z którymi prawo międzynarodowe nie miało jeszcze do czynienia. Rola prawa międzynarodowego również ulega zmianie. W okresie zimnej wojny najistotniejszym celem było zapewnienie pokojowego współistnienia wrogich państw. Obecnie świat staje przed innymi zagrożeniami terroryzmem międzynarodowym, falą uchodźców, zaostrzeniem konfliktów międzynarodowych czy też działalnością człowieka w nowej przestrzeni, czyli przestrzeni wirtualnej.

5.2 Prawo międzynarodowe wobec przestrzeni

Przestrzeń w prawie międzynarodowym może być rozumiana rozmaicie: jako ogólnie pojęte terytorium, jako obszar geograficzny bądź też jako obszar ludzkiej działalności. Teoretycy prawa międzynarodowego dzielą terytorium na dwie zasadnicze grupy. Pierwsza z nich podlega suwerenności państwowej i uznawana jest za terytorium państwowe. Druga nie podlega władzy państwowej żadnego z państw. Do tej grupy należy zaliczyć przestrzeń kosmiczną, morze otwarte, dno mórz i oceanów oraz Antarktykę. Uznaje się powszechnie, że wymienione obszary pozostają poza granicami jurysdykcji państwowej, wobec czego, nie można rozciągać na nie zwierzchnictwa terytorialnego, gdyż jako wspólne dziedzictwo ludzkości (łac. *res communis*) nie podlegają zawłaszczeniu[1238].

[1237] J. Barcik, *Zagadnienia* ..., s. 19-24.
[1238] J. Symonides, *Terytorium w prawie międzynarodowym*, [w:] R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Warszawa 2005, s. 193.

Terytorium (łac. *territorium*) jest to obszar lądowy, powietrzny i morski o określonych granicach[1239]. Janusz Gilas wyróżnia terytorium: powszechnego użytku (łac. *res usum publicum*), wspólne (łac. *res communis*) oraz terytorium niczyje. Za terytorium wspólne autor uznaje dno mórz i oceanów poza granicami jurysdykcji państwowej. Za terytorium powszechnego użytku zaś uznaje się morze pełne oraz przestrzeń kosmiczną[1240].

Według innego, bardziej szczegółowego podziału, prawo międzynarodowe wyróżnia cztery rodzaje terytoriów:

1) „podległe suwerenności poszczególnych państw,
2) zależne, które nie podlegają suwerenności żadnego państwa, lecz za ich stosunki międzynarodowe odpowiedzialność ponoszą inne państwa, ewentualnie organizacje międzynarodowe,
3) niepodlegające suwerenności żadnego państwa, lecz dostępne dla wszystkich państw w celu ich działalności w zakresie określonym przez umowy międzynarodowe i prawo zwyczajowe,
4) niczyje, które mogą być poddane suwerenności jakiegoś państwa"[1241].

Terytorium pełni w systemie prawa międzynarodowego centralną rolę wyrażoną między innymi przez zasadę jego nienaruszalności, poszanowania terytorialnej integralności oraz zakazu ingerencji w sprawy wewnętrzne innych państw. Władza w tym obszarze może być w pewnym stopniu ograniczona przez normy prawa międzynarodowego, wzrost współzależności pomiędzy podmiotami prawa międzynarodowego oraz przemiany ekonomiczne i technologiczne. Państwa przekazują również część swoich kompetencji władczych organizacjom międzynarodowym[1242].

Malcolm N. Shaw, prowadząc rozważania na temat władzy wyłącznej państw w zakresie terytorium podkreśla różnorodność następstw wynikających ze zmiany właściciela terytorium w prawie międzynarodowym i w prawie wewnętrznym. W prawie międzynarodowym zmiana właściciela określonego terytorium powoduje zmianę suwerenności oraz władz rządzących tym obszarem (i wszystkich związanych z tym konsekwencji takich, jak obywatelstwo czy system prawny). W przypadku zmiany własności

[1239] T. Srogosz, *Terytorium*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2014, s. 205.
[1240] J. Gilas, *Prawo międzynarodowe*, Toruń 1995, s. 174-175.
[1241] W. Góralczyk, S. Sawicki,.... 2015, s. 168.
[1242] M.N. Shaw, *Prawo*... 2006, s. 267-268.

w prawie wewnętrznym jej skutki nie są tak daleko idące[1243]. Z tych też względów terytorium odgrywa szczególną rolę w prawie międzynarodowym, ponieważ jest granicą działalności i władzy państw.

Problematykę przestrzeni ponadziemskiej poruszano już w czasach starożytnych. W kodyfikacji justyniańskiej uznawano powietrze, wodę, morze i wybrzeże morskie za rzecz wspólną dla wszystkich: *Et quidem naturali iure omnium communia sunt illa: aer, aqua profluens, et mare, et per hoc litora maris*. W średniowieczu terytorium opisywano jako *Cuius est solum, eius est usque ad coelum et ad inferos* bądź też jako *dominus soli est dominus coeli*. Początek XX wieku, w związku z pojawieniem się pierwszych samolotów, przyniósł rozłam w zakresie stanowiska dotyczącego przestrzeni powietrznej. Część przedstawicieli doktryny opowiadało się za wolnością przestworzy i wolnością żeglugi morskiej, inni z kolei stali na stanowisku, że przestrzeń powietrzna rozciągająca się nad danym terytorium winna podlegać kompetencji wyłącznie tego państwa[1244]. Kolejnym rewolucyjnym momentem był ogromy rozwój techniczny, który pozwolił na eksplorację nieznanych dotąd obszarów: przestrzeni kosmicznej oraz dna mórz i oceanów.

5.3.1 Przestrzeń państwowa - terytorium

Na terytorium państwa składa się obszar lądowy, morski (jeżeli państwo ma dostęp do morza) oraz powietrzny[1245]. Powszechnie uznaje się, że „terytorium państwowe stanowi przestrzeń, na którą rozciąga się władza suwerenna (zwierzchnictwo terytorialne) określonego państwa"[1246]. W prawie międzynarodowym nie ma jednej, ogólno przyjętej definicji terytorium państwowego. Według Władysława Czaplińskiego i Anny Wyrozumskiej terytorium państwa można zdefiniować jako: „wycinek powierzchni Ziemi, ograniczony od innych państw i podlegający jurysdykcji danego państwa (zgodnie z tzw. teorią kompetencji)"[1247]. Janusz Symonides z kolei twierdzi, że: „terytorium państwowe stanowi tak przedmiot władzy państwowej (co wyraża się przede wszystkim w dysponowaniu nim), jak

[1243] Ibidem, s. 268.
[1244] J. Pieńkos, op. cit., s. 612-613.
[1245] T. Srogosz, *Terytorium*..., s. 207.
[1246] W. Góralczyk, S. Sawicki, *Prawo międzynarodowe publiczne w zarysie,* Warszawa 2007, s. 177.
[1247] W. Czapliński, A. Wyrozumska, op. cit., s. 186.

przestrzeń, w granicach której państwo wykonuje władzę w sposób wyłączny i pełny w stosunku do osób, rzeczy i zdarzeń. Terytorium jest także podstawą wykonywania kompetencji państwowych (personalnych) poza jego granicami”[1248]. Podobną definicję proponuje Jan Białocerkiewicz, który uznaje, że „terytorium państwowe można określić jako, oznaczony co do tożsamości, wycinek globu ziemskiego, stanowiący niezbędny element państwa, będący przedmiotem władzy państwowej, w obrębie którego państwo wykonuje władzę w sposób suwerenny w stosunku do osób, rzeczy i zdarzeń nawet poza jego granicami na podstawie zwyczajowej albo umownej normy prawa międzynarodowego”[1249].

W doktrynie wyróżnia się cztery podstawowe teorie dotyczące terytorium:

1) teorię przedmiotową - wywodząca się jeszcze z czasów feudalnych, uznającą terytorium za przedmiot (obiekt) władzy państwowej, którą można uznać bądź za własność opartą na *dominium publicum*, czyli na zasadach prawa publicznego bądź opartą na *imperium,* czyli na zasadach suwerenności,
2) teorię podmiotową - występuje bądź jako część szerszej teorii przestrzennej bądź jako koncepcja samodzielna, w której państwo uznawane jest za „quasi - biologiczny” organizm, gdzie terytorium pełni nijako rolę „ciała”; zwolennicy tej teorii porównują prawo do terytorium do prawa przysługującego człowiekowi do decydowania o swojej osobie ze skutkami *erga omnes*,
3) teorię przestrzenną - pojawiła się w drugiej połowie XIX wieku; terytorium uznane jest za przestrzeń, w obrębie której władza państwowa wykonuje swoje kompetencje, uznaje się, że terytorium nie jest wówczas przedmiotem, lecz granicą władzy państwowej,
4) teorię kompetencji - uznaje, że państwo jest „porządkiem prawnym” bądź „porządkiem normatywnym” wobec czego terytorium jest strefą kompetencji państwa, w której porządek prawny obowiązuje[1250].

Terytorium państwa składa się z kilku elementów: przestrzeni lądowej, morskiej i powietrznej. W skład terytorium morskiego wchodzą wody wewnętrzne i morze terytorialne, a w państwach archipelagowych, także wody położone pomiędzy wyspami archipelagu oraz znajdująca się nad nimi przestrzeń powietrzna. Terytorium państwa ma postać trójwymiarową, co oznacza, że roztacza sie nie tylko nad jego terytorium, lecz również

[1248] J. Symonides, op. cit., s. 196.
[1249] J. Białocerkiewicz, *Prawo międzynarodowe publiczne. Zarys wykładu*, Toruń 2007, s. 148.
[1250] J. Symonides, op. cit., s. 193.

obejmuje obszar podziemny, w teorii sięgający aż do wnętrzna kuli ziemskiej. Faktyczna granica ograniczona jest jedynie technicznymi możliwościami eksploatacji tych obszarów[1251]. Z kolei terytorium powietrzne państwa rozciąga się nad terytoriami lądowymi, morskimi wodami wewnętrznymi, wodami archipelagowymi oraz morzem terytorialnym. Górna granica nie została do tej pory ustalona w sposób niebudzący wątpliwości, zazwyczaj uznaje się, że granice państwa sięgają około 80-100 kilometrów ponad powierzchnią ziemi. W przestrzeni powietrznej na przykład państwa traktatami międzynarodowymi wprowadzają pewne uprawnienia dla państw trzecich związanych z żeglugą międzynarodową[1252].

Władza państwowa na terytorium jest określona mianem zwierzchnictwa terytorialnego bądź suwerenności. Władza wykonywana na terytorium państwa jest władzą najwyższą, pełną i wyłączną, co oznacza, że wszystkie osoby i rzeczy znajdujące się w jego granicach podlegają władzy i prawu tego państwa[1253]. Znawcy tematu uznają, że: „zwierzchnictwo terytorialne obejmuje władzę podlegającą z jednej strony na sprawowaniu w obrębie terytorium wszystkich działań i funkcji właściwych państwu, z drugiej zaś - na zapobieganiu wykonywania analogicznych działań ze strony innych podmiotów”[1254]. Wobec powyższego wyróżnić należy dwa podstawowe aspekty zwierzchnictwa terytorialnego: pozytywny oraz negatywny. Skutkiem pierwszego z nich jest „podporządkowanie władzy państwowej wszystkiego, co się na terytorium danego państwa znajduje i jego obrębie zachodzi”. Stanowi to konsekwencję rzymskich zasad *qui in territorio meo est, etiam meus subditus est,* a w odniesieniu do rzeczy - *quidquid est in territorio, est etiam de territorio*. Pozytywnym aspektem zwierzchnictwa terytorialnego jest również zwierzchnictwo personalne, które jest wynikiem obywatelstwa i przynależności państwowej. Zwierzchnictwo terytorialne w aspekcie negatywnym oznacza, że państwo może wykluczyć działanie jakiejkolwiek obcej władzy na swoim terytorium, co przejawia się w monopolu ustanawiania organów władzy państwowej, jurysdykcji oraz działalności służb publicznych[1255].

Mimo, że władza państwa jest wyłączna, pełna i najwyższa, to nie ma charakteru absolutnego. Wojciech Góralczyk i Stefan Sawicki akcentują, że „zasada zwierzchnictwa terytorialnego, a więc suwerenności terytorialnej oznacza jednak, że:

[1251] Ibidem, s. 196-197.
[1252] J. Białocerkiewicz, op. cit., s. 150.
[1253] W. Góralczyk, S. Sawicki, ... 2015, s. 169-170.
[1254] J. Symonides, op. cit., s. 199.
[1255] Ibidem, s. 199-200.

1. ten, kto powołuje się na ograniczenie zwierzchnictwa terytorialnego, tzn. pełnej władzy i kompetencji państwa, musi dowieść, iż ograniczenie takie wynika z konkretnej normy prawa międzynarodowego, wiążącej dane państwo,
2. każde państwo związane jest tylko takimi ograniczeniami, jakie uznało, przyjmując konkretne zobowiązania międzynarodowe"[1256].

Należy odnieść się także do sposobów nabycia terytoriów oraz ustalania metod ich granic państwowych. Granice są wyznaczane zazwyczaj w formie umowy międzynarodowej (na przykład traktat pokoju) lub umowy dwustronnej. Granice są wytyczane orograficznie - zgodnie z rzeźbą terenu bądź geometrycznie - liniami prostymi łączącymi dwa wybrane punkty[1257]. Pojęcie granicy nie jest sporne, powszechnie uznaje się, że jest to „płaszczyzna pionowa lub pozioma, która oddziela terytorium jednego państwa od innego państwa lub od terytorium nie podlegającym niczyjej jurysdykcji"[1258]. Ustalenie granic terytorium państwowego, co do zasady nie budzi większych wątpliwości. Przez wieki państwa działały w granicach swoich terytoriów, ponieważ nie było problemów z ustaleniem ich granic - miały one fizyczny, namacalny charakter. Dopiero ekspansja człowieka związana z rozwojem techniki - początkowo w zakresie morza otwartego - a w ostatnich dekadach w kwestii przestrzeni powietrznej i kosmosu oraz dna mórz i oceanów, doprowadziła do wykształcenia się koncepcji przestrzeni międzynarodowych.

5.3.2 Przestrzeń międzynarodowa

W prawie międzynarodowym zostały wyróżnione przestrzenie, które nie podlegają suwerenności żadnego z państw i w związku z tym - na podstawie zwyczaju bądź umowy międzynarodowej - nie może być na nie rozciągnięta władza suwerenna żadnego z państw. Obszary te - morze pełne, dno mórz i oceanów oraz kosmos są przestrzeniami, które mogą być używane i eksploatowane przez wszystkie państwa na zasadzie równości. Cechą wspólną tych przestrzeni jest również obowiązek pokojowego ich wykorzystania, wolność

[1256] W. Góralczyk, S. Sawicki, *Prawo międzynarodowe publiczne w zarysie,* Warszawa 2013, s. 181.
[1257] J. Pieńkos, op. cit., s. 245-246.
[1258] J. Białocerkiewicz, op. cit., s. 155.

prowadzonych badań oraz równość korzystania przez wszystkie państwa, organizacje międzynarodowe i inne podmioty prawa międzynarodowego[1259].

Koncepcja wspólnego dziedzictwa ludzkości została zaprezentowana w 1967 roku przez Aldo Cocca oraz Arvida Pardo w trakcie wystąpień przed organami ONZ. W zamierzeniu miała stanowić uzupełnienie niejasności występujących w prawie międzynarodowym w odniesieniu do wykorzystania zasobów kosmosu oraz morza otwartego. Została uznana za rewolucyjną oraz szybko stała się hasłem państw rozwijających się, dążących do określonych rozwiązań prawnych w zakresie przestrzeni morza otwartego i kosmosu. „Postawa ta wyrażała wolę tych państw zapewnienia sobie określonych korzyści nieosiągalnych dla państw pozbawionych technologicznych możliwości prowadzenia takiej działalności. Dyplomatyczna walka o wprowadzenie koncepcji wspólnego dziedzictwa ludzkości do prawa pozytywnego była jednakże walką o coś więcej niż preferencyjny (dla krajów rozwijających się) podział korzyści wynikających z tej eksploatacji. Była ona również walką o nowy kształt prawa międzynarodowego"[1260]. Podmiotem wspólnego dziedzictwa ludzkości jest oczywiście ludzkość, rozumiana jako „wszyscy", „obecne i przyszłe pokolenia", „wszystkie narody i wszystkie ludy" czy po prostu wszystkich bez rozróżnienia. W doktrynie pojawił się również sprzeczny pogląd, który uznawał, że ludzkość nie może być uznana za podmiot prawa międzynarodowego i tym samym nie może mieć kompetencji do przedkładania prawnomiędzynarodowych roszczeń. Idea wspólnego dziedzictwa ludzkości w odniesieniu do przestrzeni kosmicznej oraz morza otwartego, dna mórz i oceanów zawiera wspólne elementy składowe. Zaliczyć do nich należy zakaz zawłaszczania, wolność badań naukowych, wolność pokojowego wykorzystywania, ochronę środowiska naturalnego, równowagę ekologiczną, międzynarodowy reżim regulujący poszukiwanie i eksploatację ich zasobów naturalnych oraz sprawiedliwy i słuszny podział korzyści - przy preferowanym uwzględnieniu potrzeb krajów rozwijających się[1261].

Malcolm N. Shaw odnosząc się do obszarów uznanych za wspólne dziedzictwo ludzkości wyjaśnia: „koncepcja wspólnego dziedzictwa ludzkości charakteryzuje się pewnymi elementami wspólnymi z innymi teoriami prawa międzynarodowego. Podobnie jak w przypadku *res communis* obszary objęte tym reżimem nie mogą stać się przedmiotem zawłaszczenia żadnego państwa. Nie dotyczy ich zasada suwerenności i nie mogą być niczyją

[1259] W. Czapliński, A. Wyrozumska, op. cit., s. 208.
[1260] J. Stańczyk, *Pojęcie wspólnego dziedzictwa ludzkości w prawie międzynarodowym*, „Państwo i Prawo" 1985, z. 9, s. 56.
[1261] Ibidem, s. 59-61.

własnością. Ponadto nie może być mowy o żadnych uprawnieniach jurysdykcyjnych poza instytucjonalnymi ramami ustanawiającymi reżim wspólnego dziedzictwa ludzkości. O ile jednak reżim *res communis* zapewnia wolność dostępu, badania i eksploatacji danego obszaru, o tyle reżim wspólnego dziedzictwa ludzkości, dotyczący wspomnianych wyżej terenów, ściśle reguluje zagadnienia związane z ich badaniem i eksploatacją, ustanawia mechanizmy zarządzania tymi obszarami oraz wprowadza kryterium sprawiedliwego podziału korzyści płynących z tego rodzaju działalności"[1262]. Koncepcja wspólnego dziedzictwa ludzkości jest pomysłem stosunkowo młodym, dlatego też dopiero w przyszłości okaże się jak ukształtuje się praktyka w tym obszarze. Co ciekawe Janusz Stańczyk w swoim opracowaniu z 1985 roku wskazał, że przyjęcie tej koncepcji skłania do jej transpozycji na inne dziedziny prawa międzynarodowego - chociażby w odniesieniu do technologii czy zasobów roślinnych ziemi[1263].

W 1998 roku Darrel C. Menthe zaproponował, by cyberprzestrzeń uznać za czwartą - obok morza otwartego, przestrzeni kosmicznej i Antarktyki- przestrzeń międzynarodową. Autor założył, że jurysdykcja w cyberprzestrzeni wymaga jasnych zasad zakorzenionych w prawie międzynarodowym i tylko stosując te normy sądy wszystkich państw mogłyby rozstrzygnąć jednolicie swoje kompetencje[1264]. Należy pokrótce opisać także podstawowe zasady rządzące przestrzeniami międzynarodowymi niepodlegającymi niczyjej suwerenności. Następnie konieczne będzie zbadanie, czy i jakie zasady mogłyby zostać zastosowane w odniesieniu do przestrzeni wirtualnej, a które z nich zupełnie nie przystają do nowej cyfrowej przestrzeni działalności człowieka.

5.3.2.1 Morze otwarte oraz dno mórz i oceanów

Panująca obecnie zasada wolności mórz nie zawsze była powszechnie akceptowalna. W okresie podbojów morskich Portugalia i Hiszpania podzieliły między siebie Ocean Atlantycki, a następnie Ocean Spokojny[1265]. Idea wolności morza otwartego, zwana również

[1262] M.N. Shaw, *Prawo*... 2011, s. 339-340.
[1263] J. Stańczyk, op. cit., s. 63-64.
[1264] D.C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, "Michigan Telecommunications and Technology Law Review" 1998, t. 4, nr 1, s. 71. Koncepcja ta zostanie przedstawiona w szóstym rozdziale niniejszej dysertacji.
[1265] W. Góralczyk, S. Sawicki, ... 2013, s. 220.

morzem pełnym, pierwszy raz została teoretycznie uzasadniona przez Hugo Grocjusza w pracy pod tytułem *Mare liberum* (Wolność mórz) z 1609 roku, w której dowodził, że wolność mórz jest dana przez przyrodę, a bogactwo jego zasobów wystarczy dla wszystkich narodów[1266]. Grocjusz do opisu statusu prawnego morza otwartego użył pojęć: rzeczy niczyjej (*res nullius*), rzeczy wspólnej (*res communis*) oraz rzeczy publicznej (*res publicum*). Obecnie część doktryny postuluje by uznać morze otwarte za *res usus publicum*[1267].

Zgodnie z Konwencją o morzu pełnym[1268], sporządzoną w Genewie w 29 kwietnia 1958 roku, za morze pełne uznaje się wszelkie części morza nienależące do morza terytorialnego ani do państwowych wód wewnętrznych. Artykuł 2 konwencji stwierdza, że: morze pełne jest otwarte dla wszystkich narodów. Żadne z państw nie może prawnie próbować poddania jakiejkolwiek jego części swej suwerenności. Korzystanie z wolności morza pełnego odbywa się na warunkach określonych w konwencji o morzu pełnym i w innych normach prawa międzynarodowego. Wolność morza pełnego obejmuje między innymi (zarówno dla państw posiadających, jak i nieposiadających dostępu do morza) wolność żeglugi, rybołówstwa, przelotu oraz układania podmorskich kabli i rurociągów. Stwierdzono również, że korzystanie przez każde państwo z tych swobód, jak i z innych uznanych przez podstawowe zasady prawa międzynarodowego, powinno odbywać się przy rozsądnym uwzględnieniu interesów, jakie mogą mieć inne państwa, wynikających z wolności morza pełnego.

Konwencja Narodów Zjednoczonych o prawie morza sporządzona w Montego Bay 10 grudnia 1982 roku[1269] rozszerza wskazany wyżej katalog o dwie kolejne wolności - wolność budowania sztucznych wysp oraz innych instalacji dozwolonych przez prawo międzynarodowe, a także wolność badań naukowych. W opinii Jana Białocerkiewicza, w Konwencji o prawie morza z 1982 roku znalazły się przepisy, które świadczą o postępie prawa międzynarodowego publicznego. Zaliczył on do nich zastrzeżenie morza otwartego wyłącznie dla celów pokojowych oraz nieważność roszczeń zgłaszanych przez państwa do poddania swej suwerenności jakiejkolwiek części morza pełnego[1270].

Wolność mórz, pierwotnie, opierała się na założeniu, że korzystanie z morza pełnego nie jest szkodliwe, a zasoby morskie są niewyczerpane. Współczesne intensywne

[1266] J. Symonides, op. cit., s. 230.
[1267] D. Pyć, *Prawo oceanu światowego. Res usus publicum*, Gdańsk 2011, s. 38-39.
[1268] Dz.U. z 1963 r., Nr 33, poz. 187.
[1269] Dz.U. z 2002 r., Nr. 59, poz. 534.
[1270] J. Białocerkiewicz, op. cit., s. 192.

użytkowanie mórz wskazuje na to, iż wymienione wyżej przesłanki przestały być aktualne. Rozwój techniki połowów doprowadził do wyniszczenia łowisk, zagrażając wyginięciem części gatunków. Nie można również obecnie uznać, by korzystanie z morza otwartego było zupełnie nieszkodliwe. Intensywność połowów spowodowała konieczność wytyczenia tras morskich, a przewożone towary takie, jak ropa naftowa czy niebezpieczne substancje chemiczne w przypadku ich wycieku grożą zanieczyszczeniem wód morskich. Z tych też względów niezbędne okazało się podjęcie działań mających na celu ograniczenie pełnej wolności morza otwartego[1271]. Wolność eksploatacji bogactw morskich nazywana wolnością rybołówstwa straciła swój nieograniczony charakter. By zapobiec przełowieniu i wyniszczeniu łowisk podpisano szereg umów międzynarodowych, w których wyrażono zgodę na ograniczenie połowów niektórych gatunków, wprowadzono okresy ochronne, zakaz używania określonych narzędzi i wprowadzenie kwot połowowych[1272]. Wolność mórz i oceanów nie jest zatem bezwzględna. Utrzymanie łowisk i dalszych połowów w przyszłości będzie możliwe tylko w przypadku zastosowania odpowiednich międzynarodowych kroków - ograniczających, w wymaganym zakresie, wolność rybołówstwa. Opisywany obszar - mimo, że nie podlega jurysdykcji żadnego z państw - musi być chroniony przez całą społeczność międzynarodową.

Statki pływające po morzu otwartym podlegają jurysdykcji i prawu państwa przynależności statku - to jest państwa bandery. W doktrynie wskazuje się również, iż bandera ma zapewnić pewność obrotu - pomiędzy statkiem a państwem powinien istnieć rzeczywisty łącznik. Statek, który pływa pod banderą dwóch lub więcej państw, nie mając do tego żadnego tytułu prawnego, jest traktowany jak statek morski nieposiadający żadnej przynależności państwowej. Istotne jest istnienie faktycznego związku pomiędzy statkiem a państwem, w którym jest on zarejestrowany. W przypadku nastąpienia jakiegokolwiek zdarzenia powodującego odpowiedzialność karną lub dyscyplinarną kapitana, bądź jakiejkolwiek innej osoby, to właściwym do wszczęcia i prowadzenia postępowania będzie państwo, pod którego banderą statek pływa (*lex banderae*) lub państwo obywatelstwa sprawcy czynu (*lex patriae*)[1273]. Należy zasygnalizować, że istnieje kilka wyjątków od zasady wyłącznej jurysdykcji państwa bandery statku. Jako przykład wymienić można piractwo morskie, handel niewolnikami, czy środkami odurzającymi bądź substancjami

[1271] W. Góralczyk, S. Sawicki, ...2013, s. 221-222.
[1272] Ibidem, s. 225.
[1273] J. Białocerkiewicz, op. cit., s. 192-193.

psychotropowymi, prawo pościgu czy nielegalne nadawanie audycji[1274]. Wymienione wyżej czynniki, destabilizują bezpieczeństwo na morzu z jednej strony narażając na bezpośrednie niebezpieczeństwo życie ludzkie, z drugiej generując straty materialne oraz wprowadzając poczucie zagrożenia. Z tych też względów uznano, że za walkę z piractwem morskim (powiązanym nierzadko z organizacjami przestępczymi oraz terrorystycznymi[1275]) odpowiedzialna jest cała społeczność międzynarodowa.

Na uwagę zasługuje wykorzystanie morza otwartego w celach wojskowych. Konwencja o prawie morza z 1982 r. zakazuje działań wojskowych wymierzonych w integralność terytorialną, suwerenność czy też niepodległość polityczną państwa. Oznacza to, że dozwolone jest przeprowadzanie na morzu pełnym operacji wojskowych, o ile nie mają one charakteru działań agresywnych. Skoro jednak zgodnie z art. 88 Konwencji morze pełne jest wykorzystywane wyłącznie do celów pokojowych, to nasuwa się pytanie, jakie operacje wojskowe będą uznane za pokojowe. Prawo do prowadzenia działań operacyjnych obejmuje przeprowadzanie manewrów i ćwiczeń, testowanie uzbrojenia, patrolowanie, obserwacja, rozpoznanie, kotwiczenie oraz prowadzenie badań hydrograficznych i wojskowych. W art. 2 ust. 4 Karty Narodów Zjednoczonych wymieniono akty wymierzone przeciwko integralności terytorialnej lub niezawisłości innego państwa[1276]. W piśmiennictwie podkreśla się, że militarne wykorzystanie morza otwartego wynika bardziej z zasady wolności mórz niż z konwencji o prawie morza. Respektowanie wymienionych wyżej zasad w ocenie Andrzeja Makowskiego nie wynika z traktatu, lecz raczej z interesów państw i praktyki historycznej potęg morskich[1277].

Za przestrzeń międzynarodową niepodlegającą jurysdykcji żadnego z państw uznano również dno morskie i oceaniczne pozostające poza granicami państwowymi. Granicą jurysdykcji i władzy państwa nadbrzeżnego jest zewnętrzna granica szelfu kontynentalnego. Przez wieki obszar ten pozostawał poza zainteresowaniem praktyków i teoretyków prawa. Gdy jednak okazało się, że teren ten jest zasobny w bogactwa mineralne takie, jak nikiel, miedź czy mangan, a możliwości technologiczne umożliwiają wydobycie tych zasobów

[1274] M.N. Shaw, *Prawo*... 2006, s. 355-356.
[1275] Por.: J. Padzik, *Piractwo morskie: historyczna ciągłość i zmiana*, „Bezpieczeństwo narodowe" 2013, nr 1(25).
[1276] L. Łukaszuk, *Współpraca i spory międzynarodowe na morzach. Wybrane zagadnienia prawa, polityki morskiej i ochrony środowiska*, Warszawa 2009, s. 232-233.
[1277] A. Makowski, *Koncepcja wolności mórz w działalności wojskowej mocarstw morskich na wszechoceanie*, [w:] U. Jackowiak, I. Nakielska, P. Lewandowski (red.), *Współczesne problemy prawa. Księga pamiątkowa dedykowana profesorowi Jerzemu Młynarczykowi*, Gdynia 2011, s. 36-40.

Zgromadzenie Ogólne ONZ w 1970 roku uznało, że dno mórz i oceanów znajdujące się poza granicami jurysdykcyjnymi państw stanowi wspólne dziedzictwo ludzkości[1278].

Postanowienie to zostało następnie powtórzone w art. 136 Konwencji o prawie morza z 1982 r., w którym stwierdzono, że dno mórz i oceanów oraz jego zasoby stanowią wspólne dziedzictwo ludzkości. Do zasad rządzących nim zaliczono między innymi pokojowe wykorzystanie, wolność badań naukowych, prowadzenie działalności w tym obszarze dla dobra całej ludzkości, wprowadzając równocześnie zasadę niewysuwania roszczeń i zawłaszczania jakiejkolwiek części obszaru[1279].

Żadne państwo nie może zgłaszać roszczeń ani wykonywać praw suwerennych nad tym obszarem. Eksploatacja zasobów dna morskiego winna być przeprowadzana w interesie całej ludzkości. By spełnić ten postulat powołany został organ nadzorczy - Organizacja Dna Morskiego (ang. *Sea-Bed Authority*). Ma ona za zadanie dzielenie wydobytych zasobów pomiędzy wszystkie państwa, ze szczególnym uwzględnieniem państw rozwijających się i narodów, które nie uzyskały pełnej niepodległości bądź innego autonomicznego statusu przyznanego przez Organizację Narodów Zjednoczonych[1280]. W celu ustalenia zasad wydobycia przyjęto Kodeks wydobywczy, który reguluje proces działań górniczych w obszarze dna morskiego. Wprowadzono regułę, według której państwa strony popierają współpracę naukową i techniczną w opisywanym obszarze. Współpraca ma następować przez pomoc techniczną, rozwijanie programów szkoleń, współpracę naukową o morzu i technologii oraz programach ochrony i zachowania środowiska morskiego[1281].

Wolność mórz stanowi kluczową zasadę gwarantującą pokojowe wykorzystanie przestrzeni mórz i oceanów. Ta głęboko zakorzeniona zasada ma zastosowanie zarówno w czasie wojny, konfliktu zbrojnego jak i w czasie pokoju. Po II wojnie światowej państwa nadbrzeżne w coraz większym stopniu wysuwały roszczenia do kolejnych obszarów wolnego morza otwartego, między innymi przez strefy ekonomiczne. W tym stanie rzeczy Andrzej Makowiecki, postawił tezę, że „w ramach tych nowych i poszerzanych morskich obszarów wyłączonych, większość państw prawo wolności żeglugi i prawa przelotu ceni sobie o wiele mniej, niż bliższe im interesy narodowe. W tym przypadku, zasada terytorialnej suwerenności uzyskuje przewagę nad zasadą wolności mórz i nie widać oznak by tendencja ta uległa

[1278] W. Góralczyk, S. Sawicki, ... 2013, s. 226.
[1279] J. Białocerkiewicz, op. cit., s. 205.
[1280] J. Barcik, *Międzynarodowe prawo morza*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne. 2 wydanie*, Warszawa 2014, s. 252-253.
[1281] L. Łukaszuk, *Współpraca…*, s. 85.

zmianie. Kryteria *mare liberum*, takie jak wolność korzystania i otwarty dostęp, zostają w ramach tych nowych stref morskich zastąpione przez krańcowo odmienne zasady zarządzania oparte na kontrolowanym, uregulowanym i ograniczonym wykorzystaniu i dostępie"[1282]. Żądania państw polegające na wysuwaniu roszczeń do coraz większych obszarów przybrzeżnych stanowi pewną tendencję do rozszerzenia przez nie władztwa jurysdykcyjnego. Sytuacja ta ma miejsca zazwyczaj wówczas, gdy jest to uzasadnione polityką bądź interesem danego państwa.

5.3.2.2 Przestrzeń kosmiczna

Zainteresowanie prawa międzynarodowego publicznego statusem prawnym przestrzeni kosmicznej przypada na drugą połowę XX wieku. Pierwszy raz w historii ludzkości posiadana wiedza i technologia pozwoliła wznieść się w przestrzeń kosmiczną. Świat stanął w obliczu zupełnie nowych możliwości, a znawcy prawa w obliczu nowych wyzwań legislacyjnych. Eksploracja przestrzeni kosmicznej spowodowała narodzenie się dwóch zupełnie nowych reżimów prawnych - normujących status prawny przestrzeni kosmicznej oraz status prawny przestrzeni powietrznej. Do chwili obecnej nie przyjęto jednej, jasno zakreślonej granicy delimitacji dwóch wymienionych wcześniej przestrzeni. Uznaje się, że za granicę tę można przyjąć orbitę geostacjonarną (około 35800 km od powierzchni ziemi - granica ta była przyczyną licznych sporów w doktrynie) bądź bardziej ogólnikowo wysokość około 80-100 km nad powierzchnią ziemi[1283].

W doktrynie wykształciły się dwa różne podejścia w zakresie rozgraniczenia przestrzeni kosmicznej - podejście przestrzenne oraz funkcjonalne. Pierwsze z wymienionych opiera się na rozgraniczeniu przestrzeni według właściwości geofizycznych atmosfery. Zwolennicy tego podejścia uznają, że granicą jest występowanie gazów tworzących powietrze - a zatem granica pomiędzy atmosferą a przestrzenią kosmiczną. Pogląd ten jest krytykowany przez przedstawicieli nauki, ponieważ nie zostało jednoznacznie rozstrzygnięte czy przestrzeń powietrzna obejmuje troposferę i stratosferę (około 40 km nad powierzchnią ziemi) czy też rozciąga się wyżej na mezosferę, termosferę i egzosferę. Inna koncepcja, za granicę przyznaje

[1282] A. Makowski, *Koncepcja…*, s. 42.
[1283] T. Srogosz, *Międzynarodowe prawo lotnicze i kosmiczne*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2014, s. 268-269.

kryterium możliwości technicznych eksploatacji statków powietrznych (również około 35-40 km nad powierzchnią ziemi). Kolejną propozycją było przyjęcie granicy na wysokości, na której są umieszczane sztuczne satelity, czyli na orbicie okołoziemskiej (najniższa możliwa orbita to 120 km). Wobec trudności w rozgraniczeniu tych przestrzeni pojawiła się w doktrynie koncepcja funkcjonalna, która nie wprowadza rozgraniczenia pomiędzy przestrzenią powietrzną a przestrzenią kosmiczną, lecz uznaje, że jurysdykcja w przestrzeni kosmicznej ustalana byłaby na podstawie prowadzonej działalności eksploratorskiej. Oznaczałoby to, że państwo eksploatujące dany obiekt posiadałoby nad nim pełną jurysdykcję. Przedstawiciele doktryny uznali jednak, że i ta teoria nie odpowiada realiom współczesnego świata[1284]. Problematyką ustalenia granicy przestrzeni kosmicznej od lat 50 zajmował się również Komitet *ad hoc* do spraw Pokojowego Wykorzystania Przestrzeni Kosmicznej ONZ, jednakże udało się opracować jednoznacznej odpowiedzi, która jednoznacznie wskazałaby tę granicę[1285].

Pierwsze państwa, które umieściły w kosmosie sztuczne satelity, czyli USA oraz ZSRR, uczyniły to zakładając, że działanie takie nie jest zakazane przez prawo międzynarodowe. Inne państwa nie protestowały przeciwko tym posunięciom, wobec czego uznano, że milcząco wyraziły zgodę na taką praktykę, zgadzając się równocześnie na przelot obiektów kosmicznych ponad ich terytoriami. W ten sposób powoli zaczął tworzyć się zwyczaj wolności wykorzystywania oraz badania przestrzeni kosmicznej[1286]. Stosunkowo szybko powstało też prawo nieszkodliwego przelotu statków kosmicznych nad terytorium innych państw. Jan Białocerkiewicz stanął na stanowisku, że: „trzy doniosłe wydarzenia: wysłanie w kosmos pierwszego sztucznego satelity Ziemi - »Sputnik - I« (4 października 1957 r.), pierwszy lot załogowy - J. Gagarin (12 kwietnia 1961 r.) oraz wylądowanie pierwszego człowieka na Księżycu - 20 lipca 1969 r. (N. Amstrong. E. Aldrin), otworzyły ponownie trochę zapomniany problem władztwa państw *ad infinitum*. Brak protestów przeciwko lotowi satelity bezzałogowego z jednej strony i wprowadzenie do przestrzeni statków kosmicznych bez pytania o zgodę pozostałych państw z drugiej strony, ukształtowały w krótkim czasie, zwyczajową normę prawa międzynarodowego - wolność wykorzystania i badania przestrzeni kosmicznej, a tym samym odrzucona została koncepcja władztwa *ad infinitum*."[1287] Wraz z rozwojem nowej dziedziny prawa międzynawowego - prawa

[1284] W. Czapliński, A. Wyrozumska, op. cit., s. 192-193.
[1285] Ibidem, s. 192.
[1286] W. Góralczyk, S. Sawicki, … 2013, s. 237.
[1287] J. Białocerkiewicz, op. cit., s. 206.

kosmicznego - przyjęto zasadę niezawłaszczalności kosmosu, wolności przeprowadzanych tam badań naukowych oraz zasadę nieszkodliwego przelotu statków kosmicznych. Wymienione wyżej zasady zostały zastosowane na wzór morskich praw wolności żeglugi, nieszkodliwego przepływu i badań naukowych. Prawo międzynarodowe, wobec braku regulacji właściwych, sięgnęło (na zasadzie analogii) do znanego już systemu prawa to jest prawa morza.

Maciej Żylicz stanął na stanowisku, że „podstawowe i trwałe znaczenie powstałego z dnia na dzień prawa nieszkodliwego (tj. nie zagrażającego bezpieczeństwu obcych państw) przelotu statków kosmicznych - przy wspomnianych ograniczeniach tego prawa - polegało przede wszystkim na tym, że:

- stało się ono punktem wyjścia dla uznania i potwierdzenia prawem pisanym innych zasad nowego prawa kosmicznego, dotyczących wolności lotów kosmicznych (skoro wolne są loty satelitarne, chyba także w fazie wznoszenia i opadania, to tym bardziej muszą być wolne dalej sięgające loty kosmiczne), a w pewnym sensie także statusu prawnego przestrzeni kosmicznej i statków kosmicznych, odpowiedzialności za ich używanie, niezawłaszczalności przestrzeni kosmicznej i ciał niebieskich, zakazu umieszczania broni oraz współpracy międzynarodowej w kosmosie,
- zapoczątkowana została przy tym tendencja rozwoju międzynarodowego prawa kosmicznego z odchodzeniem od kryteriów terytorialnych na rzecz kryteriów funkcjonalnych. Inaczej niż w prawie morskim z coraz dalej idącymi roszczeniami państw do stref specjalnych, czy też szelfu kontynentalnego, rozszerzanego jeszcze na *outer shelf*”[1288].

Sytuacja prawna przestrzeni kosmicznej została uregulowana w wielu umowach międzynarodowych. Układ o zasadach działalności państw w zakresie badań i użytkowania przestrzeni kosmicznej łącznie z Księżycem i innymi ciałami niebieskimi, sporządzony w Moskwie, Londynie i Waszyngtonie 27 stycznia 1967 roku[1289] (układ o przestrzeni kosmicznej) wprowadził, w artykułach I - VII kilka podstawowych zasad postępowania w przestrzeni kosmicznej:

[1288] M. Żylicz, *O początkach międzynarodowego prawa kosmicznego*, [w:] Z. Galicki, T. Kamiński, K. Myszona - Kostrzewa, *Wykorzystanie przestrzeni kosmicznej. Świat - Europa - Polska*, Warszawa 2010, s. 14.
[1289] Dz.U. z 1968 r., Nr 14, poz. 82.

1) badanie i użytkowanie przestrzeni kosmicznej wraz z Księżycem i innymi ciałami niebieskimi jest prowadzone dla dobra i w interesie ludzkości,
2) zapewnienie wolność badań naukowych,
3) przestrzeń kosmiczna nie podlega zawłaszczeniu w formie suwerenności, użytkowania lub okupacji,
4) przestrzeń kosmiczna będzie wykorzystywana w sposób pokojowy (demilitaryzacja i neutralizacja),
5) państwa ponoszą odpowiedzialność za szkody kosmiczne wyrządzone w przestrzeni kosmicznej, powietrznej jak i na powierzchni ziemi.

Ponadto, układ o przestrzeni kosmicznej stanowi w art. VII, że państwo posiada jurysdykcję nie tylko nad zarejestrowanym obiektem wpuszczonym w przestrzeń kosmiczną, ale również nad znajdującą się na jego pokładzie załogą. Postanowienia te zostały następnie potwierdzone Konwencją o rejestracji obiektów wpuszczonych w przestrzeń kosmiczną, otwartą do podpisu w Nowym Jorku 14 stycznia 1975 roku[1290].

Wolność przestrzeni kosmicznej nawiązuje do koncepcji wspólnego dziedzictwa ludzkości (ang. *common heritage of mankind*). W ocenie Łukasza Kułagi koncepcja wspólnego dziedzictwa ludzkości musi być rozpatrywana również w odwołaniu do obszarów morskich znajdujących się poza jurysdykcją państw. Wskazuje on, że „odwołanie się *per analogiam* do wskazanego reżimu, w braku wystarczającej praktyki państw oraz trybunałów międzynarodowych dotyczących przestrzeni kosmicznej, wydaje się najbardziej optymalną formułą dla zdekodowania zakresu obowiązywania i charakteru koncepcji wspólnego dziedzictwa ludzkości w kontekście prawa kosmicznego (...) Dla dokonania rekonstrukcji reguł prawa kosmicznego nie zostanie natomiast wykorzystany reżim prawny dotyczący Antarktydy (...) uznać należy, że nie znajduje on praktycznego zastosowania dla określenia statusu prawnego przestrzeni kosmicznej, ponieważ jest oparty na zasadzie zamrożenia istniejących roszczeń terytorialnych szeregu państw”[1291]. Pogląd ten jest trafny, ponieważ przestrzeń kosmiczna oraz morze pełne wykazują wiele podobieństw (wolność przepływu, wolność przelotu, wolność badań naukowych), dlatego też część zasad prawa może być stosowana na zasadzie podobieństwa. O ile sytuacja morza pełnego oraz przestrzeni

[1290] Dz. U. z 1979 r., Nr 5, poz. 22.
[1291] Ł. Kułaga, *Przestrzeń kosmiczna - jako wspólne dziedzictwo ludzkości. Kontrowersje wokół Porozumienia regulującego działalność państw na Księżycu i innych ciałach niebieskich*, [w:] Z. Galicki, T. Kamiński, K. Myszona - Kostrzewa, *Wykorzystanie przestrzeni kosmicznej. Świat - Europa - Polska*, Warszawa 2010, s. 26.

kosmicznej jest ogólnie akceptowana, o tyle Antarktyda nie ma ostatecznie uregulowanej sytuacji prawnej.

Koncepcja wspólnego dziedzictwa ludzkości zawsze wzbudzała kontrowersje w nauce prawa międzynarodowego. Niektórzy specjaliści stali na stanowisku, że nie określa ona konkretnych norm i zobowiązań międzynarodowych, lecz stanowi jedynie odzwierciedlenie politycznych aspiracji części państw[1292]. Inni wskazywali, iż jest podstawową zasadą zapewniającą ogólne zobowiązania prawne dotyczące obszarów znajdujących sie poza jurysdykcją wszystkich państw. W tym kontekście wspólne dziedzictwo ludzkości było porównywane do takich zasad, jak suwerenna równość czy wolność mórz. Status wspólnego dziedzictwa ludzkości może być nadany jedynie przez społeczność międzynarodową przestrzeniom, które winny być wykorzystywane na potrzeby całej ludzkości, dla wspólnego dobra. Ma to zapewnić wspólne czerpanie korzyści oraz równy dostęp do zgromadzonych tam zasobów. Łukasz Kułaga podkreśla, że „brak orzecznictwa międzynarodowych lub krajowych trybunałów w tym zakresie oraz niewielka liczba odnoszących się do niej porozumień międzynarodowych powoduje, że konieczna jest każdorazowa ocena jej charakteru i znaczenia w kontekście regulacji prawnej, w której jest zawarta"[1293].

Do koncepcji wspólnego dziedzictwa ludzkości odniesiono się w układzie o przestrzeni kosmicznej z 1967 r., gdzie w pierwszym akapicie art. 1 przyjęto, że badanie i użytkowanie przestrzeni kosmicznej, łącznie z Księżycem i innymi ciałami niebieskimi, są prowadzone lub wykonywane dla dobra i w interesie wszystkich krajów, niezależnie od stopnia ich rozwoju gospodarczego czy naukowego i stanowi dorobek całej ludzkości. Wskazuje się, że „kluczowym elementem artykułu 1 akapit 1 Układu z 1967 r. wydaje się być koncepcja »wspólnego interesu« (i »wspólnej korzyści«), która ma stanowić podstawowy wymóg przy badaniu użytkowania przestrzeni kosmicznej. Większość przedstawicieli doktryny zgadza się, że odzwierciedla on przekonanie państw, iż przestrzeń kosmiczna stanowi wspólne dobro tj. rzecz wspólną (*res communis*), która wyklucza możliwość wysuwania jakichkolwiek roszczeń przez poszczególne kraje"[1294].

[1292] S. Ervin, *Law in a Vacuum: The Common Heritage Doctrine in Outer Space Law*, "Boston College International and Comparative Law Review" 1984, nr 2, t. 7, s. 424-425.
[1293] Ł. Kułaga, op. cit., s. 29-30.
[1294] Ibidem, s. 30-31.

Mimo kontraktowego przyjęcia koncepcji wspólnego dziedzictwa ludzkości pojęcie to jest interpretowane w praktyce niejednolicie[1295]. Łukasz Kułaga wskazuje, że „państwa prowadzące aktywną politykę kosmiczną są raczej skłonne postrzegać przestrzeń kosmiczna jako »morze otwarte«, tj. obszar umożliwiający pełną swobodę działalności, przy uwzględnieniu podstawowych reguł układu z 1967 r., ale zasadniczo bez oglądania się na interesy wszystkich, czy nawet większości krajów świata. Praktyka państw realizujących politykę kosmiczną w zakresie wykorzystywania kosmosu np. na potrzeby obserwacji ziemi czy telekomunikacyjnie wyraźnie pokazuje, że podstawowy jest tu ich własny interes natomiast brak znaczących protestów ze strony krajów rozwijających się sprzyja akceptacji takiej działalności mimo wyraźnie odmiennych postanowień Układu z 1967 r. Dowodem tego również działalność komercyjna takich podmiotów jak Intelsat[1296] czy Intersputnik[1297]. Znacząca jest również praktyka wysyłania przez państwa rozwinięte satelitów szpiegowskich, które korzystają z przestrzeni kosmicznej realizując wyłącznie interesy państwa wysyłającego”[1298]. Realizowanie polityki państwowej kierując się głównie własnym interesem nie jest niczym nadzwyczajnym w stosunkach międzynarodowych. O ile jednak przypadku prawa morza czerpanie korzyści wynikających z wolności morskich jest realizowane przez szereg podmiotów, o tyle w przypadku przestrzeni kosmicznej liczba tych podmiotów jest ograniczona (głównie ze względu na duże koszty działalności kosmicznej).

Przytoczyć również należy poprawiony projekt Kodeksu Postępowania Unii Europejskiej w sprawie Przestrzeni Kosmicznej[1299] z 2010 roku, w którym zaakcentowano konieczność pokojowego jej użytkowania w kontekście pojawiających się nowych wyzwań. Wobec rosnącego wykorzystania przestrzeni kosmicznej uznano, że wzrasta potrzeba przejrzystości wykonywanych tam czynności oraz lepszej wymiany informacji pomiędzy zainteresowanymi podmiotami. W ocenie UE najlepszym rozwiązaniem będzie utworzenie zbioru najlepszych praktyk, będących uzupełnieniem prawa pozytywnego i mających na celu zapewnienie bezpieczeństwa w przestrzeni kosmicznej. W art. 2 omawianego aktu

[1295] Por.: P. Meyer, *Outer Space and Cyberspace: A Tale of Two Security Realms*, [w:] A.M. Osula, H. Rõigas (red.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Talin 2016.
[1296] Intelsat, właściwie: Intelsat Ltd. – największy na świecie komercyjny operator satelitarny i dostawca usług telekomunikacyjnych.
[1297] Intersputnik (ros. Международная организация космической связи„Интерспутник”, pol. Międzynarodowa Organizacja Łączności Kosmicznej „Intersputnik”) – organizacja międzynarodowa, zajmująca się realizacją łączności satelitarnej.
[1298] Ł. Kułaga, op. cit., s. 36-37.
[1299] Council of the European Union Revised Draft Code of Conduct for Outer Space Activities, Bruksela 22.10.2010, http://www.consilium.europa.eu/uedocs/cmsUpload/st14455.en10.pdf [28.12.2016].

zaproponowano podstawowe zasady, którymi winny kierować się państwa podpisujące dokument:

1) wolność dostępu, korzystania i badania z przestrzeni kosmicznej, wykorzystanie obiektów kosmicznych w celach pokojowych, przy poszanowaniu ochrony, bezpieczeństwa i integralności obiektów na orbicie zgodnie z prawem międzynarodowym,
2) niezbywalne prawo do indywidualnej lub zbiorowej samoobrony zgodnie z postanowieniami Karty NZ,
3) odpowiedzialność państw członkowskich za prowadzone działania naukowe, komercyjne i wojskowe w celu promowania badania i wykorzystania przestrzeni kosmicznej oraz do podjęcia wszelkich odpowiednich środków w celu zapobiegnięcia sytuacji, w której przestrzeń kosmiczna stałaby się miejscem konfliktu,
4) odpowiedzialność państw członkowskich do podjęcia wszelkich możliwych środków oraz współpracy w dobrej wierze w celu wyeliminowania szkodliwych działań prowadzonych w przestrzeni kosmicznej[1300].

Przedstawiciele doktryny wyrażają pogląd, iż mamy obecnie do czynienia z „nową optyką", będącą skutkiem procesu reinterpretacji Układu z 1967 roku prowadzącą do wniosku, że przestrzeń kosmiczna jest obszarem o analogicznym statusie do morza otwartego[1301]. Państwa zdały sobie sprawę, iż przestrzeń kosmiczna będzie coraz szerzej wykorzystywana - również do działalności komercyjnej. Można również pokusić się o stwierdzenie, iż popularna będzie turystyka kosmiczna. Jednakże już dziś jednym z najbardziej pożytecznych sposobów wykorzystania przestrzeni kosmicznej jest utworzenie szybkiego systemu komunikacji i sieci telekomunikacyjnej. Organizacje takie, jak INTELSAT oraz ITU rozwijają system satelitarny, dzięki któremu możemy korzystać z szybkiej łączności, Internetu czy sygnału GPS.

Dostęp do przestrzeni kosmicznej jest wolny - w tym również do ciał niebieskich. Powszechnie uznaje się, że przestrzeń ta nie może być zawłaszczona przez państwa ani przez ogłoszenie suwerenności ani przez użytkowanie, okupację lub inną formę zajęcia. Jak już wcześniej zostało wskazane kosmos jest obszarem wolnym do badań i użytkowania, jednakże

[1300] Council of the European Union Revised Draft Code of Conduct for Outer Space Activities, Bruksela 22.10.2010, http://www.consilium.europa.eu/uedocs/cmsUpload/st14455.en10.pdf [28.12.2016].
[1301] Ł. Kułaga, op. cit., s. 38.

użytkowanie przez wszystkie państwa może następować wyłącznie w celach pokojowych. Z postulatem tym łączy się zatem zakaz demilitaryzacji ciał niebieskich.

Należy zastanowić się, czy zaprezentowane wyżej reguły mogą być bezpośrednio zastosowane do przestrzeni wirtualnej. Z całą pewnością cyberprzestrzeń nie może być zawłaszczona przez żadne z państw. Z jednej strony jest to fizycznie i technicznie niemożliwe, z drugiej na pewno spowodowałoby sprzeciw wszystkich podmiotów międzynarodowych, które codziennie korzystają z przestrzeni wirtualnej.

Postulatu pokojowego wykorzystania przestrzeni kosmicznej w obecnych warunkach polityczno - prawnych, wydaje się, że nie można przełożyć na przestrzeń wirtualną. Przede wszystkim cyberprzestrzeń już obecnie jest wykorzystywana przez najróżniejszych aktorów międzynarodowych do realizacji swych celów. Nie ulega wątpliwości, iż w kolejnych latach konflikty międzynarodowe częściowo będą toczyły się również w cyberprzestrzeni. Cyber-wojna wydaje się być tylko kwestią czasu. Przestrzeń wirtualna jest wykorzystywana przez siły militarne państw na przykład do inwigilacji, śledzenia, pozyskiwania informacji czy manipulowania przeciwnikiem. Coraz większy zakres działań operacyjnych odbywa się sprzed ekranu komputer (drony, bezzałogowe samoloty), hakowanie baz danych i komputerów wroga jest już codziennością. W międzynarodowym prawie kosmicznym obowiązuje całkowity zakaz militaryzacji przestrzeni kosmicznej. Nasuwają się pytania czy przekładając to na grunt przestrzeni cyfrowej można uznać, że wirusy czy też inne programy komputerowe są bronią mającą na celu zniszczenie zasobów przeciwnika oraz czy wizja cyfrowego Pearl Harbor jest realna. Odpowiadając na to pytanie trzeba stwierdzić, że wizja ta jest bardzo prawdopodobna. Postęp technologiczny będzie napędzał rozwój nowych technik i narzędzi cyfrowych, które będą miały możliwość zniszczenia bądź znacznego uszkodzenia zasobów cyfrowych wroga.

5.3.2.3 Antarktyka

Kolejną przestrzenią międzynarodową jest Antarktyka, czyli obszar położony wokół Bieguna Południowego, obejmujący Antarktydę, wyspy, Ocean Lodowaty Południowy, Ocean Spokojny i Ocean Indyjski na południe od 60^{o} równoleżnika szerokości geograficznej

południowej. Siedem państw (Argentyna, Australia, Chile, Francja, Nowa Zelandia, Norwegia i Wielka Brytania) wysuwało roszczenia w stosunku do Antarktyki. Niepewna sytuacja prawna doprowadziła do zawarcia 1 grudnia 1959 roku w Waszyngtonie wielostronnego układu w sprawie Antarktydy[1302] (Układ antarktyczny). Stwierdzono w nim, że obszar antarktyczny winien być wykorzystany wyłącznie w celach pokojowych zakazując równocześnie wszelkich działań o charakterze wojskowym, w tym przez tworzenie baz i fortyfikacji wojskowych oraz doświadczeń ze wszelkimi rodzajami broni. Zabroniono dokonywania wybuchów jądrowych oraz usuwania w tym rejonie odpadów promieniotwórczych. Układ zakłada jednak wolność badań naukowych za całym obszarze Antarktytyki.

Co istotne, postanowienia układu antarktycznego zawieszają, lecz nie eliminują całkowicie, roszczeń terytorialnych co do Antarktyki przez cały czas trwania układu. Artykuł IV, ust. 2 wskazanej umowy międzynarodowej stanowi, że: żadne posunięcia lub działalność, mające miejsce w okresie trwania Układu antarktycznego, nie stwarzają podstawy do zgłoszenia, podtrzymania lub negowania pretensji do suwerenności terytorialnej na Antarktydzie i nie stwarzają żadnych praw do suwerenności na Antarktydzie. Ponadto, uznano, że nie można zgłaszać żadnej nowej pretensji lub rozszerzenia istniejącej pretensji do suwerenności terytorialnej na Antarktydzie tak długo, jak Układ pozostaje w mocy. Przepis ten nie potwierdził ani nie zaprzeczył roszczeniom państw, lecz jedynie zakazał wysuwania kolejnych roszczeń lub rozszerzania granic już istniejących.

Kwestia jurysdykcji została uregulowana w art. VIII układu antarktycznego, który wprowadza zasadę jurysdykcji personalnej, Jan Białocerkiewicz stwierdza, że: „szereg umów międzynarodowych, które regulują różne aspekty prawne Antarktyki, daje podstawy do postawienia tezy, że Antarktyka w przyszłości, podobnie jak dno morskie i oceaniczne poza granicami jurysdykcji państwowej, będzie stopniowo uzyskiwała status wspólnego dziedzictwa ludzkości”[1303]. Odmiennie zdania jest Tadeusz Srogosz, który stwierdza, że: „Antarktyka stanowi specyficzny reżim prawny. Nie jest ona ziemią niczyją (*res nullus*). Na pierwszy rzut oka wydawałoby się, że jest ona wspólnym dziedzictwem ludzkości. Jednak pamiętać należy o tym, że obszary o statusie wspólnego dziedzictwa ludzkości położone są poza terytoriami podlegającymi suwerenności państwowej (np. dno mórz i oceanów). W

[1302] Dz. U. z 1961 r., Nr 46, poz. 237.
[1303] J. Białocerkiewicz, op. cit., s. 211.

przypadku Antarktyki istotne jest natomiast, że państwa zgłaszające roszczenia terytorialne się ich nie wyrzekły. Problem roszczeń terytorialnych został jedynie »zamrożony«"[1304].

Początkowo układ antarktyczny miał obowiązywać 30 lat do 1991 roku, jednakże na mocy Protokołu o ochronie środowiska naturalnego do traktatu antarktycznego z 4 października 1991 r. (tak zwany Protokół madrycki) przedłużono jego obowiązywanie na kolejne 50 lat. Protokół poszerza zakres ochrony wymieniony ogólnikowo w układzie antarktycznym. Co więcej, zawarto w nim 5 załączników regulujących różne zagadnienia z ochrony środowiska (ocena skutków wobec środowiska, zapobieganie zanieczyszczeniom morskim, zachowanie antarktycznej flory i fauny, ochrona i zarządzanie obszarem oraz niszczenie odpadów i gospodarka odpadami)[1305]. Znawcy tematu podkreślają, iż celem przedłużenia stosowania umowy jest przekształcenie Antarktyki w najlepiej zachowany, dziewiczy ekosystem - ogólnoświatowy rezerwat naturalny[1306]. Przychylić należy się do poglądu Jana Białocerkiewicza, który stwierdza, że: „pełna realizacja idei zawartej w Protokole madryckim, by Antarktyka stała się rezerwatem nauki i pokoju jest jeszcze daleka. Intensywne badania naukowe nie są przecież sztuką dla sztuki. W tym stanie rzeczy, bez względu na to czy Antarktyka zostanie uznana za wspólne dziedzictwo ludzkości, czy też nie, społeczność międzynarodowa winna przyjąć konwencję o bezwzględnym zakazie dokonywania bezpośrednich i pośrednich zmian w środowisku arktycznym, gdyż zmiany w tym środowisku mogą wywołać ekologiczny efekt domina prowadzący nie tylko do stopniowej degradacji tej szczególnej części globu ziemskiego, ale wpływający na pozostałe części globu ziemskiego, podobnie jak wpływa wycinanie dżungli nad Amazonką"[1307]. W 2016 roku obchodzono dwudziestopięciolecie uchwalenia Protokołu madryckiego. Oznacza to, że minęła połowa okresu jego obowiązywania. Za dwie dekady społeczność międzynarodowa stanie w obliczu konieczności podjęcia decyzji, jakie będą dalsze losy Antarktyki. Nasuwa się więc pytanie czy ostatecznie zostanie ona uznana za wspólne dziedzictwo ludzkości, czy może - w obliczu potencjalnego kryzysu paliwowego (na Antarktyce znajdują się duże złoża ropy naftowej, węgla kamiennego, miedzi, żelaza, srebra i innych) roszczenia państw zostaną uznane.

[1304] T. Srogosz, *Obszary podbiegunowe*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne.* wyd. 2 Warszawa 2014, s. 288.
[1305] J. Białocerkiewicz, op. cit., s. 211 - 212.
[1306] W. Góralczyk, S. Sawicki, … 2013, s. 197.
[1307] J. Białocerkiewicz, op. cit., s. 212.

W ocenie Jacka Machowskiego pomiędzy prawem kosmicznym a prawem dotyczącym obszarów podbiegunowych zachodzi wiele podobieństw, wobec czego w niektórych przypadkach analogia może mieć zastosowanie. Podkreśla się podobieństwa tych dwóch obszarów. Warunki klimatyczne na Antarktyce są bliższe warunkom panującym w przestrzeni kosmicznej i na ciałach niebieskich, niż na innych kontynentach, oba środowiska są nieprzyjazne dla człowieka, podróż wiąże się z dużym niebezpieczeństwem, koniecznością zachowania wymogów bezpieczeństwa i ewentualnym przymusem podjęcia odpowiednich działań w celu ratowania życia i zdrowia. Podkreśla się podobny status stacji polarnych oraz kosmicznych, wolność badań naukowych, odpowiedzialność za szkody[1308].

Układ waszyngtoński z 1959 r. stanowi podstawę, wokół której wypracowano tak zwany System Układu Antarktycznego (ang. *Antarctic Treaty System* - ATS). W skład ATS, oprócz Układu waszyngtońskiego wchodzą zalecenia spotkań konsultacyjnych oraz liczne umowy międzynarodowe. W ramach ATS funkcjonuje również szereg powiązanych międzyrządowych oraz pozarządowych organów i organizacji[1309].

5.4 Prawo międzynarodowe jako *law in action*

Jedną z cech współczesnego prawa międzynawowego są tendencje odśrodkowe. Charakteryzują się one powstawaniem nowych działów wyspecjalizowanych i interdyscyplinarnych. Przyczyną takiego stanu jest konieczność dostosowania prawa do szybko zmieniających się stosunków między państwami oraz postępującej rewolucji naukowo - technologicznej[1310]. Zauważalne zmiany nastąpiły już po II wojnie światowej. Pojawiły się zupełnie nowe działy prawa międzynarodowego, obejmujące między innymi prawo kosmiczne, prawo atomowe, prawo ochrony środowiska czy też prawo organizacji międzynarodowych. Od początku lat dziewięćdziesiątych XX wieku nastąpił dynamiczny rozwój technologii komputerowych, prowadzący do wyodrębnienia się prawa regulującego działania człowieka w cyberprzestrzeni. W podrozdziale zostanie ukazana rola prawa

[1308] J. Machowski, *Stan i perspektywy rozwoju międzynarodowego prawa polarnego (próba systematyzacji)*, [w:] K. Lankosz (red.), *Aktualne problemy prawa międzynarodowego we współczesnym świecie. Księga pamiątkowa poświęcona pamięci Profesora Mariana Iwanejko*, Kraków 1995, s. 265.
[1309] Ibidem, s. 267.
[1310] Ibidem, s. 263.

międzynarodowego w kształtowaniu obszarów związanych z ekspansją działalności człowieka na nowe terytoria i płaszczyzny.

5.4.1 Ochrona klimatu

Rozwój techniki oraz rewolucyjne uprzemysłowienie gospodarki w XX i XXI wieku spowodowały intensywnie postępujące zanieczyszczenie środowiska i zmianę klimatu. Problemy takie, jak zanikanie warstwy ozonowej, zanieczyszczenie powietrza, mórz i oceanów, globalne ocieplenie i ryzyko skażeń materiałami chemicznymi lub radioaktywnymi na masową skalę stały się realnym zagrożeniem dla ludzkości. Dbałość o środowisko ma międzynarodowy wymiar z kilku przyczyn. Przede wszystkim nie ulega wątpliwości, iż masowa produkcja przemysłowa w jednym miejscu na Ziemi może spowodować ulatnianie się składników chemicznych, które na skutek wiatrów i innych warunków atmosferycznych mogą zmaterializować się w zupełnie innym miejscu na świecie w postaci na przykład kwaśnych deszczy. Ocieplenie klimatu wpływa na wszystkie państwa globu, a topnienie lodowców zagraża najniżej położonym państwom. Ponadto, kwestia ochrony środowiska i ochrony przez jego zanieczyszczeniem zdecydowanie przekracza możliwości i kompetencje jednego państwa. Konieczne jest podjęcie międzynarodowych działań wielu państw, aby mówić chociażby o minimalnych standardach ochrony środowiska naturalnego[1311].

Problem ochrony środowiska ziemi zaczął być szerzej rozważany dopiero w drugiej połowie XX wieku. Jednym z pierwszych dokumentów międzynarodowych była rezolucja Zgromadzenia Ogólnego ONZ uchwalona 3 grudnia 1968 roku nr 2398/XXIII o nazwie Problemy środowiska człowieka, zwracająca uwagę na kwestię nadmiernego wykorzystania środowiska. Uznano wówczas, że „po raz pierwszy w historii ludzkości pojawił się kryzys o zasięgu ogólnoświatowym, obejmujący zarówno kraje rozwinięte, jak i rozwijające się - kryzys dotyczący stosunku człowieka do środowiska”[1312].

Istotnym punktem tworzenia się międzynarodowego prawa ochrony środowiska była sztokholmska konferencja ONZ z 1972 roku, na której opracowano Deklarację Konferencji

[1311] M.N. Shaw, *Prawo.*. 2006, s. 486.
[1312] J. Machowski, *Problemy prawne ochrony środowiska*, Warszawa 2000, s. 13-14.

Narodów Zjednoczonych w sprawie Środowiska Człowieka. Mimo że ani preambuła ani zawarte 26 zasad nie miało mocy wiążącej to stworzyło podwaliny dla rozwoju prawa ochrony środowiska służąc poniekąd za uniwersalny zbiór standardów. Obecnie na międzynarodowe prawo ochrony środowiska składają się konwencje międzynarodowe o zasięgu globalnym jak i regionalnym, jednakże ważną, pomocniczą rolę *de lege ferenda* pełnią akty o charakterze niewiążącym - decyzje, uchwały, rezolucje i zalecenia ONZ oraz dokumenty przyjęte na konferencjach ONZ w Sztokholmie i Rio de Janeiro[1313]. Ważnym punktem było wydanie Konwencji ramowej Narodów Zjednoczonych w sprawie zmian klimatu, określającej założenia międzynarodowej współpracy w zakresie ochrony klimatu (została podpisana w czasie szczytu w Rio de Janeiro w 1992 roku)[1314]. Początkowo konwencja nie zawierała wiążących postanowień nakazujących ograniczenie emisji gazów cieplarnianych, z czasem jednak były przyjmowane kolejne protokoły ograniczające emisję (w tym najważniejszy - protokół z Kioto).

Warto również wspomnieć o raporcie Światowej Komisji do spraw Rozwoju ONZ, wydanym pod przewodnictwem norweskiej minister spraw zagranicznych w 1987 roku. Raport o nazwie Nasza wspólna przyszłość był początkowo bardzo krytykowany wobec użycia niejasnych i nieostrych pojęć takich, jak chociażby zrównoważony rozwój. Dokument akcentował potrzebę wielopłaszczyznowego spojrzenia na temat ochrony środowiska jako obszaru kompleksowych zależności. Uznano, że globalna etyka rozwoju powinna być oparta na zasadzie „podwójnej sprawiedliwości" rozumianej jako konieczność zapewnienia odpowiednich, sprawiedliwie społecznych polityk rozwojowych w sposób uczciwy dla obecnych i przyszłych pokoleń[1315].

Współcześnie w piśmiennictwie występują poglądy, że istnieje międzynarodowe prawo człowieka do czystego środowiska naturalnego. Koncepcja ta ma opierać się między innymi na uznanych powszechnie prawie do życia, zdrowia oraz prawie do odpowiedniego poziomu życia[1316]. Twierdzenia te znajdują swoje odzwierciedlenie w międzynarodowych dokumentach i aktach prawnych. We wstępie do Deklaracji sztokholmskiej znajduje się zapis, który stanowi, że środowisko naturalne ma „podstawowe znaczenie dla (...) urzeczywistnienia

[1313] Ibidem, s. 39-43.
[1314] Więcej na temat konwencji w: J. von Stein, *The International Law and Politics of Climate Change: Ratification of the United Nations Framework Convention and the Kyoto Protocol*, "The Journal of Conflict Resolution" 2008, t. 52, nr 2.
[1315] E. Gończ, *Jak chronić środowisko naturalne?,* [w:] Z. Brodecki (red.), *Ochrona środowiska*, Warszawa 2015, s. 22-23.
[1316] M.N. Shaw, *Prawo...* 2006, s. 486-487.

podstawowych praw człowieka - nawet samego prawa do życia". Z kolei opisana w deklaracji zasada nr 1 mówi o tym, że „człowiek posiada fundamentalne prawo do wolności, równości i odpowiednich warunków życia w środowisku, którego jakość pozwala na życie w godności i dobrobycie". Podobnie Protokół dodatkowy do Amerykańskiej konwencji praw człowieka z 1988 r. w art. 11 wprowadza postanowienie, że „każdy ma prawo do życia w zdrowym środowisku" i że „państwa - strony powinny promować ochronę, zachowanie oraz ulepszanie środowiska"[1317].

Według znawców tematu normy prawa (w tym prawa międzynarodowego) powinny być instrumentem spełniającym trzy podstawowe funkcje ochrony środowiska:

1) funkcję organizatorską - polegającą na kształtowaniu zasad korzystania ze środowiska w kontekście jego ochrony poprzez ustalanie norm i kryteriów ochrony, zasad, form i rodzajów oraz ograniczeń w korzystaniu ze środowiska,
2) funkcję organizacyjną - polegającą na ustaleniu i rozdzieleniu zadań pomiędzy państwa i organizacje społeczne,
3) funkcję represyjną - przez wprowadzenie sankcji za wyrządzone szkody środowiskowe, ustalenie zasad restaurowania zniszczonych elementów środowiska i tym podobne[1318].

Malcolm N. Shaw podnosi, że „uznaje się obecnie, że międzynarodowy charakter zanieczyszczenia, zarówno jeżeli chodzi o miejsce jego powstania, jak i wyrządzonej szkody, wymaga reakcji międzynarodowej. Najpoważniejszym problem konceptualnym dla prawa międzynarodowego jest charakter tej dyscypliny, w której centrum zainteresowania jest państwo. Tradycyjnie w sensie międzynarodowoprawnym wyłącznie państwo odpowiadało za spowodowanie szkody, jeśli tylko można było udowodnić, że szkoda ta powstała w wyniku jego bezprawnych działań. Z wielu powodów okazało się to niewystarczającą podstawą do rozstrzygania problemów z zakresu ochrony środowiska. Związane to było z trudnością udowodnienia odpowiedzialności za bezprawne działania oraz ze szczególnym problemem odpowiedzialności podmiotów niebędących państwami. W związku z tym społeczność międzynarodowa powoli odchodziła od klasycznej koncepcji odpowiedzialności państw za wyrządzone szkody do współpracy międzynarodowej"[1319]. Przemyślenia Malcolma N. Shawa

[1317] Ibidem, s. 532-533.
[1318] M. Górski, *Zagadnienia wprowadzające*, [w:] idem (red.) *Prawo ochrony środowiska*, Warszawa 2009, s. 40.
[1319] M.N. Shaw, *Prawo*... 2006, s. 486-487.

można odnieść do kwestii ponoszenia odpowiedzialności w przestrzeni cyfrowej. Niezwykle trudno jest udowodnić działania państw, czy też innych podmiotów w cyberprzestrzeni polegające chociażby na bezprawnych zachowaniach czy stosowaniu cyberataków. Jedynie podjęcie współpracy międzynarodowej w celu ustalenia zasad odpowiedzialności za cyberataki, byłoby w stanie wyeliminować bądź chociażby zminimalizować część czynów bezprawnych w cyberprzestrzeni.

Prawo ochrony środowiska ukazuje, że utworzenie jednego, w miarę spójnego systemu regulującego dany problem jest czasochłonne. Tam gdzie nie ma regulacji, bądź są one cząstkowe, trafnym rozwiązaniem było wydawanie niewiążących dokumentów, które wskazywały następnie pożądaną sposób postępowania i były podstawą do przyjęcia aktów prawnie wiążących. Ochrona środowiska jest niewątpliwie jednym z najbardziej istotnych zagadnień w kontekście naszego życia oraz życia przyszłych pokoleń. Mimo, iż prawo międzynarodowe z zasady nie przewiduje sankcji za naruszenia norm to w przypadku regulacji dotyczących ochrony klimatu państwa same starają się dotrzymać postanowień umów międzynarodowych, którymi się związały. Tak było chociażby w odniesieniu do protokołu dodatkowego podpisanego na czwartej konferencji w Kioto, w którym państwa rozwinięte zobowiązały się do dobrowolnej redukcji dwutlenku węgla. W okresie tym do państw UE należało 15 krajów, które zadeklarowały obniżenie CO_2 o 8%. Już w 2005 roku Hiszpania zmniejszyła emisję o 55%, a Portugalia o 40%. Niestety, część krajów kierowała się wyłącznie własnym interesem gospodarczym i tak, jak USA zwiększyła emisję (o 25%)[1320]. Pokazuje to, że w ważnych kwestiach, osiągnięcie międzynarodowego konsensu w formie prawa pozytywnego bywa czasochłonne. Z tych względów państwa decydują się wydawać dokumenty o charakterze *soft law* - nie tylko by wskazać problem, ale by go rozwiązać. Przyjmując akty niewiążące państwa uznają ich postanowienia za słuszne i decydują się ich przestrzegać. W obszarach, w których istnieje pilna potrzeba regulacji prawo tworzy się „na bieżąco", mamy zatem do czynienia z *law in action* - prawem w działaniu.

Nie ma postępu bez zmian technologicznych i rozwoju gospodarki. Nie może on jednak mieć wartości nadrzędnej nad środowiskiem naturalnym. Konieczne jest zachowanie odpowiedniej równowagi między tymi dwoma wartościami. Środowisko naturalne jest połączone w jeden ekosystem, dlatego też ochrona klimatu musi nastąpić na poziomie

[1320] M. Nowicki, *Zobowiązania Polski dotyczące ochrony klimatu wynikające z międzynarodowych i unijnych negocjacji,* [w:] M. Lipińska (opr.) *Ochrona klimatu szansą dla gospodarki i społeczeństwa. Materiały z konferencji zorganizowanej przez Komisję Środowiska we współpracy z Instytutem na rzecz Ekorozwoju*, Warszawa 2010, s. 12.

międzynarodowym. Tylko międzynarodowe normy mogą sprostać rozbieżnym interesom państw w przyjęciu wspólnego konsensusu i podjęciu międzynarodowej współpracy[1321]. Jedynie ścisła międzynarodowa współpraca może zapewnić czyste środowisko dla przyszłych pokoleń. Obszarami sektorowymi ochrony środowiska jest ochrona powietrza, gospodarka odpadami czy też usuwanie skutków poważnych awarii i zanieczyszczeń chemicznych. W krótkim okresie istnienia międzynarodowe prawo ochrony środowiska wypracowało kilka uniwersalnych zasad i instrumentów mogących odegrać istotną rolę w przyszłości. Przede wszystkim jest to koncepcja ekorozwoju, czyli trwałego i zrównoważonego rozwoju oraz ocena oddziaływania na środowisko. Istotne znaczenie może mieć również zapoczątkowana przez UNESCO i Program Środowiskowy Organizacji Narodów Zjednoczonych idea prawnej ochrony światowego dziedzictwa naturalnego i kulturalnego[1322].

Zagrożenia środowiska naturalnego wzrastają lawinowo. Niestety mimo rosnącej liczby ekologicznych porozumień międzynarodowych ich efektywność nie jest wprost proporcjonalna do degradacji. Zasadniczym problemem są sprzeczne interesy bogatych państw wysoko rozwiniętych i biednych państw rozwijających się, w których dbałość o środowisko schodzi na drugi plan. Dlatego tak ważne jest organizowanie międzynarodowych spotkań, na przykład w formie konferencji ekologicznych, na których przedstawiciele państw mogą wymieniać poglądy i debatować nad najważniejszymi problemami ochrony środowiska. Jacek Machowski stawia słuszną tezę, że „różnorodne zanieczyszczenia środowiska naturalnego potwierdzają globalny charakter zagrożeń z ich strony. A zatem, radykalna ochrona przed nimi będzie skuteczna jedynie w wymiarze światowym i przy udziale takich instrumentów prawnych, jak umowy i organizacje międzynarodowe o charakterze uniwersalnym i zasięgu: globalnym, regionalnym i lokalnym”[1323]. Globalne zagrożenia i problemy mogą być skutecznie regulowane i niwelowane wyłącznie za pomocą skoordynowanej współpracy na wielu poziomach. Główną rolę w koordynacji i wskazywania kierunków działań należy jednak przyznać prawu międzynarodowemu.

[1321] M.N. Shaw, *Prawo...* 2011, s. 534.
[1322] J. Machowski, *Problemy …*, s. 233.
[1323] Ibidem, s. 231.

5.4.2 Kosmos

Pierwsze loty w kosmos wprowadziły potrzebę regulacji nowego, nieistniejącego do tej pory zagadnienia dopuszczalności przelotu sztucznych satelitów. Brak sprzeciwu państw, nad którymi obiekty te przelatywały, doprowadził do wykształcenia się normy zwyczajowej zezwalającej na takie działania. Brak norm prawnych w tym przedmiocie spowodował, że stopniowo ukształtowało się prawo nieszkodliwego przelotu statków kosmicznych, które swą formą przypominało prawo nieszkodliwego przepływu statków morskich przez wody terytorialne. Zaakcentować jednak należy, że uznanie prawa nieszkodliwego przelotu statków kosmicznych nie pozbawiło państw obrony swych praw związanych z zapewnieniem bezpieczeństwa swego terytorium czy też uprawnieniem do samoobrony[1324].

Prawo kosmiczne rozwija się od lat sześćdziesiątych XX wieku, ale do dzisiaj nie zostało kompleksowo skodyfikowane i odpowiednio doprecyzowane. Można zaobserwować odchodzenie podmiotów międzynarodowych od wiążących norm traktatowych na rzecz niewiążących aktów przyjmowanych w formie rezolucji. Wyzwaniem dla współczesnego prawa kosmicznego są dwa zasadnicze obszary. Pierwszy jest związany z interpretacją bądź realizacją już przyjętych traktatów międzynarodowych - ustaleniem delimitacji przestrzeni powietrznej i przestrzeni kosmicznej, doprecyzowaniem używanych pojęć takich, jak obiekt kosmiczny, badanie czy też użytkowanie kosmosu. Drugim problem są nieuregulowane w prawie kosmicznym zagadnienia praktyczne[1325]. Podobne stanowisko wyraża Leonard Łukaszuk, który stwierdza, że „współczesne prawo kosmiczne wymaga nowych badań, uwzględniających wiele nowych uwarunkowań: cywilizacyjnych, technicznych, gospodarczych, kulturowych i prawnych a także politycznych”[1326]. Działania w przestrzeni kosmicznej nie są podejmowane wyłącznie przez państwa. Coraz więcej badań i aktywności jest przeprowadzanych przez pozapaństwowe podmioty takie, jak organizacje międzynarodowe oraz podmioty prywatne, które wykorzystują kosmos do celów komercyjnych. Z tych też względów zasadne jest rozpoczęcie dyskusji o wprowadzeniu odpowiednich, nowych norm prawnych. Obecnie, jako podstawowe, problemy wskazuje się -

[1324] M. Polkowska, *Prawo kosmiczne w obliczu nowych problemów współczesności*, Warszawa 2011, s. 32-33.
[1325] K. Myszona-Kostrzew, *Kierunki rozwoju międzynarodowego prawa kosmicznego*, [w:] K. Karski (red.), *Kierunki rozwoju współczesnego prawa międzynarodowego*, Warszawa 2015, s. 135.
[1326] L. Łukaszuk, *Prawo kosmiczne - z europejskiej perspektywy. Kierunki rozwoju i dziedziny zastosowania*, [w:] Z. Galicki, T. Kamiński, K. Myszona - Kostrzewa (red.), *Wykorzystanie przestrzeni kosmicznej. Świat - Europa - Polska*, Warszawa 2010, s. 131.

zagadnienia związane z teledekacją, militaryzacją kosmosu, ochroną środowiska kosmicznego przed różnego rodzaju zanieczyszczeniami oraz ochroną własności intelektualnej we współczesnej działalności kosmicznej[1327].

Eksploatacja przestrzeni kosmicznej wiąże się z wykorzystaniem coraz nowocześniejszych technologii i technik, w tym związanych z umieszczaniem i użytkowaniem satelitów kosmicznych oraz stacji kosmicznych. Obecne uregulowania międzynarodowe nie poruszają kwestii jurysdykcji i odpowiedzialności podmiotów prywatnych. Jest to zagadnienie problematyczne między innymi ze względu na coraz większą współpracę agencji kosmicznych z sektorem prywatnym oraz zagadnieniami transferu technologii, ochrony patentowej oraz *know-how*[1328]. Na szczególną uwagę zasługuje podpisane w 1988 roku w Waszyngtonie międzyrządowe porozumienie o międzynarodowej stacji komicznej (ang. *International Space Station* - ISS), które stwierdza, że ISS może być używana wyłącznie do celów pokojowych, a każdy z partnerów wykonuje jurysdykcję nad personelem ISS oraz kontrolę nad zarejestrowanymi modułami. W umowie poruszone zostały również aspekty związane z prawami własności intelektualnej czy odpowiedzialności karnej[1329].

Wobec braku bezpośrednich, całościowych regulacji odnoszących się do praw własności intelektualnej w kosmosie znawcy tematu uznali, że ochrona w przestrzeni kosmicznej, w tym na międzynarodowej stacji kosmicznej, odbywa się zgodnie z zasadami prawa międzynarodowego, nawet gdy normy traktatowe nie odnoszą się bezpośrednio do takiej sytuacji, to podstawowe zasady będą wiążące[1330]. Własność intelektualna w działalności kosmicznej ma znaczenie w zakresie ochrony wiedzy, stanowiącej „kapitał intelektualny" organizacji krajowej bądź międzynarodowej (wiedza rozumiana jako przedmiot zarządzania i ochrony), a poszczególne rodzaje wiedzy podlegające ochronie (patenty, wzory użytkowe i przemysłowe, programy komputerowe i inne) są ograniczone w zakresie podmiotowym, czasowym i geograficznym[1331]. Prace dotyczące własności intelektualnej w kosmosie zostały podjęte między innymi przez Europejską Agencję Kosmiczną, której Rada w 1989 roku przyjęła dokument Ogólne reguły dotyczące informacji

[1327] L. Łukaszuk, *Działalność związana z kosmosem a międzynarodowa ochrona własności intelektualnej - wybrane zaganiania,* [w:] J. Menkes (red.), *Prawo Międzynarodowe. Księga pamiątkowa prof. Renaty Szafarz*, Warszawa 2007, s. 399-400.
[1328] Ibidem, s. 400.
[1329] M. Polkowska, op. cit., s. 189-193.
[1330] L. Łukaszuk, *Działalność…*, s. 406.
[1331] Ibidem, s. 402.

danych i własności intelektualnej[1332]. Regulacje te kilkukrotnie modyfikowano, wprowadzając nowe rozwiązania odpowiadające rozwojowi techniki. Zaznaczyć jednak trzeba, że normy te stanowią jedynie wyrywek w obliczu ogromu problemu międzynarodowej własności intelektualnej w kosmosie. Brak wiążącej umowy międzynarodowej powoduje, że zarówno na gruncie międzynarodowym, jak i europejskim trwają prace nad wprowadzeniem odpowiednich zmian legislacyjnych.

Ciekawym zagadnieniem jest również eksploatacja surowców w przestrzeni kosmicznej. Znawcy tematu wskazują, że w związku z uznaniem kosmosu za wspólne dziedzictwo ludzkości jakakolwiek komercjalizacja w formie zawłaszczenia kosmosu i ciał niebieskich bądź ich części nie jest możliwa w świetle prawa międzynarodowego. Niezawłaszczalność kosmosu jest nie tylko normą traktatową, lecz przede wszystkim normą zwyczajową *ius cogens*. Postanowienia Układu normującego działalność państw na Księżycu i innych ciałach niebieskich z dnia 18 grudnia 1979 r.[1333] stanowią, że zasoby kosmiczne „nie mogą stać się własnością któregokolwiek państwa, międzynarodowej organizacji albo jednostki pozarządowej czy jakiejkolwiek osoby fizycznej". Kolejne postanowienia nakładają na państwa obowiązek stworzenia reżimu regulującego sposób postępowania dotyczącego eksploatacji. Katarzyna Myszona-Kostrzewa wskazuje, że „wzorem mogą być regulacje zawarte w Konwencji o prawie morza z 1982 roku dotyczące wydobywana złóż naturalnych obszaru, czyli dna i podziemia dna morza otwartego. Niewielka liczba państw - stron porozumienia o Księżycu (wśród których nie ma żadnego państwa prowadzącego rzeczywistą działalność kosmiczną) składnia do wniosku, że koncepcja »wspólnego dziedzictwa ludzkości« i idea stworzenia międzynarodowego reżimu eksploatacji złóż spotkały się w praktyce z nieprzychylnym przyjęciem. Wydaje się, że podmioty zdolne do eksploatacji zasobów naturalnych księżyca i innych ciał niebieskich nie zamierzają realizować jej w ramach specjalnie stworzonego reżimu międzynarodowego i tym samym poddawać ją pod kontrolę międzynarodową"[1334].

W ostatnich latach coraz śmielej mówi się o turystyce kosmicznej. Lot w kosmos nie jest już zarezerwowany wyłącznie dla astronautów. Warunkiem, który trzeba spełnić, by polecieć w kosmos jest w chwili obecnej zasobność portfela. W 2001 roku Amerykanin Denis

[1332] Rules concerning information, data and intellectual property - ESA/C/89/95 rev. 1.
[1333] Akt dostępny w języku angielskim na oficjalnej stronie internetowej Organizacji Narodów Zjednoczonych: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXIV-2&chapter=24&clang=_en, [20.03.2016].
[1334] K. Myszona-Kostrzewa, op. cit., s. 144.

Anthony Tito spędził na Międzynarodowej Stacji Kosmicznej sześć dni, rok później multimilioner z RPA, w zamian za kilkadziesiąt milionów dolarów, przebywał w kosmosie osiem dni. Od 2007 roku rosyjski program podboju kosmosu oferuje transport na ISS w zamian za gratyfikację finansową. Rozwijający się biznes podróży kosmicznych wiąże się z problemem odpowiedzialności operatorów i właścicieli działających w przestrzeni kosmicznej oraz odpowiedniego ubezpieczenia. Wobec tego powstaje również ważne pytanie o jurysdykcję karną w przypadku popełnienia czynu zabronionego w kosmosie. Na chwilę obecną, żaden akt międzynarodowy nie reguluje kwestii tego typu odpowiedzialności. Status prawny kosmicznego turysty również pozostaje zagadką, gdyż nie będziemy mogli zastosować wobec niego układu z 1968 roku o ratowaniu kosmonautów, ponieważ nie można mu przyznać tego statusu[1335].

Wciąż brak jest wielostronnej umowy międzynarodowej normującej zagadnienia techniki satelitarnej i jej zastosowania. System satelitarny umożliwia łatwiejszy i sprawniejszy dostęp do informacji - między innymi przez łączność telefonii komórkowej i sieci elektroenergetycznej. Dzięki satelitom i urządzeniom GPS zrewolucjonizował się transport drogowy, morski i powietrzny. Jedną z najbardziej problematycznych kwestii jest brak powszechnej konwencji regulującej odpowiedzialność międzynarodową za szkody związane ze stosowaniem technik satelitarnych[1336]. Zdzisław Galicki podkreśla, że „w przeciwieństwie do odpowiedzialności za naruszenie prawa, która wynika z powszechnie obowiązujących zasad prawa międzynarodowego, odpowiedzialność z tytułu ryzyka nie ma takiego charakteru i jako odnosząca się do działań przez prawo międzynarodowe dozwolonych może wynikać wyłącznie z wyraźnych zobowiązań traktatowych pomiędzy państwami, a także dotyczyć tylko tych państw, które są stronami takich umów międzynarodowych”[1337]. Ustalenie zasad odpowiedzialności, w tym zakresu odpowiedzialności poszczególnych podmiotów, ma szczególne znaczenie w kontekście systemów komunikacji opartych na partnerstwie publiczno-prywatnym. Postuluje się, by odpowiedzialność została oparta na zasadzie ryzyka oraz na podstawie odpowiedzialności ograniczonej (wprowadzając limit odszkodowań). Przyjęcie takiego rozwiązania związane by

[1335] M. Polkowska, op. cit., s. 148-155.
[1336] K. Myszona - Kostrzewa, op. cit., s. 142.
[1337] Z. Galicki, *Rozwój zasad odpowiedzialności międzynarodowej za działania kosmiczne*, [w:] A. Wasilkowski (red.), *Działalność kosmiczna w świetle prawa międzynarodowego*, Warszawa 1991, s. 56.

było z koniecznością wprowadzenia obowiązkowego ubezpieczenia dostawców usług satelitarnych[1338].

Znawcy tematu, w tym Leonard Łukaszuk, podkreślają szczególną rolę organizacji międzynarodowych współkształtujących współpracę międzynarodową: „tworzące się regionalne, europejskie, wspólnotowe i unijne prawo kosmiczne pozostaje w trwałych relacjach z powszechnym międzynarodowym prawem kosmicznym oraz wchodzi częściowo - w pewnym zakresie w godne bliższych badań relacje i interakcje z tradycyjnie ukształtowanym wspólnotowym prawem materialnym gospodarczym (transportowym, konkurencji) i niekiedy zderza się (m.in. na płaszczyźnie relacji rynkowych) z jego zasadami, które kolidują z założeniami ukierunkowanej globalnie, bądź sektorowo polityki kosmicznej, zarówno w warunkach UE jak i w szerszej perspektywie międzynarodowej"[1339].

Rozwój techniki powoduje ciągłą ewolucję prawa kosmicznego, również w zakresie relacji z sektorem prywatnym, prywatyzacją i komercjalizacją usług, a nawet w zakresie międzynarodowego sektora ubezpieczeń w przypadku podróży kosmicznych. Piśmiennictwo w tym obszarze nie jest zbyt obszerne[1340], a regulacje prawne na poziomie europejskim dopiero się kształtują. Formujące się europejskie źródła prawa kosmicznego obejmują trzy zbiory dokumentów: akty przyjęte w ramach systemu ONZ, tak zwane regulacje instytucjonalne Wspólnot Europejskich i Unii Europejskiej, porozumienia państw członkowskich z organizacjami międzynarodowymi zajmującymi się działalnością kosmiczną oraz dokumenty regulujące udział państw członkowskich w różnych projektach międzynarodowych dotyczących kosmosu, w tym obejmujących programy Ariane oraz Międzynarodową Stację Kosmiczną[1341]. Przyjęte dokumenty mają głównie na celu utworzenie odpowiedniego ustawodawstwa sprzyjającego budowaniu innowacyjności, konkurencyjności oraz koordynacji działań w polityce kosmicznej UE. Nieoceniona jest również współpraca Unii Europejskiej z Europejską Agencją Kosmiczną[1342].

Wydaje się, że prawo kosmiczne stanęło w obliczu zupełnie nowych wyzwań. Wskazane jest zatem poszukiwanie nowych rozwiązań prawnych oraz reinterpretacja obowiązujących standardów. Widoczna jest ewolucja prawa kosmicznego, w kierunku

[1338] K. Myszona - Kostrzewa, op. cit., s. 143.
[1339] L. Łukaszuk, *Prawo…*, s. 132.
[1340] Na uwagę zasługuje jednakże pozycja: J.J. van de Wouwer, F. Lambert, *European Trajectories in Space Law 2007*, Luksemburg 2008.
[1341] L. Łukaszuk, *Prawo…*, s. 136.
[1342] Więcej: Ibidem.

uregulowania zagadnień gospodarczych, związanych z partnerstwem z sektorem prywatnym, prawami własności intelektualnej, czy odpowiedzialnością za zanieczyszczenia kosmosu i ochroną jego środowiska. Kwestią, która może nastręczyć dużych problemów w przyszłości jest transport kosmiczny, czy też eksploatacja przestrzeni kosmicznej przez podmioty prywatne czy organizacje międzynarodowe oraz związana z tym odpowiedzialność i ewentualne ubezpieczenie.

Prawo kosmiczne często porównywane jest do prawa morza oraz do prawa lotniczego. Warto jednak zwrócić uwagę, że prawodawstwo kosmiczne nie jest tak bardzo rozwinięte, jak dwie wymienione wyżej dziedziny. O fakcie tym świadczy chociażby liczba konwencji oraz *soft law* o randze międzynarodowej, europejskiej i krajowej. Rozwój technologii przyśpiesza z dekady na dekadę, a nowi aktorzy (podmioty prywatne) coraz śmielej rozwijają swoją działalność w przestrzeni kosmicznej. Prawo kosmiczne stoi w obliczu nowych wyzwań. W związku z tym konieczne jest uaktualnienie i rewizja ustawodawstwa[1343].

Małgorzata Polkowska stawia tezę, iż w obliczu współczesnych wyzwań znaczna część nowych źródeł prawa kosmicznego będzie pochodzić z sektora prywatnego, co zmieni charakter międzynarodowego prawa kosmicznego z publicznego na mieszany. W trakcie powstawania prawa kosmicznego głównymi aktorami były państwa. Obecnie, w związku z coraz większą komercjalizacją przestrzeni kosmicznej, znaczna część działań podejmowana jest przez podmioty prywatne. Autorka słusznie zauważa, że: „tak jak kiedyś chodziło głównie o prymat polityczny dwóch mocarstw (okres zimnej wojny), tak w chwili obecnej wydaje się, iż przeważają interesy ekonomiczne państw w dostępie do technologii kosmicznych i rozwoju telekomunikacji, nawigacji satelitarnej i teledetekcji (...). Z drugiej strony, przyczyną małej aktywności organizacji kosmicznych (na przykład COPUOS, ITU) jest niechęć państw do uczestnictwa w światowym systemie konwencyjnym (umów wielostronnych) między innymi z obawy o własną suwerenność”[1344]. Konsekwencją tych rozważań jest zatem stwierdzenie, że wobec jednolitych regulacji międzynarodowych jedynym rozwiązaniem jest legislacja krajowa, która dostosuje prawo do bieżących potrzeb[1345].

Nowe regulacje winny uwzględniać zróżnicowany zakres podmiotowy i przedmiotowy działań podejmowanych w przestrzeni kosmicznej. Państwa, organizacje

[1343] M. Polkowska, op. cit., s. 122.
[1344] Ibidem, s. 259 -261.
[1345] Ibidem, s. 261.

międzynarodowe i podmioty prywatne winny podjąć współpracę w unormowaniu najistotniejszych zagadnień dla całej ludzkości takich, jak łączność, nawigacja satelitarna, własność intelektualna oraz zasady współpracy z sektorem prywatnym.

5.4.3 Inne

Postęp technologiczny szczególne korzyści przyniósł medycynie. Inwestowanie w technologie i badania na przestrzeni ostatnich lat przyniosło wymierne wyniki w postaci przełomowych odkryć i stworzenia nowych urządzeń, które znacznie poprawiły jakość życia ludzkiego i dały nowe możliwość leczenia chorób. Ostatnie dziesięciolecia to postępująca rewolucja medyczna - odkrycie DNA, przeszczepy organów, wykorzystanie narzędzi takich, jak drukarki 3D do produkcji protez czy implantów. Pomimo wymiernych korzyści nasuwają się także pytania o prawną i etyczną dopuszczalność stosowania nowych metod leczenia.

Jedynie pokrótce wymienić należy najbardziej problematyczne - z punktu widzenia prawa międzynarodowego - zagadnienia medyczne. Klonowanie pierwszy raz stało się faktem w 1996 roku wraz ze sklonowaniem słynnej owcy Dolly. W 2001 roku Zgromadzenie Ogólne ONZ przyjęło rezolucję nr 56/93 zakazującą klonowania istot ludzkich. Obecnie pojawiają się też pytania o możliwość dokonywania klonowania w celach naukowych, partenogenezy czy też wytwarzania chimer. Jeszcze innym problemem jest prokreacja wspomagana, czyli metoda *in vitro*, a w szczególności jej status prawny, sposób przechowywania, decyzja o wykorzystaniu embrionów w przyszłości bądź zniszczeniu, ale również możliwości ich wykorzystania w przypadku orzeczenia rozwodu[1346]. Kolejnym wyzwaniem jest również genetyka oraz możliwość wprowadzania zmian w genomie ludzkim, roślinnym czy zwierzęcym. Zwiększa się produkcja i uprawa organizmów modyfikowanych genetycznie (ang. *Genetically Modified Organisms*). Zupełnie rewolucyjnym pomysłem wydaje się być patentowanie genów ludzkich, jednakże możliwość uzyskania patentu na sekwencję genów jest dopuszczalna zarówno przez polski, jak i europejski system patentowy[1347].

[1346] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 7 marca 2006 r. w sprawie *Evans przeciwko Wielkiej Brytanii*, skarga nr 6339/05.
[1347] Więcej: J. Stanek, *Patentowanie genów ludzkich*, Warszawa 2016.

Aktem prawa międzynarodowego o szczególnym znaczeniu jest Konwencja Rady Europy o ochronie praw człowieka i godności istoty ludzkiej w odniesieniu do zastosowań biologii i medycyny (konwencja bioetyczna)[1348]. Stronami konwencji jest 26 państw, w tym Polska, która nie ratyfikowała jeszcze omawianego aktu prawnego. Konwencja zawiera istotne postanowienia dotyczące między innymi zakazu klonowania, badań z wykorzystaniem embrionów oraz przepisy dotyczące praw pacjenta[1349]. Do problematyki GMO odnosi się protokół o bezpieczeństwie biologicznym do Konwencji o różnorodności biologicznej oraz porozumienia zawierane w ramach WTO[1350]. Wiele pytań pozostaje jednak otwartych. Trwają dyskusje o istocie i charakterze prawnym danych genetycznych[1351], genomu ludzkiego[1352] czy też dopuszczalności zapłodnienia *post mortem*[1353].

Istnieje zauważalna tendencja regulowania zagadnień związanych z medycyną, biologią, biotechnologią na początku dokumentami o charakterze *soft law*, a dopiero po wypracowaniu konsensusu, umowami międzynarodowymi. Szczególnie aktywnie działają w tych obszarach Zgromadzenie Ogólne ONZ oraz Rada Europy, które rekomendacjami i zaleceniami buduje pewne minimalne standardy ochrony. Prawo miękkie w tych przypadkach staje się następnie fundamentem, na którym buduje się normy konwencyjne. Część poglądów doktryny negatywnie odnosi się do *soft law* argumentując, iż nie jest to prawo i co więcej naraża prawo międzynarodowe na ryzyko zatarcia granicy pomiędzy tym, co wiążące, a co nie wiążące. Przychylić się jednak należy się do poglądu Agaty Wnukiewicz - Kozłowskiej, która stwierdza: „oczywiście, badając charakter prawa miękkiego z użyciem tekstu na podstawie kryteriów przypisywanych tradycyjnym źródłom prawa, trzeba uczciwie stwierdzić, że nie można mówić o *soft law* jako pełnoprawnych instrumentach prawa międzynarodowego. Z drugiej jednak strony, nie można nie przyznać, że instrumenty te spełniają część, a nawet więcej - znaczną część - kryteriów wymaganych od zasad, które miałyby być rozważane jako zasady prawa międzynarodowego. W związku z tym nie mogą

[1348] Tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/164 [01.03.2017].
[1349] A. Wnukiewicz - Kozłowska, *Prawo międzynarodowe wobec wyzwań współczesnej medycyny*, [w:] E. Dynia (red.), *Prawo międzynarodowe i wspólnotowe wobec wyzwań współczesnego świata*, Rzeszów 2009, s. 358-359.
[1350] Więcej: M. Słok, *Regulacje prawnomiędzynarodowe dotyczące handlu organizmami modyfikowanymi genetycznie*, [w:] J. Menkes, *Prawo międzynarodowe. Księga pamiątkowa prof. Renaty Szafarz*, Warszawa 2007.
[1351] Więcej: D. Krekora-Zając, *Istota i charakter prawny danych genetycznych*, „Prawo i Medycyna" 2015, nr 4.
[1352] Więcej: M. Kramska, *Międzynarodowe i europejskie standardy ochrony genomu ludzkiego a preimplantacyjna diagnostyka genetyczna*, „Prawo i Medycyna" 2011, nr 3.
[1353] Więcej: M. Marszelewski, *Zapłodnienie post mortem w europejskim prawie porównawczym. Przyczynek do oceny polskiej ustawy o leczeniu niepłodności*, „Prawo i medycyna" 2015, nr 4.

zostać automatycznie odrzucone jako nie-prawo. Zatem *soft law* wypełnia przestrzeń pomiędzy czarnym i białym jako obszar szary"[1354].

Rozwój medycyny, biologii i biotechnologii stawia nas w obliczu pytania o etykę i zakres prowadzonych badań. Prawo, a prawo międzynarodowe w szczególności, może przyjąć jedną z dwóch możliwych ścieżek. Pierwsze podejście przyjmuje jak najszerszą regulację - zarówno w zakresie *soft law,* jak i prawa wiążącego. Drugie, wstrzymuje się od nadmiernej regulacji. Agata Wnukiewicz - Kozłowska stoi na stanowisku, że prawo nie jest w stanie przewidzieć wszystkich możliwych sytuacji, jakie mogą mieć miejsce w praktyce. Dlatego też konieczne jest podjęcie działań w konkretnych obszarach prawa - praw człowieka jako podmiotu współczesnej medycyny. Budowanie nowych standardów musi nastąpić przez przechodzenie od formuły *soft law* do prawa wiążącego[1355]. Pogląd ten zasługuje na pełną aprobatę. W obszarach, w których regulacje są niewystarczające, lub ich po prostu nie ma, czekanie na ostatecznie sformułowanie się (a następnie wejście w życie) norm konwencyjnych stawia społeczność międzynarodową w niebycie prawnym. Tymczasem za pomocą *soft law* można próbować sterować rozwojem prawa stanowionego w pożądanym kierunku, wykształcić praktykę, a może nawet zwyczaj międzynarodowy.

Przestrzeń wirtualna powstała jako sieć wojskowa, a w wyniku komercjalizacji i coraz większej popularności stała się podmiotem niezależnym od władzy państw. Tak jak w przypadku kosmosu, cyberprzestrzeń na skutek ciągłego rozwoju techniki wkracza w obszary nieuregulowane prawnie. Obowiązujące akty prawne wydają się być przestarzałe i nieprzystające do współczesnych stosunków. Powstające wciąż regulacje organizacji międzynarodowych oraz porządki krajowe starają sie sprostać nowym wyzwaniom, jednakże nie można oprzeć się wrażeniu, że zamiast harmonizacji wprowadzają zamęt legislacyjny. Małgorzata Polkowska proponowała, by wobec braku odpowiednich norm międzynarodowych w odniesieniu do kosmosu zastosować prawo krajowe[1356], które sprawniej dostosuje ustawodawstwo do wyzwań technicznych. Zastosowanie podobnej analogii w stosunku do cyberprzestrzeni nie byłoby trafnym rozwiązaniem. Wręcz przeciwnie, to prawo międzynarodowe winno wpływać na odpowiednie zmiany w legislaturze krajowej, wprowadzając spójne i jednolite ustawodawstwo.

[1354] A. Wnukiewicz - Kozłowska, op. cit., s. 357.
[1355] Ibidem, s. 363.
[1356] M. Polkowska, op. cit., s. 261.

Dokonana w niniejszych rozważaniach analiza wyzwań współczesności pokazuje, że tak jak nigdy w historii ludzkości mamy do czynienia z coraz większą liczbą obszarów, w których brak jest regulacji prawnych (zarówno krajowych, jak międzynarodowych). Dotyczy to głównie nowych przestrzeni działalności człowieka, związanych z rozwojem medycyny, techniki czy też skutków eksploatacji ziemi (zanieczyszczenie środowiska, przeławianie łowisk). W tej sytuacji, należy zatem zastosować podejście pragmatyczne - wobec braku norm traktatowych koniecznie jest podjęcie chociażby tymczasowych rozwiązań legislacyjnych. Istnieje wiele obszarów, w których prawo nie ma gotowych odpowiedzi i propozycji metod regulacji. Jednym z tych obszarów jest również cyberprzestrzeń. Mamy obecnie zatem do czynienia z prawem w działaniu *law in action*. Skoro nie ma jeszcze opracowanych wiążących kompleksowych rozwiązań prawnych dotyczących bezpośrednio przestrzeni cyfrowych, to należy - *per analogiam* - posiłkować się istniejącymi, powszechnie uznanymi normami.

Rozdział 6

Postulaty i propozycje rozwiązań prawnych dla cyberprzestrzeni

Wobec braku modelu regulacji cyberprzestrzeni na poziomie krajowym, regionalnym czy międzynarodowym problemem tym zainteresowały się liczne podmioty takie, jak organizacje międzynarodowe, organizacje non-profit (na przykład ICANN, *Creative Commons*), czy też jednostki działające w ramach instytutów badawczych (CERT). W rozdziale zostaną przedstawione propozycje zarządzania cyberprzestrzenią oraz tworzenia właściwego dla niej prawa. Jedno ze stanowisk optuje za tym, by przestrzeń wirtualna była autonomicznym bytem, w stosunku do którego należy wypracować nowe, niekonwencjonalne, dostosowane specjalnie do niego regulacje. Wedle innego stanowiska cyberprzestrzeń powinna być uznana za czwartą przestrzeń międzynarodową obok przestrzeni kosmicznej, morza otwartego oraz dna mórz i oceanów. Oznaczałoby to, że nie podlegałaby ona jurysdykcji żadnego z państw.

Dotychczasowe rozważania wykazały, że granice geograficzne mają znaczenie marginalne w odniesieniu do przestrzeni cyfrowej, a podstawowym problemem jest aterytorialność tego nowego obszaru działalności człowieka. Za pomocą jednego kliknięcia można uzyskać informacje, dokonać czynu przestępczego czy zawrzeć umowę w innym kraju, kontynencie, w innym systemie prawnym. W związku z tym należy postawić następujące pytania. Jak regulować Internet? Kto jest uprawniony do regulacji przestrzeni wirtualnej? Czy cyberprzestrzeń może podlegać samoregulacji? Czy już można mówić o autonomicznym prawie cyberprzestrzeni? Czy istnieją ponadnarodowe normy prawne, które mogą być wykorzystywane do rozstrzygania konfliktów w przestrzeni wirtualnej?

W rozdziale zostanie zaprezentowana koncepcja nowego ładu cyberprzestrzeni w aspekcie podmiotowym, przedmiotowym oraz proceduralnym. Zaproponowane rozwiązanie, ze względu na znaczny obszar regulacji, nie może być uznane za holistyczną i kompletną

regulację rozwiązującą wszystkie problemy cyberprzestrzeni, lecz będzie przyczynkiem do dalszej dyskusji nad tym nowym, problematycznym zagadnieniem.

6.1 Koncepcje samoregulacji cyberprzestrzeni

Globalna sieć komunikacji oparta na sieciach i systemach komputerowych sięga poza granice terytorialne, tworząc nową sferę działalności człowieka, podważając możliwość i legitymację do stosowania prawa wyłącznie na zasadzie jurysdykcji terytorialnej. Użytkownicy nowej, wirtualnej przestrzeni ponad wszystko cenią sobie wolność i przeciwstawiają się wszelkiej nadmiernej ingerencji w nowy cyfrowy ład.

Internet wykształcił się jako projekt wojskowy, jednakże bardzo szybko relacje panujące pomiędzy jego twórcami wpłynęły na kształtującą się sieć cyfrową, która wymknęła się ze sformalizowanych rządowych struktur. Internet ukształtowały środowiska naukowe, w których panowała niesformalizowana, oddolna struktura. Nieoficjalne relacje pomiędzy pierwszymi użytkownikami sieci miały ogromny wpływ na obecny kształt, formę i architekturę cyberprzestrzeni. Kolejne lata rozwoju sieci wirtualnej porównuje się do efektu kuli śnieżnej, gdzie elektroniczne forum dyskusji akademickiej w stosunkowo krótkim okresie czasu przekształciło się w „globalne medium wszechstronnego zastosowania”[1357]. Miliardy użytkowników i urządzeń podłączonych do sieci wirtualnej przyczyniły się do powstania pytania, jak regulować problematyczną przestrzeń cybernetyczną.

W latach dziewięćdziesiątych XX wieku zaczęły tworzyć się pierwsze koncepcje zarządzania Internetem. W 1996 roku John Perry Barlow, założyciel *Eletronic Frontier Foundation*[1358] ogłosił Deklarację Niepodległości Cyberprzestrzeni:

„Rządy Świata Przemysłu: O, wy zmęczone giganty z ciała i stali. Przybywam z Cyberprzestrzeni, nowej ojczyzny Umysłu. W imieniu przyszłości żądam, byście - jako związani z przeszłością - zostawili nas w spokoju. Nie jesteście wśród nas mile widzianymi gośćmi. Nie posiadacie żadnej władzy tu, gdzie się gromadzimy. Nie mamy wybranego rządu,

[1357] K. Dobrzeniecki, *Autonomiczne prawo cyberprzestrzeni: mit czy rzeczywistość?,* [w:] O. Bogucki, S. Czepita (red.), *System prawny a porządek prawny*, Szczecin 2008, s. 316.
[1358] *Electronic Frontier Foundatio*n - amerykańska organizacja pozarządowa walcząca o zapewnienie wolności obywatelskich (tj. prawo do prywatności, anonimowości, wolności słowa) w przestrzeni wirtualnej.

ani nigdy go mieć nie będziemy. Dlatego nie zwracam się do was z pozycji autorytetu, lecz przemawiam głosem wolności. Oświadczam, że globalna przestrzeń społeczna, którą budujemy, jest naturalnie niezależna od tyranii, którą próbujecie na nią narzucić. Nie posiadacie moralnych praw, by nami rządzić. Brakuje wam też metod przymusu, których mielibyśmy się obawiać. Rządy świata opierają swoją siłę na zgodzie rządzonych. Nie ubiegaliście się o naszą zgodę, ani jej nie otrzymaliście. Nie zapraszaliśmy was do współrządzenia. Nie znacie ani nas, ani naszego świata. Cyberprzestrzeń nie leży w zasięgu waszych granic. Nie myślcie, że możecie ją zbudować, traktując jak kolejny budowlany projekt. Nie jesteście w stanie tego dokonać. Cyberprzestrzeń jest aktem natury, która wzrasta poprzez nasze zbiorowe działania. (...) Wasze prawne pojęcia własności, wolności słowa, tożsamości, ruchu i kontekstu nie mają zastosowania do naszej sytuacji. Wszystkie oparte są na zjawiskach świata materialnego. Tymczasem tu nie istnieje materia. Nasze tożsamości nie posiadają ciał, więc - w przeciwieństwie do was - nie możemy stworzyć porządku z użyciem przymusu fizycznego. Wierzymy, że nasza metoda rządzenia wyniknie z etyki, oświeconego samo-zainteresowania i wspólnego dobra. Jedyne prawo uznawane przez należące do nas kultury to Złota Zasada. Mamy nadzieję, że na jej podstawie zbudujemy szczegółowe rozwiązania. Nie możemy przyjąć rozwiązań, jakie próbujecie sam narzucać. (...) W Chinach, Niemczech, Francji, Rosji, Singapurze, Włoszech i w Stanach Zjednoczonych próbujecie pokonać wirusa wolności, wznosząc strażnice na granicach Cyberprzestrzeni. Mogą one zatrzymać zarazę na jakiś czas, ale nie znajdą zastosowania w świecie, który zostanie niebawem zwyciężony przez niosące bity media. (...) Zbudujemy cywilizację Umysłu w Cyberprzestrzeni. Oby był on bardziej ludzki od świata, który stworzyły wasze rządy”[1359].

Wizja Johna P. Barlowa samoregulacji i autonomii zdobyła wielką popularność i w ogromnym tempie rozpowszechniła się wśród użytkowników sieci. Dyskusja nad zagadnieniem niepodległości przestrzeni wirtualnej przerodziła się w koncepcję autonomicznego prawa cyberprzestrzeni.

[1359] J.P. Barlow, *Deklaracja Niepodległości Cyberprzestrzeni*, tłum. J. Staniszewski, [w:] „Magazyn Internetowy WWW” 2000, listopad, s. 36.

6.1.1 Autonomiczne prawo cyberprzestrzeni

W doktrynie pojawiają się poglądy traktujące Internet jako dobro uniwersalne. Brak kompleksowych i przede wszystkim jednolitych zasad funkcjonowania przestrzeni cyfrowej jest jednym z głównych dylematów współczesnej doktryny oraz praktyki prawa[1360]. Wykształcenie się koncepcji autonomicznego prawa cyberprzestrzeni jest zbieżne czasowo z jej powstaniem. Autorami koncepcji autonomicznego prawa cyberprzestrzeni byli David R. Johnson i David G. Post, którzy w głośno komentowanym artykule[1361] stwierdzili, że cyberprzestrzeń jest obszarem posiadającym swój własny, suwerenny i autonomiczny ład prawny, charakteryzujący się anonimowością występujących w nim podmiotów. Wśród jej zwolenników wymienić należy chociażby dyrektorów Instytutu Prawa Cyberprzestrzeni (ang. *Cyberspace Law Institute*), autorów wielu publikacji naukowych czy też Lawrence Lessiga, założyciela inicjatywy *Creative Commons*[1362]. Koncepcja ta znalazła również zwolenników w Polsce. Byli to między innymi Janusz Bart i Ryszard Markiewicz, którzy pod koniec lat dziewięćdziesiątych stwierdzili, że: „warto więc chyba stworzyć autonomiczne prawo cyberprzestrzeni dla sieci komputerowych. Zwolennicy tej interesującej koncepcji wskazują na to, że w cyberprzestrzeni nie występuje terytorialność oparta na granicach państwowych. Co więcej, przy funkcjonowaniu międzynarodowej sieci nie można w zasadzie wskazać na istotne związki z jakimkolwiek konkretnym krajem. Należałoby więc zastanowić się nad przyznaniem cyberprzestrzeni statusu innego miejsca (innej rzeczywistości) niż realny świat, łącznie z własnym porządkiem prawnym. Ten swoisty, odrębny porządek prawny miałby obejmować oczywiście nie tylko prawo autorskie, lecz także prawo patentowe, znaków towarowych, ochronę dóbr osobistych, a być może także elementy prawa procesowego oraz cywilnego"[1363]. Według wskazanej koncepcji regulacja Internetu powinna nastąpić przez stworzenie odrębnego, niezależnego i niezwiązanego z dotychczasowym porządkiem prawnym systemu, który nadawałby cyberprzestrzeni autonomię. Winny zatem zostać wprowadzone oddzielne regulacje, uwzględniające specyfikę przestrzeni wirtualnej, a

[1360] F. Cłapka, *Internet jako wyzwanie dla współczesnych systemów prawa*, [w:] E. Galewska, S. Kotecka (red.), *X-lecie. Księga pamiątkowa z okazji dziesięciolecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego - Blok Prawa Komputerowego*, Wrocław 2012, s. 472-475.
[1361] D. R. Johnson, D. Post, *Law and Borders: The Rise of Law in Cyberspace,* "Stanford Law Review" 1996, t. 48, nr 5.
[1362] J. Kulesza, *Międzynarodowe…*, s. 291.
[1363] J. Barta, R. Markiewicz, *Prawo cyberprzestrzeni i stare konwencje*, „Rzeczpospolita" 1997, 15 listopada.

odnoszące się do określonych dziedzin prawa takich, jak prawo własności intelektualnej, czy też poruszających określone problemy cyberprzestrzeni, na przykład cyberprzestępczość[1364].

Przedstawiciele nauki amerykańskiej David R. Johnson i David G. Post twierdzą, że nie jest możliwe stosowanie tradycyjnego, geograficznego podziału terytorialnego systemu władzy do świata wirtualnego, opartego na zupełnie odmiennych zasadach, gdzie fizyczna lokalizacja przedmiotu nie ma tak istotnego znaczenia. Wskazani autorzy twierdzą, że konieczne jest ustanowienie specjalnych zasad, które będą miały zastosowanie do działań podejmowanych *on-line*. Tylko uznanie prawnego i elektronicznego znaczenia granic elektronicznych, które określają, oddzielają i chronią poszczególne przestrzenie wirtualne zapewni możliwość ustanowienia skutecznego i słusznego systemu zarządzania. Twórcy stoją na stanowisku, że zarządzanie Internetem, które nie jest oparte na koncepcji społeczeństwa obywatelskiego i zasadach demokratycznych, stosowanych do tej pory w określonych geograficznie systemach politycznych, będzie musiało wykazać się wyższością moralną w procesach zarządzania i dialogu publicznym. Proponują zatem stworzenie jednolitego zbioru praw, które będą miały zastosowanie do przestrzeni wirtualnej. Miałoby to nastąpić nie na podstawie zdewaluowanego systemu demokratycznego, w którym przedstawiciele władzy dbają wyłącznie o swoje interesy, lecz za pomocą architektów wirtualnych systemów zarządzania (ang. *architects of on-line governance systems*), którzy opracowaliby system oparty na „cnotach obywatelskich" (ang. *civic virtue*), mogący funkcjonować w zdecentralizowanym i złożonym świecie cyberprzestrzeni. Autorzy uznają, że oddolne wypracowanie reguł, którymi miałyby kierować się społeczności internetowe jest najlepszym rozwiązaniem. Samodzielne wypracowanie systemu norm odpowiadałyby wirtualnej specyfice i regułom rządzącym się autonomią wirtualnych społeczności i cyberprzestrzeni[1365].

Odnosząc się do koncepcji autonomicznego prawa cyberprzestrzeni Joanna Kulesza wskazuje, że: „atrakcyjność koncepcji odrębnego prawa cyberprzestrzeni polega przede wszystkim na wyeliminowaniu wątpliwości jurysdykcyjnych związanych z prawem właściwym i umożliwieniu wypracowania nowych, swoistych konstrukcji prawnych, właściwych jedynie dla Internetu. Reżim taki pozwoliłby na zachowanie obecnego *status quo* wszystkich tych dziedzin prawa, na których Internet wymusił przedsięwzięcie diametralnych zmian (np. prawo autorskie) Mógłby on zawierać reguły dotyczące np. przepływu dóbr

[1364] J. Kulesza, *Międzynarodowe…*, s. 291.
[1365] D.R. Johnson, D.G. Post, *The New 'Civic Virtue' of the Internet: A Complex Systems Model for the Governance of Cyberspace*, "Review of the Institute for Information Studies" 1998, http://www.temple.edu/lawschool/dpost/ Newcivicvirtue.html [10.08.2015].

chronionych między światem pozacybernetycznym a przestrzenią Internetu. Bezsprzeczny jest również fakt, że Internet jest narzędziem posiadającym specyficzne cechy, wymuszające modyfikację dotychczasowej praktyki i zasad. Najistotniejsze z nich to utrudnienia identyfikacji stron stosunku zobowiązaniowego, zdecentralizowany sposób przepływu informacji, możliwość dostępu do informacji przez osoby postronne czy potencjalna dostępność wszelkich informacji potencjalnie naruszających interesy prawne"[1366]. Z kolei Karol Dobrzeniecki wyraził pogląd, że: „regulacja zachowań użytkowników Internetu, bazująca na wewnętrznym prawie państwowym, może być rozwiązaniem skutecznym, na co wskazują doświadczenia ostatnich lat, np. w dziedzinie zwalczania niektórych aspektów przestępczości komputerowej, ale jego zakres oddziaływania jest siłą rzeczy ograniczony podmiotowo i terytorialnie. Żaden lokalny suweren nie ma legitymacji do samodzielnego regulowania globalnego zjawiska, a każde działanie zmierzające w tym kierunku jest zarazem ingerencją w suwerenne kompetencje innych państw. Uzyskiwanie przez poszczególne państwa pełnej kontroli nad transmitowaną w ramach ich granic informacją w postaci elektronicznej, może wywołać poważne zaburzenia w sektorze gospodarczym, opartym na racjonalności globalnej. Rozumieją to nawet państwa o ustroju totalitarnym, takie jak Chiny Ludowe, które nie zdecydowały się całkowicie na „odcięcie" swojego odgałęzienia Sieci, mimo że byłoby to najskuteczniejszym środkiem ochrony przed niepożądanymi treściami pochodzącymi z Zachodu. Rozczłonkowany Internet, podzielony na odseparowane sieci zamknięte w granicach państwowych, straciłby wiele ze swoich właściwości, generujących wzrost gospodarczy i cywilizacyjny. W arsenale tradycyjnych środków kontroli zjawisk wykraczających poza strefę wpływów jednego państwa znajdują się również instrumenty prawa międzynarodowego. Zawodzą one jednak w sytuacjach, gdy przedmiotem regulacji miałyby być gwałtowne, transnarodowe procesy społeczne. Ujawnia się wówczas słabość prawa międzynarodowego, której przejawem są długotrwałe, skomplikowane procedury stanowienia norm oraz trudności w osiąganiu konsensu w wielu fundamentalnych kwestiach. W przypadku Internetu możliwość dokonania szerokich uzgodnień rozbija się m.in. o kwestie ochrony własności intelektualnej i wolności słowa"[1367]. W opozycji do wskazanych wyżej poglądów stanął Filip Cłapka, który stwierdził, że tworzenie prawa Internetu jako zupełnie nowej gałęzi prawa, która miałaby zastosowanie wyłącznie w odniesieniu do przestrzeni cyfrowej mogłoby doprowadzić do „nadregulacji" i tym samym konfliktem norm

[1366] J. Kulesza, *Międzynarodowe …*, s. 291.
[1367] K. Dobrzeniecki, *Autonomiczne…*, s. 316-317.

wewnątrzpaństwowych norm prawnych[1368]. Stworzenie nowego prawa cyberprzestrzeni byłoby procesem długotrwałym, dlatego też jego istota musiałyby oprzeć się (przynajmniej w części) na istniejących podstawach takich, jak ogólne zasady prawa czy stopniowo kształtujące się zwyczaje i normy.

Najważniejszym zadaniem nowego autonomicznego systemu regulacji cyberprzestrzeni byłoby stworzenie zestawu procesów i instytucji mających na względzie wspólne dobro użytkowników. Projektując system należałoby określić, jakie czyny uznane zostałyby za bezprawne, stworzyć zasady etyki i zasad oraz ustanowić mechanizmy ich egzekwowania. Konieczne jest zapewnienie legitymacji działania systemu. Pozwoli to na zapewnienie autorytetu organu władzy oraz zapewni długotrwałe poparcie. Dawid R. Johnson i Dawid G. Post sugerują, by władza była oparta na uznanym autorytecie, który podejmie właściwe kroki w przypadku naruszenia ogólnie przyjętych zasad. Katalog sankcji za naruszenia winien być też zaakceptowany przez całą społeczność. Kolejnym działaniem, jakie należy podjąć jest internalizacja, mająca na celu ograniczenie rozciągania się autorytetów poza „granice", w których są stosowane. Autorzy uważają, że w świecie realnym głównym powodem konfliktów są spory o kompetencje między suwerenami, których da się uniknąć w cyberprzestrzeni, dzięki wyraźnemu ograniczeniu grup w internetowych społecznościach[1369].

Omawiając teorię autonomicznego prawa cyberprzestrzeni należy odnieść się do kwestii obywatelstwa. W świecie rzeczywistym suweren może sprawować władztwo nad osobami znajdującymi się na jego terytorium oraz posiadającymi dane obywatelstwo. Dzieje się tak, gdyż skutki działań podejmowane przez te osoby mają zazwyczaj miejsce na terytorium suwerena. David R. Johnson i David G. Post uważają, że w cyberprzestrzeni brak jest tego geograficznego, terytorialnego „podgrupowania" (ang. *clustering*). Autorzy stawiają tezę, że choć ludzie wciąż mieszkają w określonych geograficznie terytoriach, to cyberprzestrzeń transformowała ludzkość w świat, w którym fizyczne podgrupowanie zanika, przynajmniej w odniesieniu do działań podejmowanych *on-line*. Cyberprzestrzeń w widoczny sposób osłabia więzi terytorialne, ponieważ położenie geograficzne nie ma znaczenia dla zobowiązań podejmowanych w sieci[1370].

Joanna Kulesza odnosząc się do koncepcji Davida R. Johnsona i Davida G. Posta słusznie podnosi, że jej autorzy nie wzięli pod uwagę wszystkich aspektów cyberprzestrzeni.

[1368] F. Cłapka, op. cit., s. 478.
[1369] D.R. Johnson, D.G. Post, op.cit.
[1370] Ibidem.

Autorka zgadza sie z nimi, co do braku możliwości zakreślenia fizycznych barier Internetu, lecz uznaje, że „całkowite abstrahowanie od fizyczności i położenia geograficznego jest za daleko posuniętym uogólnieniem. Z jednej strony skutki działań elektronicznych zawsze odczuwalne są przez konkretne, fizyczne osoby, posiadające obywatelstwo »geograficznego« państwa i podlegające jego porządkowi prawnemu. Z drugiej strony trudno mówić o tak skutecznym i zamkniętym wyodrębnieniu grup w cyberspołeczności, żeby pozwoliło to na zapobieżenie interakcji między nimi, przed czym autorzy próbują ochronić młodą, »elektroniczną«, społeczność”[1371]. Celnie wskazuje ona, że: „trudno wyobrazić sobie grupy - nawet internetowe - tak zamknięte, aby nie następowała między nimi interakcja, a z drugiej strony autorytety tak silne moralnie, żeby nie ulegały pokusie nadużywania swojej władzy (schematy takie znane są już także w rzeczywistości pozawirtualnej, gdzie niektóre z nich, nazywane sektami, zostały zdelegalizowane przez władze krajowe). Wydaje sie, że autorzy zapomnieli o trzecim warunku dla realizacji swojej teorii - nieskazitelnym charakterze i absolutnym posłuszeństwie wobec prawa członków cyberspołeczności, którzy przecież w cyberprzestrzeni czy poza nią pozostają tylko ludźmi. Postulat »cnoty obywatelskiej« w odwołaniu do powszechnych problemów z cyberprzestępczością z jednej, a cenzurą w Internecie z drugiej strony, wydaje się utopijny, choć nie sposób odmówić mu atrakcyjności”[1372]. Należy zgodzić się z poglądem Joanny Kuleszy. O ile koncepcja Davida R. Johnsona i Davida G. Posta, wydaje się być słuszna, o tyle widoczne są jej niedoskonałości i poniekąd idealistyczne podejście, które nie będzie mogło mieć realnego zastosowania w cyberprzestrzeni. Trudno jest wypracować konsensus moralny na ponadnarodowym szczeblu, w którym podmioty kierują się sprzecznymi interesami.

Koncepcja autonomiczności cyberprzestrzeni znalazła też odniesienie w filozofii prawa. Konkurencyjną do pozytywizmu prawniczego tezą jest koncepcja państwa postregulacyjnego (ang. *post - regulatory state*). Główną cechą państwa regulacyjnego jest nacisk na hierarchię systemów jako mechanizmów kontroli. Prawo jest wówczas jednym z głównych mechanizmów zarządzania. Tymczasem w państwie postregulacyjnym zaciera się granica pomiędzy tym, co państwowe a prywatne, a prawo staje się jednym z wielu mechanizmów kontroli. Innymi organami nadzorującymi stają się instytucje takie, jak

[1371] J. Kulesza, *Międzynarodowe …*, s. 293-294.
[1372] Ibidem, s. 294.

stowarzyszenia, organizacje pozarządowe, ponadnarodowe zrzeszenia, związki zawodowe, banki, ubezpieczyciele, jednostki akredytujące czy agencje ratingowe[1373].

Karol Dobrzeniecki odnosząc się do idei państwa postregulacyjnego podnosi, że „w dobie informacjonalizmu katalog potencjalnych środków kontroli poszerza się dodatkowo o rozwiązania techniczne wykorzystywane w informatyce. Na coraz większą skalę ośrodki prawodawcze starają się »wkomponować« reżimy prawne w technikę, osadzić je w technice, nadać jej kształt, który w najwyższym stopniu odpowiadałby ustalonym przez nie dyrektywom. Wykonywanie władzy coraz częściej przejawia się poprzez codzienne kształtowanie, formację i nadzór niż przez wymierzanie sankcji *ex post facto*. Określone ścieżki przemian technicznych są wyznaczane przymusowo lub stymulowane przez bodźce ekonomiczne, podczas gdy inne są tłumione i wypierane z rynku. Po przełomie informatycznym ochrona wielu wartości prawnych, takich jak chociażby wolność słowa, zaczyna być domeną informatyków, inżynierów i programistów, czyli osób, które kształtują cyfrowe środowisko, określają reguły konstrukcyjne technicznej bazy dla interakcji społecznych”[1374]. Z jednej strony cyberprzestrzeń musi być rozpatrywana jako nowa przestrzeń wolności, ale również zagrożeń, ze strony państwa i sektora prywatnego. Nie można dopuścić do nadmiernej regulacji powodującej inwigilację i nieuzasadnione naruszenie prywatności użytkowników sieci. Z drugiej natomiast nie można zupełnie odstąpić od regulacji przestrzeni wirtualnej, ponieważ nie może być to obszar bezprawia, w którym prawa nie ma lub jest całkowicie nieskuteczne. Dopiero po upływie czasu będzie można stwierdzić, czy koncepcja autonomicznego prawa cyberprzestrzeni upowszechni się, czy pozostanie jedynie martwą teorią.

6.1.2 *Lex informatica*

Pojęcie *lex informatica* zostało użyte po raz pierwszy w 1996 roku w pracy holenderskich naukowców Willema H. Van Brooma i Sjefa Van Erpa zatytułowanej

[1373] C. Scott, *Regulation in the Age of Governance: The Rise of the Post Regulatory State*, [w:] J. Jordana, D. Levi-Faur (red.), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance*. Cheltenham 2004, s. 162-164.
[1374] K. Dobrzeniecki, *Autonomiczne…*, s. 317-318.

Electronic Highnvays: On the Road to Liability[1375]. Autorzy użyli tego terminu wyłącznie do określenia możliwych systemów kolizji prawa, mogącego mieć zastosowanie do Internetu[1376]. Wkrótce termin ten zdobył popularność. Według Karola Dobrzenieckiego „»lex informatica« mieści się w zakresie szeroko rozumianego pojęcia »prawo«. Podobnie jak prawo związków wyznaniowych i organizacji sportowych zalicza się do niepaństwowych porządków prawnych. W tym sensie można mówić o jego autonomii. Elementy, które w przekonaniu autorki przesądzają o oryginalności *lex infomatica*, to multicentryczność, globalny zasięg oddziaływania oraz specyficzny sposób ogłaszania i egzekucji reguł, polegający na »wkomponowaniu« ich w techniczną infrastrukturę (architektonikę środowiska). Jest to prawo mające ograniczony zakres przedmiotowy, ponieważ obecnie rozwija się głównie w ramach »nisz« pozostawianych przez regulację państwową i międzynarodową. Jest specyficzne i charakterystyczne dla technicznych uwarunkowań Internetu"[1377].

W związku z wieloznacznością terminu *lex informatica* Stuart Bigel opracował model regulacji Internetu rozróżniając stronę przedmiotową i podmiotową problemu. Strona podmiotowa odpowiada na pytanie, kto może regulować przestrzeń wirtualną. Autor stwierdza, że mogą to być pojedyncze państwa, organizacje międzynarodowe oraz podmioty niepubliczne. Z kolei strona przedmiotowa opisuje za pomocą jakich środków mogłaby nastąpić regulacja Internetu. Uważa się, że istnieje możliwość zastosowania sześciu metod regulacji cyberprzestrzeni. Są to:

1) regulacja behawioralna w stanowieniu prawa wewnętrznego przez poszczególne państwa,
2) regulacja państwowa za pomocą metod infrastrukturalnych,
3) regulacja przez przepisy prawa międzynarodowego,
4) regulacja przez odgórnie narzucone rozwiązania techniczne przygotowane przez organizacje międzynarodowe,
5) regulacja przez podmioty niepubliczne ustalające wzorce zachowań,
6) prywatne środki implementacji „kodu" (ang. *private architectural adjustment*)[1378].

[1375] V. Bekkers, B.J. Koops, S. Nouwt (red.), *Emerging Electronic Highways: New Challenges for Politics and Law*, Haga - Boston - Londyn 1995.
[1376] A. Mefford, *Lex informatica: Foundations of Law on the Internet*, "Indiana Journal of Global Legal Studies" 1997, t. 5, nr 1, s. 211.
[1377] K. Dobrzeniecki, *Autonomiczne…*, s. 323.
[1378] S. Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Cambridge (Massachusetts) 2001, s. 124 i 315, tłum. za: K. Dobrzeniecki, *Autonomiczne…*, s. 318.

Lex informatica obejmuje piątą i szóstą metodę regulacji cyberprzestrzeni, czyli regulację oddolną przez podmioty niepubliczne i użytkowników sieci globalnej. Odnosi się do wszelakiego postępowania internautów w przestrzeni wirtualnej. W latach dziewięćdziesiątych XX wieku przypadających na prywatyzację Internetu pojawiła się potrzeba wypracowania mechanizmów postępowania w odniesieniu do chociażby przetwarzania danych osobowych internautów, zarządzania nazwami i protokołami. Regulacje takie wyłoniły się na różnych szczeblach i w odmiennych formach[1379].

Karol Dobrzeniecki stoi na stanowisku, że „Egzekucja reguł *lex informatica* następuje poprzez wykorzystanie właściwości architektoniki - czyli tzw. »kodu« Internetu. Do tego celu używane są środki sterowania infrastrukturalnego, przede wszystkim standaryzacja techniczna. Stanowi ona »tworzywo«, które może posłużyć do budowania systemów kontroli zachowań. Należy zwrócić uwagę na pewną cechę strukturalną *lex informatica*, którą można określić mianem swoistej warstwowości. Wiąże się one ze wspomnianym zapośredniczeniem oddziaływania *lex informatica* w »kodzie« jako medium regulacji. Architektonikę Sieci tworzy co najmniej kilka poziomów (warstw), w ramach których może dochodzić do ingerencji quasi - poznawczej. Poziomem najniższym są standardy technologiczne (*technical standards*), które wyznaczają obowiązujące protokołu transmisji danych. Niekiedy nazywane są one prawem inżynieryjnym, ze względu na fakt, że tworzą je przede wszystkim specjaliści od kwestii technicznych. Kolejny poziom zajmują tzw. standardy technologiczne (te*chnological standards*)[1380]. Standardy »drugiego poziomu« wyznaczają wzorce oprogramowania (software), które również może być użyte do regulacji zachowań. Każdy kolejny poziom jest niejako fundowany na poziomie wcześniejszym. Zmiana w obrębie tego ostatniego determinuje zmianę w obrębie rozwiązań *lex informatica* wyższego rzędu. Egzekucja norm *lex informatica* na niższych poziomach może następować niezależnie od świadomości osoby, której zachowanie jest poddawane kontroli. Na wyższych poziomach pojawia się potrzeba jej internalizacji przez użytkowników”.[1381]

Przykładem organizacji niepaństwowej, która ma istotny wpływ na kształtowanie formy cyberprzestrzeni jest Korporacja Internetowa do spraw Przyznawania Nazw i Numerów (ICANN). Spory dotyczące domen są rozstrzygane arbitralnie za pomocą Polityki jednolitego rozstrzygania sporów domenowych, która zawiera przepisy materialne i

[1379] K. Dobrzeniecki, *Autonomiczne…*, s. 320.
[1380] Por.: D. Benoliel, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistomology*, “California Law Review” 2004, t. 92, s. 1078.
[1381] K. Dobrzeniecki, *Autonomiczne…*, s. 320-321.

proceduralne. Na podstawie tego dokumentu na przestrzeni lat wykształcił się semiprywatny, autonomiczny system normatywny[1382]. Z tych też względów idea autonomicznego prawa Internetu w ostatnich latach odnosi się głównie do paneli arbitrażowych rozpatrujących spory domenowe.

W doktrynie podkreśla się, że w ICANN: „poszczególne składy arbitrów tworzą system prawa precedensowego, rozstrzygając na podstawie wcześniej wydanych decyzji (...), albo też wprowadzając rozróżnienia (...) dokonują »autonomicznej reprodukcji praw fundamentalnych w obrębie niezależnej logiki internetowego systemu społecznego«. Opierają się przy tym na fikcji »wspólnego rdzenia« zasad prawnych o globalnym zasięgu, obejmującym także prawa człowieka. Konkretyzują specyficzne dla Internetu prawa podstawowe w obrębie prawa powszechnego »między-sieci«[1383]. Rozwój porządku normatywnego ICANN prowadzi zatem do formowania się katalogu praw podstawowych na zasadzie prawa precedensowego, w zakresie np. ochrony znaków towarowych, wolności ekspresji, dóbr osobistych etc. Legitymacja ICANN do stanowienia reguł nie ma charakteru legalistycznego ani demokratycznego. Można ją raczej określić jako odmianę legitymacji charyzmatycznej, której podstawę stanowi efektywność i profesjonalizm. Funkcjonowanie ICANN wsparły te ośrodki władzy, którym najbardziej zależało na utrzymaniu stabilności i operatywności »między-sieci«, a więc przede wszystkim organizacje ekspertów technicznych, przedsiębiorstwa działające w branży teleinformatycznej oraz państwa o rozwiniętym sektorze telekomunikacyjnym. Przypadek ICANN pokazuje, że możliwe jest istnienie pozarządowej instytucji, która koordynuje jeden z kluczowych aspektów funkcjonowania transgranicznego Internetu."[1384] Podnosi się jednak, że działalność ICANN nie równoważy interesów państw rozwiniętych i rozwijających sie, użytkowników i dostawców usług, którzy nie są dostatecznie reprezentowani w instytucji. Można również spotkać się z zarzutami o braku międzynarodowej legitymizacji, wobec czego podnosi się, iż ICANN winien być poddany pod międzynarodowy nadzór ograniczający jej władzę[1385].

Arbitrażowe rozstrzyganie sporów domenowych ujawnia podobieństwo *lex digitalis* (prawa cyfrowego) do tradycyjnego *lex mercatoria*. Porównanie tych systemów doprowadziło Vaiosa Karavasa i Gunthera Teubnera do zaskakujących wniosków. Wzięli oni pod uwagę

[1382] Ibidem, s. 322.
[1383] Por.: A.D. Murray, *Regulation and Rights in Networked Space,* "Journal of Law and Society"2003, t. 30, nr 20.
[1384] K. Dobrzeniecki, *Autonomiczne…*, s. 322-323.
[1385] J. Kulesza, *Międzynarodowe…*, s. 317.

orzecznictwo ICANN, system precedensowy, naturę stosowanych norm, wysoki poziom politycznej legitymacji oraz natychmiastową wykonalność decyzji. Analiza wskazanych instrumentów doprowadziła ich do przekonania, że *lex digitalis* ma znacznie wyższy stopień jakości jurydycznej niż orzeczenia wydane na podstawie historycznej *lex mercatoria*. Wniosek powyższy uzasadniono tym, że decyzje w sprawach domenowych wydane arbitrażowo przez ICANN oparte są na jasnych regułach, publikowanych *on-line*, a ich egzekucja następuje niemal natychmiastowo[1386].

Również I. Trotter Hardy przewidział tworzenie się w Internecie prawa zwyczajowego podobnego do średniowiecznej *lex mercatoria*[1387]. David R. Johnson i David Post zauważyli, że być może najbardziej odpowiednią analogią do nowo tworzącego się prawa cyberprzestrzeni będzie historyczna *lex mercatoria* jako odrębny zestaw reguł opracowany z myślą o nowej cybernetycznej przestrzeni. Stworzony suwerenny, autonomiczny ład prawny powstałby w odłączeniu od odgórnego władztwa państw, które winny albo stosować nowe prawo bądź przynajmniej nie ingerować w jego działanie[1388].

Do największych różnic pomiędzy *lex digitalis* i *lex mercatoria* należy zaliczyć dysproporcję pomiędzy możliwością zastosowania sankcji, egzekwowania i wdrażania decyzji. Okazuje się, że niejednokrotnie nieformalne sankcje stosowane przez rynek są niewystarczające i strona dochodząca swych praw musi poddać się władztwu sądu krajowego i właściwej mu jurysdykcji[1389].

Przemysław Polański postawił tezę, że jesteśmy świadkami tworzenia się nowej, elektronicznej *lex Mercatora,* to jest *Internet lex mercatoria,* którą zdefiniował jako: „zespół zwyczajowych norm postępowania w Internecie, które mogą być użyte do rozstrzygnięcia sporu prawnego"[1390]. Już pod koniec lat dziewięćdziesiątych XX wieku w amerykańskiej doktrynie zaczęły pojawiać się poglądy, że w dobie technologii sieciowych i komunikacyjnych, użytkownicy cyberprzestrzeni napotykają niestabilne i niepewne warunki wielu sprzecznych porządków prawnych. Zasady dotyczące działalności człowieka w cyberprzestrzeni muszą zapewniać stabilność i przewidywalność, tak by użytkownicy mieli

[1386] V. Karavas, G. Teubner, *The Horizontal Effect of Fundamental Rights on 'Private Parties' within Autonomous Internet Law,* "German Law Journal" 2003, nr 4(12), s. 1355-1356.
[1387] I.T. Hardy, *The Proper Legal Regime for Cyberspace*, "University of Pittsburgh Law Review"1994, nr 55, s. 1010.
[1388] D.R. Johnson, D. Post, op. cit., s. 1387-1389.
[1389] V. Karavas, G. Teubner, op. cit., s. 1355.
[1390] P. Polański, *Zarys autonomicznego prawa Internetu*, „Studia Iuridica" 2006, nr 45, s. 179.

wystarczająco dużo zaufania, a społeczność ta mogła się rozwijać. W ocenie Joela R. Reidenberga istnieją trzy obszary cyberprzestrzeni, które wymagają koniecznej regulacji: przetwarzanie informacji osobowych, prawa własności oraz udostępniane w przestrzeni wirtualnej treści[1391].

Konieczne wydaje się wskazanie swoistego katalogu źródeł norm, na którym miałby oprzeć się *Internet lex mercatoria*. Jednak wobec charakteru cyberprzestrzeni nie należy traktować wymienionych poniżej norm jako autonomicznych norm prawnych, lecz jako pewne wskazówki sposobu ich regulacji w Internecie. Podkreśla się, że: „dopiero poprzez powszechne stosowanie tych norm, dla których źródłem powstania mogą się okazać zarówno ukształtowane spontanicznie praktyki handlowe, jak i normy konwencyjne czy umowne, ale wiążące jedynie niewiele państw czy stron, mogą one zostać wykorzystane do rozstrzygania sporów w sieci *erga omnes*. Innymi słowy, takie źródła norm, jak spontanicznie ukształtowana praktyka, orzecznictwo, konwencje, ogólne zasady prawa, modelowe umowy czy standardy techniczne należy postrzegać przez pryzmat ich powszechnego stosowania w praktyce. Bez potwierdzenia norm, których źródłem jest orzeczenie czy standard techniczny w praktyce obrotu, nie można w ogóle mówić o autonomicznym prawie Internetu. Normy wywodzące sie ze wskazanych źródeł należy zatem traktować jedynie jako szczególną formę prawa zwyczajowego. W istocie bowiem tylko powszechne stosowanie praktyki w Internecie, mające swe źródła zarówno w spontanicznych zachowaniach jak i umowach czy konwencjach, można próbować rozważać w kategoriach uniwersalnego, autonomicznego prawa cyberprzestrzeni”[1392]. Jednocześnie podnosi się, że ogólne zasady prawa mogą przyczynić się do standaryzacji w tych obszarach prawa elektronicznego, w których sprzeczności wynikają z różnic kulturowych i prawnych. Nie mniejszą rolę odegrały ustawy modelowe UNCITRAL, proponujące wprowadzenie międzynarodowych rozwiązań w zakresie podpisów elektronicznych, formułowania i ważności umów[1393].

Przez ostatnie lata wzmożonego handlu elektronicznego w praktyce wykształciło się wiele internetowych zwyczajów handlowych. Dotyczą one chociażby ochrony prywatności internautów, własności intelektualnej czy umów elektronicznych. Przy zawieraniu umowy na odległość powszechnie stosowane są następujące normy:

[1391] J.R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, “Texas Law Review” 1998, t. 76, nr 3, s. 554.
[1392] P. Polański, *Zarys…*, s. 180.
[1393] U. Kacker, T. Saluja, *Online Arbitration For Resolving E-Commerce Disputes. Gateway to The Future*, “Indian Journal of Arbitration Law” 2014, t. 3, nr 1, s. 33-34.

- obowiązek zabezpieczenia dostępu do danych za pomocą loginu, hasła bądź innych zabezpieczeń,
- obowiązek umożliwienia kontrahentowi dokonania poprawek danych transakcyjnych przed sfinalizowaniem zakupu,
- obowiązek wprowadzenia zabezpieczeń i szyfrowania transakcji,
- obowiązek używania obowiązujących certyfikatów wydanych przez uprawnionego, kwalifikowanego dostawcę[1394].

Powstaje więc pytanie, czy takie czynności mogą przekształcić się w zwyczaj w rozumieniu prawa międzynarodowego. Na zwyczaj składają się dwa elementy: praktyka (*usus*) oraz przekonanie, że praktyka tworzy prawo (*opinio iuris sive necessitatis*). Odnosząc się do praktyki można brać pod uwagę zachowania podejmowane w Internecie, na które składają się działania zwykłe (na przykład złożenie zamówienia za pomocą kliknięcia w ikonę) i działania zaprogramowane (na przykład automatycznie wygenerowane potwierdzenie zarejestrowania transakcji). Badanie powszechności praktyki internetowej może nastręczyć pewnych problemów. Przemysław Polański wskazuje, iż można dokonać takiej oceny w sposób ilościowy lub jakościowy. Jako metodę ilościową wskazuje przykład szyfrowania transakcji za pomocą protokołu SSL (ang. *Secure Sockets Layer*), wykorzystującego klucze: 128-bitowe, 56-bitowe czy 40-bitowe, oferujące różne poziomy bezpieczeństwa. Ustalając, który z nich jest najczęściej stosowany można by stwierdzić powszechność danej praktyki. Koncepcja wyraźnej większości zakłada, iż praktyka uznana za dominującą musi przewyższać co najmniej o połowę drugą w kolejności praktykę[1395].

Istotne znaczenie dla kształtowania norm prawnych w sieci ma orzecznictwo. W doktrynie zwraca się uwagę, iż uwidacznia się to szczególnie na dwóch płaszczyznach: ponadnarodowego arbitrażu domenowego oraz orzeczeń sądów państwowych, których wyroki są podobne lub identyczne. Ułatwienie mechanizmu alternatywnego rozwiązywania sporów w trybie *on-line* wymagałoby w przyszłości powołania odrębnego organu stosującego ponadnarodowe zasady dotyczące handlu elektronicznego. Konieczne jest również przeprowadzenie kompleksowych badań w celu doprecyzowania dokładnej treści istniejących

[1394] P. Polański, *Zarys…*, s. 181.
[1395] Ibidem, s. 185.

międzynarodowych zasad i sposobów korzystania z handlu elektronicznego oraz monitorowania nowych rozwiązań w celu ciągłego rozwoju *lex informatica*[1396].

Arbitraż domenowy opiera się nie na prawie stanowionym, lecz na zasadach stworzonych przez społeczność internetową. Rządzi się podobnymi prawami co arbitraż międzynarodowego prawa handlowego z trzema różnicami:

1) arbitraż w cyberprzestrzeni jest ograniczony jedynie do rozstrzygania sporów dotyczących rejestracji domen internetowych, nie zajmując się innymi problematycznymi kwestiami, z jakimi można mieć do czynienia w cyberprzestrzeni,
2) arbitraż domenowy w większym stopniu niż tradycyjny wykorzystuje Internet; za jego pomocą następuje nie tylko komunikowanie się ze stronami, lecz nawet rozstrzyganie sporów,
3) rozstrzyganie sporów domenowych następuje w głównej mierze za pomocą stałych sądów polubownych, czyli Centrum Arbitrażu i Mediacji Międzynarodowej Organizacji Własności Intelektualnej, który rozstrzyga w ponad 50% sporów domenowych[1397].

Sądy w sprawach domenowych mogą wydać jeden z trzech typów decyzji: pierwszą, uwzględniającą wnioski powoda, na skutek czego następuje przeniesienie prawa do rejestracji nazwy domeny, drugą (również uwzględniająca wniosek powoda), powodującą unieważnienie prawa z rejestracji domeny oraz trzecią, nieuwzględniającą zarzutów powoda. Zakres spraw i możliwych rozstrzygnięć wydaje się wąski, lecz mimo wszystko działa stosunkowo sprawnie, między innymi ze względu na szybkość postępowania, jego przejrzystość oraz stosunkowo niskie koszty arbitrażu. Nie mniej istotny jest fakt, iż w sądach arbitrażowych do spraw domen zasiadają wykwalifikowani prawnicy specjalizujący się w handlu elektronicznym, domenach internetowych, znakach towarowych oraz Internecie[1398].

Ogólny charakter źródeł prawa internetowego zapewnia ponadnarodowy charakter norm i ich odzwierciedlenie nie tylko w orzecznictwie arbitrażowym, ale również w wyrokach sądów krajowych i międzynarodowych. Podkreśla się, że do wykształcenia się zwyczaju nie jest konieczne jego potwierdzenie w judykaturze sądowej. Jednakże istnienie

[1396] U. Kacker, T. Saluja, op. cit., s. 43.
[1397] P. Polański, *Zarys…*, s. 187.
[1398] M. Rogowski, *Arbitraż w przedmiocie nazw domen internetowych na podstawie Uniform Domain Resolution Policy*, „Rynek - Społeczeństwo - Kultura" 2014, nr 2(10), s. 18-20.

jednolitej linii orzeczniczej współtworzy rozumienie norm obowiązujących w danej dziedzinie prawa. Przy rozpatrywaniu norm, pomocnych do rozstrzygania sporów w sieci, wziąć pod uwagę należałoby ogólne zasady prawa, które również mają zastosowanie w handlu elektronicznym. Zasady takie, jak *pacta sunt servanda, impossibilia nulla est obligatio* czy *rebus sic stantibus* wywodzące się jeszcze z prawa rzymskiego znajdą też zastosowanie w cybernetycznych stosunkach prawnych. Do powyższego katalogu można także zaliczyć kodeksy dobrych praktyk oraz wzorce umów, które mogą pełnić funkcję oddolnego modelu regulacji cyberprzestrzeni[1399].

Przyszłość *lex informatica* oraz jej stosunek do prawa tworzonego przez państwa zależy od wielu czynników. Wśród nich należy wymienić szybkość przemian technologicznych, tempo zmian legislacyjnych oraz to, w jak dużym stopniu państwa będą chciały kontrolować cyberprzestrzeń, a w jakim zakresie pozostawią ją nieunormowaną. Nie ulega jednak wątpliwości, iż potrzebuje ona ponadnarodowego systemu rozstrzygania sporów, który oparty będzie na uniwersalnych normach. Źródłem takich norm mogą okazać się zwyczaje internetowe (*lex mercatoria*), które mogą występować pod postacią spisanych i niespisanych praktyk, jednolitego orzecznictwa czy też prawa modelowego[1400]. Dalsza praktyka pokaże, czy teoria ta zyska zwolenników, czy będzie rozwijać się arbitraż internetowy oraz, w którym kierunku będzie postępować krajowa i międzynarodowa judykatura.

6.1.3 Inicjatywa *Creative Commons*

Creative Commons (CC) jest to międzynarodowy projekt oferujący darmowe rozwiązania prawne oraz narzędzia umożliwiające zarządzanie prawami autorskimi przez twórców i utworów. Inicjatywa powstała w 2001 roku jako amerykańska organizacja pozarządowa założona przez naukowców, prawników oraz intelektualistów zaangażowanych w ochronę dóbr kultury. Obecnie *Creative Commons* działa przez instytucje partnerskie w

[1399] P. Polański, *Zarys…*, s. 188 - 191.
[1400] Ibidem, nr 45, s. 195.

ponad osiemdziesięciu krajach na świecie. Oddział w Polsce został stworzony w 2005 roku[1401].

Celem działania *Creative Commons* jest stworzenie prawa autorskiego, które daje twórcom możliwość zdecydowania, w jaki sposób ich utwór może być wykorzystany. Organizacja wspiera wolną kulturę, produkcję i wymianę utworów traktowanych jako dobro wspólne. *Creative Commons* oferuje różnorodne licencje, które są kombinacją czterech głównych warunków udostępniania utworu:

1) uznanie autorstwa (ang. *attribution*) - pozwala na kopiowanie, rozprowadzenie, przedstawianie i wykonywanie utworu oraz opracowanie na jego podstawie innych utworów zależnych, pod warunkiem przytoczenia nazwiska autora utworu pierwotnego,
2) użycie niekomercyjne (ang. *noncommercial*) - pozwala na kopiowanie, rozprowadzanie, przedstawianie i wykonywanie utworu objętego licencją oraz na opracowanie na jego podstawie utworów zależnych, pod warunkiem, że zostaną one wykorzystane jedynie do celów niekomercyjnych,
3) wyłączenie możliwości użycia utworów zależnych (ang. *no derivative works*) - licencja ta pozwala na kopiowanie, przedstawianie i wykonywanie utworu jedynie w jego oryginalnej wersji; tworzenie zaś utworów zależnych nie jest dozwolone,
4) na tych samych warunkach (ang. *share alike*) - licencja ta pozwala na rozprowadzenie utworu zależnego, jedynie na takiej samej licencji, na jakiej udostępniono utwór oryginalny[1402].

Oprócz wskazanych wyżej rodzajów licencji wprowadzono dwa dodatkowe, które odzwierciedlają globalne trendy działalności twórców. Są nimi:

5) licencja *sampling* - dzięki której możliwe jest samplowanie[1403], remiksowanie i przetwarzanie utworu, zarówno do celów komercyjnych, jak i niekomercyjnych; licencja ta zabrania jednakże zwielokrotniania oryginalnej wersji utworu oraz użycia sampli do celów reklamowych; istnieje również wersja *sampling plus*, która przyznaje

[1401] Dane z oficjalnej strony *Creative Commons*: http://creativecommons.pl/o-nas/, [12.08.2015].
[1402] J. Kulesza, *Międzynarodowe…,* s. 296-297.
[1403] Samplowanie (ang. *sampling*) - jest to użycie fragmentu nagrania muzycznego, zwanego samplem, do stworzenia nowego utworu przy użyciu komputera bądź urządzenia zwanego samplerem.

prawo do zwielokrotniania całości utworów dla celów niekomercyjnych, a wersja *noncommercial plus* - na wykorzystanie jedynie w celach niekomercyjnych,

6) licencja *developing nations* - umożliwia udostępnianie utworu w państwach rozwijających się przy zachowaniu jedynie niektórych praw, z jednoczesnym zastrzeżeniem, że w państwach rozwiniętych autorowi przysługuje pełny zakres praw autorskich[1404].

Jeden z twórców *Creative Commons* Lawrence Lessig w swej książce *Wolna kultura* opisując ideę organizacji stwierdza, że „Creative Commons chce zbudować warstwę treści, chronioną przez warstwę rozsądnego prawa autorskiego, na zrębach której budować mógłby każdy. Nam z kolei te zasoby umożliwią odbudowanie domeny publicznej. Jest to zaledwie jeden z wielu projektów prowadzonych przez Creative Commons i oczywiste jest, że Creative Commons nie jest jedyną organizacją, która w swych działaniach dąży do omówionych powyżej wartości. Cechą odróżniającą Creative Commons od innych jest to, iż nie ograniczamy sie tylko do prowadzenia dyskusji o domenie publicznej i do nakłaniania ustawodawców, aby pomogli tworzyć tę domenę. Jej podstawowym celem jest stworzenie ruchu skupiającego konsumentów i twórców treści (adwokat Mia Garlick nazywa ich »konducentami treści«, *content conducers*), którzy wspomagają budowę domeny publicznej i swoją pracą ukazują znaczenie domeny publicznej dla innych form twórczości”[1405]. Wskazuje on następnie, że: „problemy, jakie obowiązujące prawo stwarza w naszej kulturze wynikają z szalonych i niezamierzonych konsekwencji praw spisanych wieki temu, a zastosowanych obecnie wobec technologii, którą jedynie Jefferson mógł sobie wyobrazić. Te reguły prawne mogły mieć sens w kontekście technologii sprzed wieków, lecz utraciły go wobec technologii cyfrowych. Potrzebujemy nowych reguł, obejmujących różnorodne swobody i wyrażonych tak, że żaden prawnik nie będzie potrzebny. Creative Commons daje ludziom skuteczne narzędzie, za pomocą którego mogą zacząć tworzyć te reguły”[1406]. Inicjatywa *Creative Commons* jest odzwierciedleniem wolnościowej idei cyberprzestrzeni, zarządzanej oddolnie przez użytkowników sieci. Skoro prawa tworzone przez władze krajowe i międzynarodowe nie przystają do nowej przestrzeni cyfrowej to twórcy sami postanowili stworzyć reguły, które będą najlepiej chronić ich prawa do utworu.

[1404] J. Kulesza, *Międzynarodowe…*, s. 297.
[1405] L. Lessig, *Wolna kultura*, Warszawa 2005, s. 312.
[1406] Ibidem, s. 312-213.

W doktrynie trafnie podnosi się jednak, że „o ile inicjatywa L. Lessiga i wszystkich członków CC, jak żadna inna, odpowiada obecnym potrzebom cyfrowego społeczeństwa, o tyle trudne wydaje się pokonanie oporu korporacji medialnych, strzegących swoich wielomiliardowych interesów. Z racjonalnego punktu widzenia jasne jest, że koncepcja CC jest najlepszym rozwiązaniem cyfrowych bolączek prawa autorskiego - zmieniając zupełnie strukturę i zasady jego funkcjonowania, upraszcza obrót i katalizuje postęp. Argumenty L. Lessiga, kierowane są do przedstawicieli organizacji zarządzających prawami autorskimi, dotyczące konieczności zmiany modelu prowadzonej przez nich działalności, wymagają poparcia faktami, także w postaci regulacji prawnych (np. rozszerzających dowolny użytek), które zmusiłyby przedsiębiorców do bliższego przyjrzenia się owej koncepcji."[1407] Nie sposób nie zgodzić się z takimi twierdzeniami. Faktycznie licencje *Creative Commons* stanowią elastyczną alternatywę wobec reguły prawa autorskiego: „wszystkie prawa zastrzeżone", która czasami nadmiernie ogranicza możliwość twórczego korzystania z dóbr kultury. Zaproponowane przez CC rozwiązania w pełniejszy sposób odzwierciedlają światowe trendy działalności autorów i ich potrzeb.

Inicjatywa *Creative Commons* jest również przykładem oddolnego rozwiązania problemów, które są tak charakterystyczne dla cyberprzestrzeni. Twórcy idei wyszli z założenia, że współczesne prawo, czy to na poziomie krajowym czy też międzynarodowym, nie spełnia swojej roli w nowej, cyfrowej przestrzeni. Ochrona praw twórców jest nadrzędna i to oni powinni decydować, w jaki sposób będą udostępniać swoje utwory. *Creative Commons* wychodzi na wprost tym oczekiwaniom, proponując nowe rozwiązania, odzwierciedlające globalne trendy w przestrzeni wirtualnej. Tak jak w przypadku organizacji ICANN inicjatywa *Creative Commons*, bez nadzoru państw, oddolnie proponuje pewne rozwiązania, procedury, mechanizmy i instytucje, które mają bardziej adekwatne zastosowanie do przestrzeni cyfrowej.

[1407] J. Kulesza, *Międzynarodowe…*, s. 298.

6.1.4 Cyberprzestrzeń jako czwarta przestrzeń międzynarodowa

Teoria przestrzeni międzynarodowych opiera się na założeniu, że to nie czynnik terytorialny, lecz narodowy jest podstawą jurysdykcji. Na morzu otwartym o jurysdykcji będzie decydować państwo rejestracji statku, w przestrzeni kosmicznej państwo rejestracji obiektu, a w przypadku Antarktydy narodowość osób tam przebywających. W większości porządków prawnych, w tym w polskim systemie, przyjmuje się, że statek morski jest quasi-terytorium państwa, wobec czego stosuje się do niego zasadę jurysdykcji terytorialnej. Darrel C. Mente przyjmuje jednakże za amerykańskim Sądem Najwyższym[1408], że wejście na statek pływający pod amerykańską banderą nie wywołuje takich samych skutków prawnych, jak wejście na terytorium Stanów Zjednoczonych. Wychodzi on z założenia, iż uznanie statków morskich za quasi - terytorium państwa wynika z przestarzałego prawa uznającego, że prawo do rozciągnięcia swej jurysdykcji musi zawsze mieć związek z terytorium[1409].

W poszukiwaniu odpowiedniego reżimu prawnego dla cyberprzestrzeni wykształciła się teoria uznająca cyberprzestrzeń za czwartą, obok Antarktyki, morza otwartego i przestrzeni kosmicznej, przestrzeń międzynarodową niepodlegającą jurysdykcji żadnego z państw. Darrel C. Manthe uważa, iż motywującym do zawarcia międzynarodowych traktatów regulujących status klasycznych przestrzeni międzynarodowych była wizja potencjalnego konfliktu między innymi przez roszczenia wysuwane co do Antarktyki czy też pierwsze wyprawy w przestrzeń kosmiczną, wysyłane w czasie zimnej wojny. W jego ocenie presja związana z rozwojem cyberprzestępczości i innych zagrożeń cybernetycznych wkrótce doprowadzi do stworzenia odpowiednich uregulowań prawnych również w odniesieniu do przestrzeni cyfrowej[1410].

Ustalenie łącznika jurysdykcyjnego w przypadku morza otwartego, przestrzeni kosmicznej i Antarktydy nie stanowi większego problemu. Nasuwa się pytanie, jaki można by było zastosować w stosunku do cyberprzestrzeni. Darrel C. Menthe uważa, iż jurysdykcja w

[1408] Wyrok Sądu Najwyższego USA, z dnia 10 kwietnia 1929 r., w sprawie *United States ex rel. Claussen przeciwko Day*, sygn. akt 279 U.S. 398, 401.
[1409] D.C. Menthe, op. cit., s. 84-85.
[1410] Ibidem, s. 88.

cyberprzestrzeni winna oprzeć się na zasadzie czynnej jurysdykcji personalnej i proponuje kilka metod umożliwiających ustalenie przynależności państwowej w przestrzeni wirtualnej. Teoretycznie, w przypadku stron internetowych ustalenie narodowości ich twórców nie stanowi większego problemu. Przeważnie wskazani są oni na stronie internetowej. Twórcą może być zarówno osoba fizyczna jak i organizacja. Tę samą metodę analizy jurysdykcyjnej można zastosować do linków stron w cyberprzestrzeni. Twórca linka podlega swemu prawu krajowemu, które stanowi, jakie odesłania, dane i treści wolno mu utworzyć. Osoba, która podąża za linkiem, jest odbiorcą danych, podlega jurysdykcji terytorialnej państwa, w którym przebywa oraz prawu stosowanym w tym państwie w cyberprzestrzeni. W ocenie Darrela C. Menthe'go uznanie cyberprzestrzeni za czwartą przestrzeń międzynarodową spowodowałoby, że osoby umieszczające dane w sieci odpowiadałyby wyłącznie prawu państwa, w którym treści te zostały udostępnione. Uniknąć w ten sposób można by było sytuacji, w której nadawca udostępnia treści nie wiedząc, iż są one niezgodne z prawem innego państwa. Nie ma również przesłanek na podstawie tej teorii by państwo nadawcy tworzyło prawo ograniczające działania odbiorcy danych[1411]. Autor nie dostrzega jednak negatywnych konsekwencji tej koncepcji. Poddanie danych treści wyłącznie prawu państwa, w którym zostały one udostępnione powodowałoby *forum shopping*, czyli tworzenie stron internetowych w porządkach prawnych, które nie zakazują danych czynów bądź przyjmują liberalniejszą wykładnię chociażby wolności słowa czy czynów rasistowskich i ksenofobicznych.

Teorię Darrela C. Menthe popiera Joanna Czekalska. Stwierdza ona, że: „cyberprzestrzeń jako przestrzeń międzynarodowa rządziłaby się podstawowym kryterium jurysdykcji personalnej państwa w stosunku do swoich obywateli, niezależnie z którego miejsca na ziemi i przy pomocy jakiego serwera operują. Nie ma tu zastosowania wymóg podwójnej penalizacji działania ze względu na fakt, że kara jest wymierzona podmiotom będącym obywatelami suwerena, działającymi na jego szkodę i tylko naruszenie istotnego interesu własnego państwa daje temu państwu legitymację do ścigania. Wobec faktu powszechnej dostępności sfery, jaką jest przestrzeń elektroniczna, to narodowość powinna być pierwszym kryterium regulującym zachowania podmiotów sieci. Oczywiście, tak jak choćby w przypadku morza otwartego i prawa państwa bandery do sądzenia czynów popełnionych na pokładzie jego okrętu, także państwo, w którym znajduje się potencjalny naruszyciel, regulować powinno spektrum dozwolonych i niedozwolonych zachowań,

[1411] Ibidem, s. 93-94.

korzystając ze swojego podstawowego atrybutu władztwa terytorialnego. Niemniej jednak zastosowanie teorii przestrzeni międzynarodowych pozwala na przekształcenie cyberprzestrzeni z miejsca podlegającego nieskończenie wielu regulacjom w miejsce podlegające najwyżej dwu konkurującym porządkom prawnym. Przeciętny użytkownik sieci nie będzie musiał obawiać się skazania w kraju odległym czy egzotycznym tylko dlatego, że jego wiadomość tam także będzie dostępna. Jest to jedyne rozwiązanie pozwalające zapewnić pewność prawa w obrocie elektronicznym".[1412] W licznych przypadkach oparcie jurysdykcji na zasadzie narodowości mogłoby w znacznym stopniu ograniczyć spory jurysdykcyjne. Jednakże wydaje się, że nie może to być zasada wyłączna.

Krytycznie do teorii cyberprzestrzeni jako czwartej przestrzeni międzynarodowej wypowiada się z kolei Joanna Kulesza: „propozycja D.C. Menthe'go może okazać się zbyt radykalna. Uznanie cyberprzestrzeni za przestrzeń międzynarodową nie jest warunkiem koniecznym dla zastosowania w niej zasady personalnej. Przedstawiona przez niego analiza nie uwzględnia istniejących mechanizmów prawa międzynarodowego prywatnego, które pozwalają na zastosowanie prawa nadawcy treści elektronicznych w relacjach opartych o kontakty internetowe. Jednocześnie wskazany łącznik, determinujący przynależność jurysdykcyjną podmiotu, jakim jest strona www, nie wyczerpuje całego katalogu możliwości działania, jakie przedstawia swoim użytkownikom Internet. Koncepcja ta korzysta z utrwalonych już schematów jurysdykcji personalnej, która nie jest przypisywana wyłącznie przestrzeniom międzynarodowym, a stosowana jest także w obrocie terytorialnych państw. W przedstawionej propozycji niezbyt wyraźnie widać także szczególne korzyści, jakie płynęłyby z przyjęcia teorii czwartej przestrzeni międzynarodowej, których nie sposób uzyskać stosując odpowiednio modyfikowane zasady tradycyjnej jurysdykcji personalnej. Ponadto, sama natura owych »przestrzeni« także bardzo silnie opiera się o ich terytorialny wymiar, którego to aspektu nie sposób przypisać cyberprzestrzeni. Niemniej jednak koncepcja ta z pewnością stanowi rozwiązanie oryginalne i w pewien sposób jest uzupełnieniem (...) koncepcji D.G. Posta, D.R. Johnsona, wyłączenia cyberprzestrzeni jako takiej spod regulacji terytorialnych państw, idąc o krok dalej w kierunku sformalizowania tego statusu".[1413] Należy przychylić się do krytycznych uwag Joanny Kuleszy w przedmiocie oparcia łącznika jurysdykcyjnego na zasadzie personalnej. Zastanowić się jednak należy, które z zasad stosowanych do przestrzeni międzynarodowych mogłyby mieć rekonstrukcyjne zastosowanie w cyberprzestrzeni, gdyż

[1412] J. Czekalska, op. cit., s. 80.
[1413] J. Kulesza, *Międzynarodowe…*, s. 300-301.

obszary te zachowują jednak pewne punkty styczne (związane na przykład z zasadą niezawłaszczalności).

Rozważania dotyczące przestrzeni międzynarodowych przeniesione na grunt cyfrowy prowadzą znawców tematu do następujących wniosków: „trzy uznane już za międzynarodowe przestrzenie różnią się jednak od cyberprzestrzeni jedną podstawową cechą, jaką jest fizyczność. To, co je jednak łączy, to przede wszystkim względna wolność od wszelkiej suwerennej władzy. Jako czwarta przestrzeń międzynarodowa cyberprzestrzeń powinna być zarządzana przez zestaw niezależnych, samodzielnych zasad, które odpowiadałyby zasadom jurysdykcji rządzącym trzema pozostałymi przestrzeniami międzynarodowymi, nawet pod nieobecność organizacji ów reżim narzucającej (które to organizacje funkcjonują w stosunku do trzech pozostałych przestrzeni międzynarodowych)”[1414].

Koncepcja uznania cyberprzestrzeni za czwartą przestrzeń międzynarodową nasuwa pytanie o to, czy w stosunku do przestrzeni wirtualnej można wykorzystać reguły stosowane do innych przestrzeni, a jeśli tak, to jakie. Nie ulega wątpliwości, iż każda z przestrzeni międzynarodowych posiada swoją specyfikę. Szczegółowa analiza przeprowadzona w poprzednim rozdziale wskazuje, iż istnieją punkty styczne, podobieństwa cyberprzestrzeni do innych przestrzeni międzynarodowych, a co związane jest ze stosowaniem niektórych norm na zasadach *a simili*. Tak, jak w klasycznych przestrzeniach międzynarodowych żadne państwo nie może zgłaszać roszczeń ani wykonywać praw suwerennych w całej cyberprzestrzeni oraz istnieje w niej wolność „surfowania” - poruszania się, odpowiadająca wolności przepływu bądź przelotu.

Cyberprzestrzeń wykazuje najwięcej podobieństw do przestrzeni kosmicznej, która jest wolna, niezawłaszczalna, zapewnia się w niej możliwość swobodnego dostępu i użytkowania, promuje odpowiedzialność i współpracę w zakresie jej wykorzystania dla wszystkich oraz współpracę międzynarodową w tych działaniach. Wydaje się, iż przestrzeń cyfrowa mogłaby być uznana za wspólne dziedzictwo ludzkości. Przestrzeń ta, tak jak kosmos, winny być wykorzystywane dla wspólnego dobra, na potrzeby całej ludzkości, każda osoba powinna mieć dostęp do zgromadzonych w niej zasobów (dostęp do wiedzy, informacji, edukacji, rynków). Użytkowanie przestrzeni cyfrowej, mimo licznych zagrożeń i niebezpieczeństw, w skali globalnej przynosi więcej korzyści niż strat. Cyberprzestrzeń przyśpieszyła rozwój gospodarki, wymianę dóbr i towarów, stworzyła nowe gałęzie handlu,

[1414] J. Czekalska, op. cit., s. 80.

umożliwiła dostęp do edukacji, ułatwiła i zwiększyła możliwości taniej komunikacji, transportu (GPS) i współpracy międzynarodowej. John Vogler uznał, że do cech charakterystycznych globalnych dóbr wspólnych zaliczyć należy otwarty dostęp, niewykluczalny charakter oraz wspólną, niezawłaszczalną pulę zasobów[1415]. Dostęp do tych dóbr mają zarówno podmioty państwowe, jak i niepaństwowe. Jedną z ich cech jest ścisłe powiązanie z obecnym rozwojem naukowym i stopniem możliwości technologicznych. Przez setki lat za jedyne dobro wspólne uznawane było morze otwarte, jednakże dopiero rozwój techniki w XX wieku umożliwił eksplorację zupełnie nowych, nieznanych obszarów Antarktyki oraz przestrzeni kosmicznej. Znawcy tematu twierdzą, iż obok powszechnie uznanych klasycznych przestrzeni międzynarodowych pojawiają się nowe takie, jak klimat oraz przestrzeń cyfrowa. Część ekspertów postuluje, by cyberprzestrzeń oraz Internet uznać za nowe elektroniczne globalne dobra wspólne[1416].

Analogia do morza otwartego oraz do przestrzeni kosmicznej wiąże się z traktowaniem cyberprzestrzeni jako dobra wspólnego, z którego mogą korzystać wszystkie państwa, również do celów militarnych, o ile postępowanie takie jest zgodne z prawem międzynarodowym[1417]. Przestrzenie międzynarodowe w teorii winny być wykorzystywane w sposób pokojowy, nie naruszając praw innych podmiotów. Wydaje się, że zasada ta, mimo szczytnego celu, nie znajdzie zastosowania w cyberprzestrzeni. Nie ulega wątpliwości, że przestrzeń cyfrowa jest wykorzystywana do walki informacyjnej, inwigilacji, prowadzenia polityki państw, a nawet manipulacji. W przyszłości prawdopodobne jest wkroczenie konfliktów zbrojnych na nowy cyfrowy poziom. Cyberwojna jest tylko kwestią czasu, niektóre państwa już wykorzystują hakerów „cyberżołnierzy" do wspomagania walk w świecie realnym. Z tych też względów postulat pokojowego wykorzystania cyberprzestrzeni, choć szczytny, wydaje się być mało realny do wykorzystania w praktyce. Zastanowić się również należy, czy istnieje możliwość zastosowania w cyberprzestrzeni kryterium przynależności na wzór bandery czy też rejestracji statku w danym kraju. Mimo, że technicznie można uznać, że witryna w danej domenie, języku czy zapisana na serwerze znajdującym się na terytorium danego kraju, winna podlegać jurysdykcji konkretnego państwa, to nie można uznać, że przyznanie na tej zasadzie jurysdykcji będzie rozwiązaniem

[1415] J. Vogler, *The Global Commons*, Toronto 1995, s. 2.
[1416] J. Vogler, *Global Commons Revisited*, „Global Policy" 2012, t. 3, nr 1, s. 63.
[1417] J. Bryła, *Wkład Unii Europejskiej w rozwój międzynarodowego reżimu kosmicznego*, „Rocznik Integracji Europejskiej" 2015, nr 9, s. 128.

efektywnym. Wręcz przeciwnie, wprowadziłoby to chaos organizacyjny oraz mogłoby doprowadzić do *forum shopping*.

Przestrzenie międzynarodowe są uważane za wspólne dziedzictwo ludzkości. John E. Noyes wyróżnia cechy charakterystyczne wspólnego dziedzictwa ludzkości: zakaz zawłaszczenia oraz rozciągania na ten obszar suwerenności któregokolwiek z państw, uznanie obszaru za obszar należący do całej ludzkości, nakaz wykorzystania obszaru w celach pokojowych, ochronę środowiska naturalnego, dzielenie korzyści uzyskanych z obszaru, ze szczególnym uwzględnieniem państw rozwijających się, zarządzanie za pomocą wspólnego międzynarodowego reżimu[1418]. Wszystkie wymienione pryncypia (oczywiście prócz ochrony środowiska naturalnego) mogą być zastosowane bezpośrednio do cyberprzestrzeni. Wskazane wyżej koncepcje zasługują na głęboką rozwagę. Czerpanie z istniejących koncepcji mogłoby stanowić bazę do ugruntowania się w kolejnych dekadach prawa cyberprzestrzeni opartego na solidnych podstawach.

6.2 Koncepcja nowego ładu cyberprzestrzeni

Cyberprzestrzeń nie może być przestrzenią, w której nie funkcjonuje prawo. Zwiększenie się liczby użytkowników oraz powszechniejszy, łatwiejszy i szybszy dostęp do przestrzeni cyfrowej doprowadził między innymi do lawinowego wzrostu liczby zagrożeń. Słusznie podnosi, Ryszard Tadeusiewicz, że „dopóki Internet był wyłączną domeną uczonych, a następnie także relatywnie nielicznych amatorów sieciowej komunikacji, dopóki był całkowicie (programowo!) oderwany od jakiejkolwiek działalności komercyjnej - był on obszarem, w którym prawo nie było potrzebne. Mało tego, w tym pionierskim okresie rozwoju Internetu brak jakiejkolwiek władzy, która by nim zarządzała, a zwłaszcza brak jakiejkolwiek formalnej regulacji normatywnie określającej kierunki jego rozwoju - był nawet traktowany jako swoisty manifest ideowy i stanowił jeden z zasadniczych dogmatów funkcjonowania międzynarodowej społeczności Internautów”[1419]. Kolejne etapy rozwoju

[1418] J. E. Noyes, *The Common Heritage of Mankind: Past, Present, and Future*, “Denver Journal of International Law & Policy” 2012, nr 447, s. 450-451.
[1419] R. Tadeusiewicz, *Internet i prawo*, http://winntbg.bg.agh.edu.pl/skrypty/0037/cz0-r1.pdf [22.02.2017].

Internetu, a zwłaszcza jego komercjalizacja spowodowała, że wyłoniła się potrzeba wprowadzenia regulacji przestrzeni cyfrowej.

W niniejszym podrozdziale zostanie przedstawiona propozycja przyjęcia prawa cyberprzestrzeni oraz podmiotowy, przedmiotowy i proceduralny ład cyberprzestrzeni. Niniejszy rozdział nie wyczerpuje całości problematyki nowego ładu przestrzeni cyfrowej, ponieważ jest to problem zbyt złożony. Opracowanie norm i zasad postępowania w cyberprzestrzeni będzie stanowić wyzwanie dla praktyków i teoretyków prawa na kolejne dziesięciolecia. Opisane w niniejszym podrozdziale koncepcje być może staną się przyczynkiem do dalszej dyskusji.

6.2.1 Rekonstrukcja pojęcia prawa cyberprzestrzeni

W stosunku do prawa cyberprzestrzeni, w zagranicznej literaturze prawniczej, używa się wyrażeń: *cyberlaw, lex electronica, lex informatica, lex cybernetica, lex digitalis, Internet lex mercatoria*[1420]. Do cech cyberprzestrzeni zalicza się: „plastyczność, płynność, obliczalność, dokładność, hipertekstowość, interaktywność, wirtualność, kompatybilność, otwartość, nieograniczoność, wszechstronność, złożoność, sieciowość, przenikalność, konwergentność, konsolidację, automatyzację i totalność”[1421].

Do chwili obecnej nie została wypracowana powszechnie przyjęta definicja cyberprzestrzeni. Gdy rzeczywistość z powieści *since - fiction Neuromancer* stała się prawdą, zaistniała potrzeba wprowadzenia jej legalnej definicji. Zaakcentować należy, że nie można utożsamiać cyberprzestrzeni z Internetem. Jest ona pojęciem o wiele szerszym, obejmującym zarówno Internet, jak i przestrzeń cyfrową. Internet winien być rozumiany jako „sieć sieci”, czyli globalna sieć połączonych ze sobą komputerów i serwerów. Cyberprzestrzeń ma bardziej metaforyczne znaczenie i odnosi się do przestrzeni, która istnieje w zakresie Internetu. Co więcej, będzie obejmować inne niż Internet sieci takie, jak chociażby Darknet. Również w piśmiennictwie podnosi się, że „uzasadniony jest pogląd, iż to Internet stanowi jedynie nowe medium, nowy środek komunikacji, obok takich mass mediów, jak prasa, radio

[1420] F. Cłapka, op. cit., s. 476.
[1421] J. Janowski, *Cybernetyzacja*…, s. 396

czy telewizja, natomiast cyberprzestrzeń powinna być uznana za miejsce lub przestrzeń, co odpowiadałoby tej nazwie"[1422].

Konieczne jest zdefiniowanie cyberprzestrzeni, jak i prawa cyberprzestrzeni, by wprowadzić spójną międzynarodową regulację przestrzeni wirtualnej. Tymczasem na poziomie zarówno międzynarodowym, regionalnym, jak i krajowym występuje szereg rozbieżnych i często nieadekwatnych definicji. Władze krajowe w wypracowanych przez siebie definicjach często odwołują się do przestrzeni informacyjnej, wymiany, modyfikowania i przetwarzania informacji, zaznaczając równocześnie, iż cyberprzestrzeń jest pojęciem szerszym niż sam Internet, jednakże w dużej części na nim bazującym. Rozróżnienie to jest trafne, gdyż cyberprzestrzeń ma znacznie szerszy charakter i zgodnie z przewidywaniami będzie się dalej rozwijać, tworząc nowe sieci i przestrzenie.

Wobec wielu sprzecznych definicji cyberprzestrzeni i mnogości ich interpretacji Piotr Sienkiewicz wyróżnia podstawowe ujęcia:

1. Cyberprzestrzeń jako Internet, jego zasoby, użytkownicy i usługi.
2. Cyberprzestrzeń jako wirtualna rzeczywistość generowana przez Internet, sieć i komputer.
3. Cyberprzestrzeń jako społeczna megasieć - „sieć sieci", w której użytkownicy eksploatują jej globalne zasoby.
4. Cyberprzestrzeń jako ewoluujący, dynamiczny system złożony, niezależnie od przyjmowanych różnych walorów technicznych, informacyjnych czy społecznych[1423].

Wśród wyżej wymienionych propozycji najbardziej elastyczna, a zarazem odpowiednia do dynamicznie zmieniającej się cyberprzestrzeni, jest czwarta z nich. O ile różni autorzy oraz niektóre państwa podejmują się zdefiniowania pojęcia cyberprzestrzeni, o tyle termin prawo cyberprzestrzeni pojawia się stosunkowo rzadko. Wobec tego, konieczne jest zaproponowanie definicji prawa cyberprzestrzeni. Za prawo cyberprzestrzeni powinno być uznane prawo, które reguluje funkcjonowanie i wykorzystanie cyberprzestrzeni. Ta zwięzła definicja stanowi swoisty postulat, będący punktem wyjścia do dalszych rozważań w tym przedmiocie. W chwili obecnej prawo, w tym prawo międzynarodowe, jedynie próbuje regulować kwestie związane z cyberprzestrzenią. Zdefiniowanie prawa cyberprzestrzeni jest

[1422] A. Górska, *Bezpieczeństwo a aterytorialność cyberprzestrzeni*, „Prace Naukowe Wyższej Szkoły Bankowej w Gdańsku" 2014, t. 33, s. 200.
[1423] P. Sienkiewicz, *Ontologia…*, s. 93.

trudne, ale możliwe do wykonania. Prawdziwym wyzwaniem jest jednak faktyczne i adekwatne uregulowanie przestrzeni cyfrowej. Cyberprzestrzeń ze swej natury jest otwarta, niescentralizowana, oddolna, dynamiczna, aterytorialna i ponadnarodowa. Prawo z kolei oparte jest na hierarchiczności norm, formalizmie, porządku oraz konkretności przepisów i procedur. Zderzenie tych dwóch odrębnych światów prowadzi do szeregu problemów legislacyjnych, nieprzystosowania stosownych rozwiązań i norm do zupełnie nowej przestrzeni działalności człowieka.

Część doktryny uznaje, że nie można jeszcze wyodrębnić prawa cyberprzestrzeni jako samodzielnej gałęzi prawa mimo wydania aktów prawnych o charakterze zarówno globalnym, jak i regionalnym. Mają one charakter rozproszony, regulujący jedynie wąski zakres obszernej problematyki. Nie można uznać, by regulacje te składały się na kompleksowy i autonomiczny system. Również według Jacka Janowskiego prawo cyberprzestrzeni jest: „kształtującą się sferą regulacji prawnych oraz rozwijającą się dziedziną nauczania prawa, obejmującą zagadnienia na styku prawa i komputerów, ze szczególnym uwzględnieniem problemów Internetu, w zakresie prawa autorskiego, wynalazczego i znaków towarowych, odpowiedzialności dostawców usług elektronicznych i uczestników handlu elektronicznego, stosowania cenzury publikacji i kontroli korespondencji, prowadzenia reklamy i marketingu w sieci, zapewniania poufności i bezpieczeństwa danych. Zadaniem cyberprawa jest zarówno diagnozowanie nowych zjawisk w systemach informatycznych i sieciach teleinformatycznych, wymagających uregulowań prawnych, jak również prawna ich interpretacja”[1424]. Wyliczenie to, choć szczegółowe, nie odzwierciedla realnej skali problemów jakie może powodować działalność człowieka w cyberprzestrzeni, pomijając przestępczy aspekt przestrzeni wirtualnej, czyli cyberprzestępczość, cyberwojnę czy cyberterroryzm oraz związanych z tym unormowań prawnych.

W znaczeniu ogólnym prawo cyberprzestrzeni odnosi się do prawnych aspektów działalności człowieka i innych podmiotów w przestrzeni wirtualnej. Prawo cyberprzestrzeni jest związane z innymi, tradycyjnymi działami prawa, czyli prawem karnym, cywilnym, prawem własności intelektualnej, ale również prawami człowieka, wolności wypowiedzi, ochroną danych osobowych oraz kwestią jurysdykcji. W chwili obecnej każda wymieniona dziedzina prawa próbuje stworzyć własne, adekwatne do cyberprzestrzeni przepisy. Normy te

[1424] J. Janowski, *Informatyka prawa. Zadania i znaczenie w związku z kształtowaniem się elektronicznego obrotu prawnego*, Warszawa 2011, s. 414.

różnią się od siebie jednak technicznie oraz systemowo i nie zawsze w sposób najodpowiedniejszy przystają do cyberprzestrzeni.

Prawo cyberprzestrzeni musi zatem zdystansować się od pryncypialnych, tradycyjnych formalnych ram, tworząc nowy byt - prawo, które nie będzie oparte wyłącznie na czynniku terytorialnym, lecz które zmierzy się z nową wirtualną przestrzenią. Prawo cyberprzestrzeni wymaga innego, nowatorskiego podejścia. Ze względu na naturę cyberprzestrzeni również prawo w niej obowiązujące posiada cechy charakterystyczne takie, jak międzynarodowa natura, brak granic terytorialnych, występowanie nowych aktorów międzynarodowych wywołujących realny wpływ na tworzenie się prawa cyberprzestrzeni (wielkie korporacje internetowe na przykład Google, Facebook) oraz często oddolna struktura tworzenia się norm. Nasuwa się zatem pytanie, czy jest możliwe stworzenie nowej dyscypliny prawa - prawa cyberprzestrzeni, zupełnie innej od tradycyjnych gałęzi prawa. Wydaje się, że prawo to może utworzyć się w ramach prawa międzynarodowego bądź na poziomach krajowych (jednakże wówczas prawo to będzie niejednolite, rozproszone, a normy będą powstawać wolniej). Tworzenie się prawa cyberprzestrzeni będzie procesem długotrwałym, między innymi z powodu trudności w wypracowaniu międzynarodowego konsensusu wśród państw kierujących się zupełnie sprzecznymi interesami. Gdy w końcu kompromis zostanie raz wypracowany, to będzie przestrzegany przez państwa i inne podmioty. Do tego czasu i do chwili wytworzenia się prawa pozytywnego ogromną rolę odgrywa tworzone na bieżąco prawo miękkie, które wskazuje potencjalne i pożądane kierunki regulacji.

Prawo cyberprzestrzeni napotyka trudności w jego efektywnym stosowaniu. Spowodowane jest to kilkoma czynnikami. Przede wszystkim problemem jest brak międzynarodowych, powszechnie stosowanych standardów i norm prawnych, posługujących się zunifikowanymi definicjami. Kolejnym czynnikiem jest konieczność zapewnienia szeroko zakrojonej współpracy międzynarodowej, szybkiej wymiany informacji i doświadczeń oraz zapewnienia efektywnej pomocy prawnej (ma to szczególne znaczenie w przypadku cyberterroryzmu i cyberprzestępczości). Tylko ścisła współpraca międzynarodowa i ujednolicone standardy pozwolą na efektywne zwalczanie czynów przestępczych w przestrzeni wirtualnej między innymi w zakresie zbierania dowodów cyfrowych.

6.2.2 Aspekt podmiotowy nowego ładu cyberprzestrzeni

Omawiając nowy ład cyberprzestrzeni należy postawić sobie pytanie, kto jest władny do regulacji przestrzeni wirtualnej. Przegląd dotychczasowych regulacji prawnomiędzynarodowych prowadzi do wniosku, iż ogromną rolę w unormowaniu działań człowieka w cyberprzestrzeni spełniają organizacje międzynarodowe. To właśnie pod auspicjami tych podmiotów prawa międzynarodowego powstały umowy międzynarodowe i dokumenty, które przyczyniły się do harmonizacji przepisów krajowych. Szczególną rolę odegrały trzy organizacje międzynarodowe: Organizacja Narodów Zjednoczonych, Rada Europy oraz Unia Europejska. Nie można jednak umniejszać znaczenia innych instytucji, które również miały swój wkład w tworzenie prawa przestrzeni wirtualnej. Niestety, brak jest jednego, międzynarodowego organu, który miałby kompetencje do wprowadzania holistycznych zmian w ponadnarodowym zarządzaniu i regulacji cyberprzestrzeni.

Analiza międzynarodowych regulacji prowadzi do przekonania, iż obecne normy prawne dotyczące cyberprzestrzeni są rozproszone, fragmentaryczne, częściowo przestarzałe i jedynie w niewielkim zakresie regulują przestrzeń cyfrową. Głównym problemem jest brak centralnej międzynarodowej instytucji czy organizacji międzynarodowej, która koordynowałaby działania legislacyjne. W kontekście tym należy postawić sobie pytanie, kto powinien być odpowiedzialny za tworzenie prawa w cyberprzestrzeni na poziomie międzynarodowym. Jednym z rozwiązań mogłoby być utrzymanie *status quo*, w którym przepisy są tworzone przez państwa w drodze umów dwustronnych i wielostronnych bądź też w ramach organizacji międzynarodowych. Rozwiązanie to jest jednak niewystarczające, ponieważ nie zapewnia kompleksowej, holistycznej regulacji. Co więcej, prace niektórych organizacji międzynarodowych powielają się zamiast uzupełniać. Akty prawne i propozycje organizacji takich, jak Unia Europejska bardzo często proponują trafne rozwiązania, jednakże ich regionalny charakter powoduje, że prawo cyberprzestrzeni nie może mieć realnego wpływu na działania w innych regionach świata. Z tych też względów niezbędne jest powołanie globalnej instytucji międzynarodowej, która będzie odpowiedzialna za tworzenie międzynarodowych norm postępowania w cyberprzestrzeni w najróżniejszych dziedzinach prawa w zakresie cyberprzestępczości, cyberterroryzmu, praw człowieka, praw własności intelektualnej czy też handlu elektronicznego.

Instytucja taka mogłaby zostać powołana do życia bądź jako organizacja wyspecjalizowana ONZ bądź też jako nowa, niezależna organizacja zrzeszająca zainteresowane podmioty. Przyjęcie pierwszego z zaproponowanych rozwiązań, powierzenie regulacji cyberprzestrzeni organizacji wyspecjalizowanej ONZ, nie jest pomysłem wolnym od wad. Stworzenie takiej organizacji, wypracowanie jej struktury, statutu, ustalenie liczby potencjalnych członków byłoby procesem długotrwałym. Ponadto, często podnosi się, że ONZ i jej organizacje wyspecjalizowane mają niską skuteczność. Powodem takiego stanu jest między innymi to, że państwa o rozbieżnych interesach paraliżują prace poszczególnych organów. Problematyczna mogłaby również okazać się kwestia finansowania organizacji. ONZ, biorąc pod uwagę ogromną strukturę organizacji, ma stosunkowo niski budżet, tymczasem stworzenie, niemal od podstaw, międzynarodowego prawa cyberprzestrzeni mogłoby wiązać się ze sporymi kosztami. Wypracowanie pierwszych wymiernych wyników pracy i norm traktatowych zajęłoby kilka lat. Tymczasem już obecnie jest zauważalna konieczność unifikacji prawa cyberprzestrzeni. Innym pomysłem byłoby przekształcenie istniejących struktur i ewolucja podjętych działań. Pod auspicjami ONZ działa Forum Zarządzania Internetem, które stanowi forum wymiany informacji i wielostronnego dialogu w przedmiocie najpilniejszych problemów związanych z przestrzenią cyfrową. Ogromną zaletą przyjętej formy spotkań jest zaproszenie do dyskusji wszystkich zainteresowanych podmiotów, w tym z sektora prywatnego. Bez wątpienia organizacja, która miałaby zająć się regulacją przestrzeni wirtualnej musiałaby brać pod uwagę opinię użytkowników sieci oraz podmiotów prywatnych, dzięki którym przecież wciąż są wprowadzane nowe rozwiązania technologiczne. Utworzenie IGF było pierwszym korkiem w celu powołania globalnego organu, który pomógłby wypracować podstawowe działania w cyberprzestrzeni.

Drugim pomysłem jest powołanie zupełnie nowej instytucji. Instytucja ta, by racjonalnie, optymalnie i całościowo regulować cyberprzestrzeń, winna być złożona nie tylko z przedstawicieli państw, ale również sektora prywatnego, znawców prawa, informatyków, użytkowników i innych podmiotów prywatnych. Instytucja do spraw cyberprzestrzeni powinna mieć prawo do tworzenia prawa cyberprzestrzeni na poziomie globalnym. W pierwszych latach działalności, wypracowanie pełnego konsensusu mogłoby być zadaniem trudnym, stąd też postulować należy przyznanie instytucji uprawnień do wydawania rezolucji, wytycznych czy wskazywania dobrych praktyk i rozwiązań. Tak jak w przypadku ustaw modelowych UNCITRAL wydawanie aktów niewiążących mogłoby być drogowskazem dla państw wytyczającą ścieżkę pożądanych zmian legislacyjnych w zakresie cyberprzestrzeni.

Prace instytucji do spraw cyberprzestrzeni powinny obejmować najważniejsze zagadnienia związane z przestrzenią wirtualną, czyli cyberprzestępczość, własność intelektualną, handel elektroniczny, dane osobowe czy cyberbezpieczeństwo. Oznacza to, że organizacja taka musiałaby mieć wszechstronne kompetencje. Stanąć należy na stanowisku, że jedynie szerokie ujęcie tematu pozwoli na efektywne i kompleksowe wprowadzanie zmian legislacyjnych. Co więcej, przyznanie szerokich kompetencji umożliwiłoby kompleksowe uregulowanie zagadnień i harmonizację norm na poziomie międzynarodowym, a nie wyłącznie regionalnym czy krajowym.

Struktura instytucji do spraw cyberprzestrzeni powinna mieć otwarty charakter, tak by móc zapewnić reprezentację wszystkich podmiotów międzynarodowych, przedstawicieli państw, społeczeństwa obywatelskiego oraz przedstawicieli sektora prywatnego (firm telekomunikacyjnych, producentów software i hardware i innych). Instytucja winna ściśle współpracować z innymi organizacjami międzyrządowymi i wszelkimi podmiotami, które mogą przyczynić się do adekwatności i innowacyjności wprowadzanych rozwiązań. Wyłącznie szeroko zakrojona współpraca międzynarodowa może doprowadzić do stworzenia odpowiednich ram prawnych uwzględniających poszczególne problemy przestrzeni wirtualnej, w tym identyfikację kluczowych problemów oraz skoordynowanie działań legislacyjnych. Organizacja do spraw cyberprzestrzeni powinna działać opierając się na przejrzystej demokratycznej strukturę, w której przedstawiciele poszczególnych podmiotów (państw, sektora prywatnego, sektora prywatnego) są należycie reprezentowani i uprawnieni do dyskusji (w przypadku podmiotów niepaństwowych).

W raporcie z 2015 roku *Working Group on Internet Governance* (WGIG), grupy roboczej zainicjowanej w trakcie Światowego Szczytu Społeczeństwa Informacyjnego (WSIS) w Genewie, zaproponowano cztery modele zarządzania Internetem, rozumianego jako opracowywanie i stosowanie przez rządy, sektor prywatny, społeczeństwo obywatelskie wspólnych zasad, norm, reguł, procedur i programów, które kształtują rozwój i wykorzystanie Internetu[1425]. Zaproponowany podział można również uznać za propozycję tworzenia prawa cyberprzestrzeni.

Model pierwszy zakłada powołanie Światowej Rady do spraw Internetu (ang. *Global Internet Council* - GIC), składającej się z przedstawicieli członków rządów reprezentujących wszystkie regiony świata oraz inne zainteresowane strony. Funkcje GIC miałyby obejmować

[1425] Report of the Working Group on Internet Governance, lipiec 2005, s. 4.

między innymi opracowanie międzynarodowej polityki dotyczącej najważniejszych spraw związanych z siecią (cyberbezpieczeństwo, prywatność, cyberprzestępczość), nadzór nad sposobem zarządzania Internetem, ułatwianie negocjacji traktatów, konwencji i porozumień dotyczących kluczowych zagadnień oraz stworzenie zasad i mechanizmów rozwiązywania sporów i postępowania arbitrażowego. Zgodnie z tym modelem Światowa Rada do spraw Internetu podlegałaby Organizacji Narodów Zjednoczonych, a sektor prywatny i społeczny miałby sprawować funkcje doradcze[1426]. Model drugi zakłada, że utrzymanie *status quo,* bez konieczności powoływania specjalnej organizacji. Propozycja ta opiera się na wzmocnieniu roli władz państwowych w ICANN, tak by forum to oparte na zasadach równości wszystkich uczestników, mogłoby stanowić przestrzeń do negocjacji kwestii związanych z zarządzaniem Internetem. Według trzeciego modelu żaden pojedynczy rząd nie może sprawować kontroli nad międzynarodowym zarządzaniem Internetem. Uznano, że funkcję tę mogłaby pełnić Międzynarodowa Rada do spraw Internetu (ang. *International Internet Council* - IIC), która pełniłaby wiodącą rolę w zarządzaniu Internetem, a sektor prywatny i społeczny pełniłby rolę doradczą. Czwarty model zakłada powołanie oddolnych struktur, które wspólnie miałyby kształtować funkcje Internetu w zakresie polityki zarządzania, nadzoru oraz technicznej koordynacji elektronicznych zasobów.

W raporcie pojawia się propozycja powołania Światowej Rady Polityki Internetu (ang. *The Global Internet Policy Council* - GIPC), która byłaby odpowiedzialna za kwestie związane z polityką społeczną i implementacją oraz perspektywach standardów technicznych. Mechanizm kierowany przez rządy mógłby badać zagadnienia podnoszone przez istniejące organizacje międzynarodowe, które nie są przedmiotem głębszej międzynarodowej debaty. Partnerem w rozmowach byłby sektor prywatny oraz społeczeństwo obywatelskie[1427].

Joanna Kulesza stoi na stanowisku, że pierwszy zaproponowany model i poddanie GIC pod auspicje ONZ jest rozwiązaniem niewłaściwym, zwłaszcza w kontekście silnego powiązania organu z władzami państwowymi. Naraża to na duże prawdopodobieństwo wystąpienia sporu związanego z różnymi interesami państwowymi. Autorka pozytywnie wyraża się o drugim modelu, przyjmując, że wzmocnienie istniejącej struktury jest rozwiązaniem niezwykle praktycznym, choć trudnym do wdrożenia. Jednakże to trzeci model w najpełniejszy sposób realizuje postulaty formułowane wobec międzynarodowej organizacji nadzorującej Internet. Z kolei ostatni model należy według Joanny Kuleszy odrzucić, jako

[1426] Ibidem, s. 13.
[1427] Ibidem, s. 14-15.

zbyt skomplikowaną strukturę organizacyjną z występowaniem władz państwowych o sprzecznych interesach na każdym szczeblu[1428]. Pamiętać jednak należy, iż rozważania Joanny Kuleszy dotyczyły problemu zarządzania Internetem, w szczególności w kontekście działalności organizacji ICANN. Tymczasem rozpatrywany w tym miejscu podmiotowy aspekt nowego ładu cyberprzestrzeni jest znacznie szerszy - obejmuje cyberprzestrzeń jako nową, tworzącą się gałąź prawa międzynarodowego mieszczącą w sobie niezwykle szeroki aspekt działalności człowieka w cyberprzestrzeni - od jurysdykcji, prawa karnego, cywilnego, praw człowieka czy prawa własności intelektualnej. Dlatego nie należy odrzucać pomysłu powołania zupełnie nowej instytucji czy też organizacji międzynarodowej działającej w strukturach ONZ. Wręcz przeciwnie pomysł ten wydaje się być zasadny. Jako zalążek organizacji powołanej do wypracowania odpowiednich norm w cyberprzestrzeni można by uznać Forum Zarządzania Internetem, jednakże w obecnej formie stanowi ono jedynie miejsce wymiany poglądów.

Odrzucić należy pomysł powołania organizacji, która nie dopuściłaby do głosu sektora prywatnego oraz społeczeństwa obywatelskiego. To właśnie internauci w znacznym stopniu współtworzą cyberprzestrzeń, dlatego też nie można pominąć ich w dyskusji. Joanna Kulesza podkreśla wagę społeczności internetowej. Wyraża ona pogląd, że „ważne jest więc, aby także przedstawiciele cyberspołeczności mogli zabrać głos podczas szkicowania ramowej konwencji internetu. To właśnie na podstawie ich doświadczeń w zakresie samoregulacji i poszukiwania konsensusu możliwe byłoby odnalezienie drogi do polubownego rozwiązania istniejących sporów. Jeśli uda się wypracować międzynarodowe porozumienie dotyczące kwestii prawnych, okazać się ono może bezskuteczne, jeśli nie będzie oparte o zgodę samych rządzonych. Natomiast jeśli konsensus oparty zostanie na istniejących już zrębach *ius internet* - prawa cyberspołeczności - to szansa na jego skuteczne wdrożenie będzie duża. Zważywszy, że podstawą działania społeczności w cyberprzestrzeni jest odwołanie do wspólnych wartości etycznych, to właśnie podstawy moralne, jednoczące wszystkie kultury, powinny stanowić punkt wyjściowy dyskusji nad kształtem regulacji sieci globalnej”[1429].

Należy również zadać sobie pytania, kto rozstrzygałby spory mogące zaistnieć w przestrzeni cyfrowej oraz czy należy powołać sąd międzynarodowy do spraw cyberprzestrzeni. Na chwilę obecną sądy międzynarodowe takie, jak Europejski Trybunał Praw Człowieka, Międzynarodowy Trybunał Sprawiedliwości, Europejski Trybunał

[1428] J. Kulesza, *Ius internet. Między prawem a etyką*, Warszawa 2010, s. 244-246.
[1429] Ibidem, s. 267.

Sprawiedliwości oraz sądy arbitrażowe są wystarczające do rozstrzygania sporów prawnych w cyberprzestrzeni. Sądy te wydają wyroki w sprawach dotyczących cyberprzestrzeni, działając opierając się na jasnych, przejrzystych procedurach oraz zasadach działania. Sędziowie orzekający swoją wiedzą oraz doświadczeniem gwarantują gruntowne i sprawiedliwe rozstrzyganie sporów, a także wskazują kierunki rozwoju prawa cyberprzestrzeni. Nie mniej jednak w niedalekiej przyszłości pojawiać się będzie potrzeba stworzenia międzynarodowego sądu do spraw cyberprzestrzeni. Stanowisko to zdeterminowane jest kilkoma czynnikami. Termin rozpoznania sporów przed MTS, ETPC czy ETS jest bardzo długi. Można również przewidywać, iż liczba sporów prawnych związanych z działalnością człowieka w cyberprzestrzeni będzie lawinowo rosła. Zasadnym jest zatem powołanie międzynarodowego sądu, którego sędziowie będą rozumieli specyfikę cyberprzestrzeni i stosowanego w niej prawa. Ogromną rolę mogą również odegrać (zwłaszcza w stosunkach handlowych) sądy arbitrażowe, które (podobnie jak ICCAN w odniesieniu do sporów domenowych) mogą tworzyć kodeksy dobrych praktyk czy wskazywać pożądane kierunki rozwoju za pomocą precedensów.

Bezsprzecznie należy podkreślić wartość orzecznictwa w kształtowaniu się prawa w tytułowej dziedzinie. Sądy międzynarodowe i arbitrażowe działają opierając się na prawie i zwyczaju międzynarodowym oraz ogólnych zasadach prawa (na przykład *pacta sunt servanda* czy też *rebus sic stantibus*). Normy te znajdą zastosowanie również w odniesieniu do przestrzeni wirtualnej. Tam, gdzie nie ma odpowiednich norm międzynarodowych sądy są w stanie „wypełnić lukę" legislacyjną, tworząc niejako drogowskaz wskazujący pożądaną praktykę państwową. Również sądy arbitrażowe mogą przyczynić się do tworzenia się międzynarodowego prawa cyberprzestrzeni przez tworzenie na swój użytek przedmiotowych kodeksów dobrych praktyk. Z kolei zupełnie oddolną metodą regulacji cyberprzestrzeni jest kreowanie i posługiwanie się wzorami umów, które kształtują powszechnie akceptowalne normy postępowania w elektronicznych stosunkach handlowych. Niemniej istotny wpływ odgrywają regulaminy wielkich międzynarodowych przedsiębiorstw takich, jak Facebook, Amazon czy Twitter.

6.2.3. Aspekt przedmiotowy nowego ładu cyberprzestrzeni

Niezbędna jest przyjęcie międzynarodowego porozumienia ustalającego wspólne normy, prawa i definicje dotyczące cyberprzestrzeni. W doktrynie podnosi się, że jednym z podstawowych problemów prawnych w przestrzeni cyfrowej jest ustalenie właściwej jurysdykcji (sądowniczej, ustawodawczej oraz wykonawczej). Joanna Kulesza stoi na stanowisku, że „problemy dotyczące jurysdykcji w Internecie pojawiają się wtedy, kiedy spory dotyczą elementu pozaterytorialnego (np. osób z różnych państw lub transakcji międzynarodowych). Jako że wszystkie treści internetowe mogą być odbierane na całym świecie, każdy użytkownik Internetu może potencjalnie stać się podmiotem każdej z jurysdykcji państwowych. Umieszczając treści w sieci globalnej trudno jest z góry przewidzieć, które prawa krajowe, i czy jakiekolwiek w ogóle zostaną naruszone. W tym kontekście prawie każde działanie podejmowane w Internecie posiada aspekt międzynarodowy, który może prowadzić do konfliktu jurysdykcyjnego. Stosowanie w sprawach »internetowych« analogii i przepisów prawa »pozainternetowego« prowadzi do daleko idących problemów, które ograniczają możliwość ich stosowania”[1430]. Wobec braku fizycznych granic, transnarodowości i transgraniczności przestrzeń wirtualna musi być regulowana na poziomie globalnym. Wprowadzanie wyłącznie regionalnych, a tym bardziej krajowych przepisów dotyczących jurysdykcji w cyberprzestrzeni jest nieefektywne i wprowadza niepewność prawną, ponieważ użytkownik sieci nie ma pewności, czy czynności przez niego dokonywane nie stanowią na przykład występku w innym regionie świata.

Szczególnie pilna jest potrzeba ujednolicenia norm i kodyfikacji w zakresie ogólnie pojętej cyberprzestępczości. Ogromną rolę w unifikacji przepisów dotyczących działań przestępczych w przestrzeni wirtualnej odegrała Konwencja Rady Europy o cyberprzestępczości. Nie wszystkie jednak państwa zdecydowały się na związanie się powyższą umową międzynarodową, mimo że jest to powszechnie zalecane i mogłoby doprowadzić do globalnej harmonizacji przepisów w zakresie cyberprzestępczości. Dotychczasowa częściowa harmonizacja przepisów dotyczących przestępczości w przestrzeni wirtualnej nie oznacza, że cel ostateczny został osiągnięty. Wręcz przeciwnie. Dynamiczny rozwój nowych technologii, występowanie nowych urządzeń (drony, tablety, smartfony),

[1430] J. Kulesza, *Międzynarodowe…*, s. 179.

programów i aplikacji powoduje, że cyberprzestępcy wciąż wykorzystują nowe, innowacyjne, przestępcze metody działania, nierzadko wyprzedzając organy ścigania posługując się zaawansowanym technologicznie sprzętem i umiejętnościami.

Międzynarodowa współpraca winna obejmować przeciwdziałanie, zwalczanie oraz wymianę doświadczeń w zakresie cyberprzestępczości. Szczególną uwagę należy zwrócić na brak jednolitych przepisów normujących problem pornografii dziecięcej w cyberprzestrzeni oraz wykorzystania przestrzeni cyfrowej przez terrorystów. Walka z drugim z wymienionych problemów winna stać się priorytetem współpracy państw. Świat jest narażony na coraz większą liczbę ataków terrorystycznych. Cyberprzestrzeń jest wykorzystana przez terrorystów w wielorakich celach: rekrutowania nowych członków, zbierania funduszy, komunikacji czy przez typowe cyberataki na infrastrukturę krytyczną państwa. Konieczne jest wprowadzenie jednolitych międzynarodowych standardów obejmujących tożsame definicje i zasady działania, aby walka z terroryzmem czy pedofilią była skuteczna. Tylko stworzenie efektywnego systemu koordynacji i wymiany doświadczeń oraz informacji pozwoli na skuteczne zwalczanie cyberprzestępczości w sieci.

Ważnym problem jest również ustalenie, co może być uznane za naruszenie art. 5 Traktatu Północnoatlantyckiego. Omawiany przepis stanowi, że zbrojna napaść na jedną lub więcej stron NATO będzie uznana za napaść na wszystkich członków Sojuszu. Należy zatem postawić pytanie, co na arenie międzynarodowej powinno być uznane za cybernapaść na inne państwo[1431]. Czy działaniem takim będzie cyberatak na najważniejszą infrastrukturę państwową, atak na systemy komputerowe elektrowni atomowych, banków krajowych czy też jedynie zakłócenie prawidłowego działania rządowych stron internetowych? W przypadku ataku lądowego, powietrznego czy morskiego można wyodrębnić chwilę wystąpienia takiego działania, która fizycznie wywołuje określone skutki. W przypadku cyberataku można przez dłuższy czas nie zorientować się, iż doszło na przykład do przełamania zabezpieczeń i kradzieży danych bądź do zainfekowania systemu.

Kolejnym zagadnieniem nasuwającym pytanie jest, kto i w jaki sposób będzie dokonywał oceny poważności cyberataku na państwo. Wydaje się, że jedynie ataki, które pociągają za sobą poważne konsekwencje i śmierć ludności cywilnej mogą być uznane za naruszenie art. 5 Traktatu Północnoatlantyckiego. Ponadto, należy rozróżnić zwykłe ataki

[1431] Kwestię cybernapaści można rozpatrywać w konktekście agresji zbrojnej. Więcej na temat ram definicyjnych zbrodni agresji w: E. Karska, *Dorobek Konferencji Rewizyjnej Statutu MTK ze szczególnym uwzględnieniem poprawki definiującej zbrodnię agresji*, „Kwartalnik Prawa Publicznego" 2010, nr 10/3.

hackerskie od działań terrorystów, cyberprzestępców, od ataków innych państw. Wciąż nie zostało jednoznacznie sprecyzowane, jaką formę winny przybrać akcje wojskowe w obcej przestrzeni wirtualnej. Jeszcze większy problem powstaje przy próbie przypisania odpowiedzialności prawnej za atak w cyberprzestrzeni. Ustalenie prawa atrybucji w cyberprzestrzeni może okazać się nierozwiązywalnym problemem. Trudno będzie wypracować międzynarodowe przepisy regulujące te kwestie, ponieważ żadne z państw nie zgodzi się na ponoszenie odpowiedzialności za działania hakerów, znajdujących się na ich terytorium. Równocześnie państwa nie chcą przyznać się, że atak został przeprowadzony na zlecenie ich władz rządowych. Przypisanie odpowiedzialności może okazać się niezwykle trudne między innymi z powodu otwartej architektury sieci, łatwości penetracji oraz znacznego stopnia anonimowości. Ataki mogą odbywać się z kilku miejsc na świecie, co jeszcze bardziej utrudnia ustalenie podmiotu odpowiedzialnego.

Odnosząc się do zagadnień cywilnoprawnych w cyberprzestrzeni, to wydaje się, że pojawienie się nowej przestrzeni działalności człowieka nie doprowadziło do wykształcenia się zupełnie nowego, niezależnego prawa zobowiązań w przestrzeni wirtualnej. Obowiązujące przepisy zostały odpowiednio zastosowane w cyberprzestrzeni. Strony, tak jak w klasycznych stosunkach handlowych, mogą dowolnie kształtować swoje relacje, wybierać kontrahentów oraz kształtować umownie *essentialia negotii*. Realnym problemem jest jedynie kwestia ustalenia jurysdykcji w przypadku nieprawidłowego wykonania umowy. By uniknąć konfliktów jurysdykcyjnych, zaleca się zawieranie w umowie klauzuli jurysdykcyjnej wskazującej prawo właściwe w przypadku wystąpienia sporu. Nie ma zatem potrzeby tworzenia zupełnie nowego prawa zobowiązań odnoszącego się tylko i wyłącznie do umów zawieranych w cyberprzestrzeni. Można jednak rozważyć wprowadzenie jednego, holistycznego aktu prawego regulującego kwestię jurysdykcji, miejsca zawarcia i wykonania umowy, siedzib handlowych oraz innych najistotniejszych kwestii związanych z handlem elektronicznym.

Równie ważnym zagadnieniem jest rozstrzygnięcie problemu walut wirtualnych takich, jak bitcoin. Status ich do tej pory nie został uregulowany. Waluty wirtualne stają się coraz popularniejsze w obrocie handlowym, a część sklepów akceptuje je jako formę zapłaty. Niestety, coraz częściej waluty te, wobec braku odgórnej regulacji, są wykorzystywane przez organizacje przestępcze oraz terrorystów. Brak niezależnego organu nadzoru powoduje, iż kursy walut bitcoinów są niestabilne (na początku marca 2017 roku cena bitcoinów przebiła

cenę uncji złota, by zaledwie po kilkunastu dniach stracić około 20% na skutek wewnętrznego konfliktu twórców i zarządzających rynkiem bitcoina)[1432].

Innym problemem praktycznym jest wolność słowa w przestrzeni wirtualnej. Na gruncie europejskim jest ona rozumiana diametralnie inaczej niż na amerykańskim. Przeciwstawne trendy regionalne obserwowane są również w takich kwestiach, jak moralność, wolność ekspresji i wypowiedzi artystycznej. Kolejną postulowaną zmianą legislacyjną jest opracowanie jednego, holistycznego aktu prawnego o randze międzynarodowej normującego kwestię własności intelektualnej w cyberprzestrzeni. To właśnie rozwój przestrzeni wirtualnej doprowadził do lawinowego wzrostu naruszeń praw autorskich i innych praw własności intelektualnej. Piractwo komputerowe dotyka praw twórców na całym świecie, ponieważ za pomocą jednego (symbolicznego) kliknięcia myszki można nielegalnie wejść w posiadanie muzyki i filmów, nielegalnie kopiować je i udostępniać innym osobom. Należy gruntownie rozważyć możliwe kierunki zmian legislacyjnych, które mogą wyrazić się przez zaostrzenie kar dla użytkowników sieci bądź przez przyjęcie zupełnie nowego, innowacyjnego rozwiązania, które w sposób bardziej optymalny będzie chronić twórców na przykład przez wprowadzenie nowych form licencji.

Niewątpliwie jednym z istotniejszych zagadnień jest kwestia bezpieczeństwa w cyberprzestrzeni. Realny jest problem wystąpienia ponadnarodowego, międzynarodowego cyber konfliktu w przestrzeni wirtualnej. Konflikt taki może przybrać postać aktywizmu, haktywizmu bądź cyberterroryzmu[1433]. Cyberbezpieczeństwo powinno być budowane na wielu płaszczyznach: międzynarodowej, regionalnej, krajowej oraz sektorowej. Ogromną rolę w tym zakresie będą odgrywać kwestie techniczne. Należy zgodzić się z poglądem, że „zapewnienie bezpieczeństwa w cyberprzestrzeni nie będzie możliwe bez rozbudowy systemów wczesnego ostrzegania przed atakami, wdrożenia dodatkowych rozwiązań prewencyjnych i szczególnej ochrony kluczowych systemów teleinformatycznych, połączonej z ćwiczeniami pozwalającymi ocenić odporność tej infrastruktury na ataki cybernetyczne”[1434]. Zbudowanie cyberbezpieczeństwa regionu, państwa czy organizacji jest niemożliwe bez odpowiedniej współpracy z sektorem prywatnym. To właśnie dzięki przedsiębiorstwom prywatnym tworzącym *hardware* i *software* architektura cyberprzestrzeni ma swój dzisiejszy

[1432] Dane z witryny Buisness Insider Polska, http://businessinsider.com.pl/finanse/kryptowaluty/bitcoin-kurs-i-sytuacja-marzec-2017/j76bf41 [20.03.2017].
[1433] T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 15(8), s. 15.
[1434] M. Grzelak, K. Lidel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski - zarys problemu*, „Bezpieczeństwo Narodowe” 2012, nr 22, s. 137.

kształt. Oprogramowanie, sprzęty i rozwiązania systemowe w dużej części pochodzą właśnie z sektora prywatnego. Firmy takie jak Google, Facebook, Microsoft czy Apple są w posiadaniu ogromnych ilości danych, które mogą mieć kluczowe znaczenie dla bezpieczeństwa państwa. Z tych też względów budowanie bezpieczeństwa cyberprzestrzeni nie może odbyć się bez partnerstwa publiczno-prywatnego (szczególnie w obszarze infrastruktury krytycznej w zakresie współpracy z prywatnymi firmami z branży energetycznej, paliwowej, powietrznej, finansowej) oraz ścisłej współpracy z podmiotami prywatnymi.

Zidentyfikowanie obszarów cyberprzestrzeni, które potrzebują międzynarodowej regulacji jest zadaniem stosunkowo prostym. Prawdziwym wyzwaniem legislacyjnym jest jednak dostosowanie obowiązujących obecnie przepisów do potrzeb społeczeństwa informacyjnego, wybór prawa właściwego oraz skuteczność egzekucji tych przepisów. Niejednokrotnie problemem może okazać się różnorodność tradycji prawnych i brak wspólnych definicji najważniejszych terminów[1435].

Stworzenie globalnych norm prawnych możne nastręczyć wiele problemów między innymi ze względu na różny stopień zaawansowania (w szczególności technologicznego) państw, różną kulturę prawa i sprzeczne interesy polityczne poszczególnych krajów. Podstawowym jednak czynnikiem jest brak organu, pod auspicjami którego można by prowadzić rozmowy na wskazane wyżej tematy. Podmioty tworzące międzynarodowe prawo cyberprzestrzeni muszą uwzględniać specyficzny charakter przestrzeni wirtualnej, jej dynamiczność, aterytorialność oraz ponadnarodowość. Ponadto, normy prawa tworzone dla przestrzeni cyfrowej muszą być elastyczne i tworzone przy uwzględnieniu zasady neutralności technologicznej.

6.2.4. Aspekt proceduralny nowego ładu cyberprzestrzeni

Cyberprzestrzeń mimo swojego ponadnarodowego, wirtualnego i transgranicznego charakteru nie może być „krainą" bezprawia. Powstanie odpowiednich międzynarodowych

[1435]F. Cłapka, op. cit., s. 477.

norm i procedur jest procesem stopniowym. Należy wykorzystywać już istniejące instytucje i procedury oraz posiłkować się dotychczasowymi doświadczeniami w zakresie regulacji przestrzeni wirtualnej. Bez wątpienia nie będzie to proces prosty do realizacji. Optymalnym rozwiązaniem byłoby wykorzystanie istniejących norm i zasad prawa międzynarodowego, jednakże należy również wspomagać się instrumentami politycznymi. Tylko wówczas możliwe będzie wypracowanie konsensusu akceptowalnego przez wszystkie strony.

W latach osiemdziesiątych XX wieku narodził się problem występujących na coraz większą skalę zmian klimatycznych. Wówczas pierwszym krokiem do późniejszej regulacji było ustalenie, że problem ten istnieje i konieczne jest ustalenie jego rozmiaru, a następnie opracowanie zasad, które winny być zastosowane. Prace prowadzone na arenie międzynarodowej doprowadziły wówczas do uznania, że jest on globalny, wobec czego reżim prawny musi być oparty na prawie międzynarodowym. Stwierdzono, że osiągnięcie konsensusu wymaganego umową międzynarodową byłoby szczególnie czasochłonne. Z tych też względów zdecydowano się na wprowadzenie konwencji ramowej, która wskazywałaby zasady, normy i procedury ułatwiające bardziej szczegółowe dalsze negocjacje. W wyniku prac w 1992 roku przyjęto Konwencję Ramową Narodów Zjednoczonych o Zmianach Klimatycznych[1436], która regulowała najbardziej podstawowe kwestie dotyczące zmian klimatu[1437]. Co do zasady brak powszechnych norm, zasad i procedur istnieje również w przestrzeni wirtualnej. Uznano zatem, że istnieje potrzeba stworzenia regulacji na wzór Konwencji NZ o Zmianach Klimatycznych, która byłaby podstawą do dalszych negocjacji nad przestrzenią cyfrową.

Wskazana wyżej koncepcja zasługuje zasadniczo na aprobatę. Nie jest możliwe natychmiastowe stworzenie ogólnie akceptowalnych norm prawnych regulujących działalność człowieka w cyberprzestrzeni. Wypracowanie jednak pewnego zestawu reguł czy też zasad, na których będą opierać się państwa może przyczynić się do powstania rozwiązań *de lege ferenda*. Wydaje się, że najbardziej odpowiednią formą do dyskusji nad rozwiązaniami prawnymi będzie organizacja międzynarodowa bądź forum skupiające zainteresowane państwa.

[1436] Dz.U. z 1996 r., Nr 53, poz. 238.
[1437] J. Kulesza, *Międzynarodowe…*, s. 337.

Internet Governance Project (niezależna grupa amerykańskich badaczy[1438]) wyszedł z ciekawą inicjatywą opracowania Ramowej Konwencji Narodów Zjednoczonych w zakresie Zarządzania Internetem. Zgodnie z założeniami, konwencja ramowa powinna:

- definiować, na czym polega problem zarządzania Internetem i jakie są jego granice; powinny się tam zawrzeć kluczowe definicje zagadnień związanych z zarządzaniem przestrzenią cyfrową, w tym definicja Internetu oraz wskazanie podmiotów uprawnionych do zarządzania cyberprzestrzenią; w ocenie Joanny Kuleszy punktem wyjścia do tych rozważań powinna być zasada subsydiarności, w której zaleca się stosowanie rozwiązań międzynarodowych jedynie wówczas, gdy są one najefektywniejsze,
- ustanawiać normy zarządzania Internetem; postulowane jest zachowanie elementów takich, jak otwartość i wolność cyberprzestrzeni jako medium komunikacji oraz zapewnienie nieograniczonego, powszechnego dostępu, niezbędne jest również wskazanie w konwencji ramowej obszarów, które powinny być uregulowane oraz dopuszczenie do dyskusji sektora prywatnego, który odegrał kluczową rolę w rozwoju i zarządzaniu przestrzenią cyfrową,
- ustanawiać zasady, na podstawie jakich będą prowadzone dalsze negocjacje, kolejne porozumienia mogłyby zostać dołączone do konwencji w formie protokołów dodatkowych,
- konwencja powinna przyznawać państwom - stronom, możliwość działania jako „nadzorcy" w określonych, konkretnych zagadnieniach stanowiących sedno zarządzania przestrzenią cyfrową; postuluje się również, by państwa przyznały część z omawianych uprawień organizacjom społeczeństwa obywatelskiego[1439].

Twórcy propozycji utworzenia konwencji ramowej w sprawie cyberprzestrzeni oparli swe założenia na analogii do Ramowej Konwencji NZ w sprawie zmian klimatu, podnosząc następujące podobieństwa pomiędzy tymi dwoma obszarami: zaangażowanie wielu podmiotów, w tym organizacji pozarządowych, konieczność zawarcia porozumienia w sprawie zasad i norm, konieczność ustanowienia procedur postępowania w zakresie przyszłych, możliwych do podniesienia problemów[1440]. Zgodnie z założeniami ramowa

[1438] J. Kulesza, *Projekt Ramowej Konwencji Internetu*, „Państwo i Prawo" 2009, z. 10, s. 15.
[1439] J. Kulesza, *Międzynarodowe…*, s. 338.
[1440] J.M. Bauer, *Internet Governance: Theory and First Principles*, artykuł dostępny *on-line*: https://www.researchgate.net/profile/Johannes_Bauer3/publication/228800513_Internet_Governance_Theory_and_First_Principles/links/09e4150fee13f84c8a000000.pdf [10.03.2017].

konwencja dotycząca cyberprzestrzeni powinna zawierać kluczowe definicje oraz reguły zarządzania przestrzenią cyfrową. Postuluje się, by utrzymać wolnościowy charakter przestrzeni wirtualnej, gwarantującej powszechny i nieograniczony dostęp, jednakże z wyjątkami, do których należy zaliczyć cybernetyczne nadużycia takie, jak chociażby pornografia dziecięca czy cyberterroryzm. Ponadto, konwencja ramowa winna wskazywać, które z problemowych obszarów wymagają dalszych prac i ściślejszej regulacji. Pożądanym byłoby również wskazanie zasad i mechanizmów, na podstawie których wprowadzane byłyby dalsze regulacje[1441]. Oczywiste jest, że przyjęcie zasad i norm postępowania w cyberprzestrzeni - ze względu na różnorodne interesy państw nie będzie procesem prostym. Okazać się może, że różne rejony globu będą wymagać przyjęcia innych rozwiązań, co jest spowodowane chociażby innym stopniem rozwoju[1442].

Propozycja wprowadzenia nowego schematu zarządzania Internetem została zaproponowana przez Grupę Roboczą ONZ do spraw Zarządzania Internetem (ang. Working Group on Internet Governance - WGIG) w raporcie z 2005 roku[1443]. Stwierdzono w nim, że zarządzanie Internetem to nie tylko nadawanie domen, adresów, którymi zajmuje się ICANN. Zarządzenie cyberprzestrzenią według WGIG opiera się na czterech kluczowych obszarach:

1. Kwestiach związanych z infrastrukturą oraz zarządzaniem krytycznymi zasobami w Internecie, włączając w to system nadawania domen oraz adresów www, standardy techniczne, sieci telekomunikacyjne. Zagadnienia te są bezpośrednio związane z zarządzaniem Internetem i wchodzą w zakres działalności wyspecjalizowanych w tej dziedzinie, istniejących już organizacji.
2. Kwestiach związanych z użyciem Internetu, włączając w to spam, bezpieczeństwo sieci oraz cyberprzestępczość. Problemy te są bezpośrednio związane z zarządzeniem Internetem, jednakże globalne zasady kooperacji w tej dziedzinie nie są dobrze zdefiniowane.
3. Kwestiach, które są związane z cyberprzestrzenią, ale mają o wiele większy zasięg na przykład własność intelektualna czy handel międzynarodowy.

[1441] J. Kulesza, *Ius…*, s. 238-239.
[1442] Eadem, *Międzynarodowe…*, s. 338.
[1443] *Report of the Working Group on Internet Governance. Château de Bossey June 2005*, raport dostępny na stronie: http://www.wgig.org/docs/WGIGREPORT.pdf [25.08.2015].

4. Kwestiach odnoszących się do rozwojowych aspektów zarządzania Internetem, w szczególności, w zakresie budowania potencjału w krajach rozwijających się[1444].

Wobec braku wielostronnych umów międzynarodowych czy organizacji międzynarodowej (która unifikowałaby prawo cyberprzestrzeni) prawo międzynarodowe musi posiłkować się istniejącymi normami i zasadami. W przestrzeni wirtualnej, tak jak w innych obszarach prawa, znajdą zastosowanie ogólne zasady prawa, zwyczaje międzynarodowe oraz pomocniczo judykatura i poglądy doktryny. Szczególną rolę w kształtowaniu się prawa cyberprzestrzeni może odegrać *soft law*. Stworzenie norm o charakterze pozytywnym jest przede wszystkim czasochłonne ze względu na trudność w osiągnięciu konsensu oraz odmienną politykę i interesy państw. Stanowienie norm prawa miękkiego czy to w postaci zaleceń, rekomendacji, rezolucji, czy ustaw modelowych może być podwaliną pod stworzenie norm o charakterze traktatowym. Ponadto, są one drogowskazem pożądanego kierunku zmian legislacyjnych i mogą, wbrew pozorom, przyczynić się do przynajmniej częściowej harmonizacji przepisów. Zgodna praktyka podmiotów prawa międzynarodowego w jakimś obszarze może z kolei przyczynić się do powstania normy zwyczajowej dotyczącej cyberprzestrzeni. Zwyczajem, który być może wykształci się w przyszłości jest na przykład zasada wolności i niezawłaszczalności cyberprzestrzeni.

Pamiętać należy, że cyberprzestrzeń wykształciła pewne oddolne, nieformalne zasady zwane netykietą (ang. *netiquette*) pochodzące od słów sieć (ang. *net*) oraz etykieta (ang. *etiquette*). Netykieta jest zbiorem zasad, dobrych praktyk i norm obowiązujących internautów w cyberprzestrzeni. Zasady te mają charakter luźnych zaleceń i dobrych zwyczajów określanych niekiedy mianem cyfrowego *savoir-vivre'u*. Użytkownicy sieci starają się przestrzegać netykiety, a osoby które postępują wbrew przyjętym, cyfrowym normom spotyka kara na przykład zakaz publikowania komentarzy, skreślenie z listy subskrybentów, poinformowanie administratora, skasowanie lub zablokowanie konta[1445]. Za działania niepożądane mogą być uznane: umieszczanie obraźliwych, wulgarnych komentarzy, udostępnianie nielegalnych treści, przesyłanie spamu czy też inne formy zachowań. W serwisie Webmaster.net.pl zamieszczono „Dziesięć przykazań etyki komputerowej" -

[1444] *Report of the Working Group on Internet Governance. Château de Bossey June 2005,* pkt. 13.
[1445] R. Chmura, *Kodeks Internetu*, [w:] R. Skubisz (red.) *Internet 2000 prawo - ekonomia- kultura*, Lublin 2000, s. 460.

jednolitych wskazówek postępowania dla wszystkich internautów. W dekalogu netykiety znalazły się następujące „przykazania":

1. Nie będziesz używał komputera aby szkodzić innym.
2. Nie zakłócaj pracy na komputerach innym.
3. Nie zaglądaj bez pozwolenia do cudzych plików.
4. Nie będziesz używał komputera aby kraść.
5. Nie będziesz używał komputera do dawania fałszywego świadectwa.
6. Nie będziesz używać ani kopiować programów, za które nie zapłaciłeś.
7. Nie będziesz używał zasobów cudzych komputerów bez zezwolenia (autoryzacji).
8. Nie będziesz przywłaszczał sobie wysiłku intelektualnego innych.
9. Będziesz myślał o społecznych konsekwencjach programu, który piszesz.
10. Będziesz używał komputera z rozwagą i ostrożnością[1446].

Część z zaprezentowanych wyżej zasad, znajduje potwierdzenie w prawie. Katalog netykiety jest obszerny i zróżnicowany, obejmuje zarówno normy o znaczeniu podstawowym, jak i te wzywające do poszanowania prawa (między innymi prawa autorskiego, prywatności innych użytkowników), które znajdują odzwierciedlenie w prawie pozytywnym, za naruszenie których ustawodawca przewidział odpowiednie sankcje[1447]. Inne reguły odnoszą się jedynie do zasad etycznych, niesankcjonowanych przepisami prawa (kurtuazja internetowa, przestrzeganie reguł redakcyjnych, ortograficznych, technicznych, dbałość o sprzęt). W przeszłości, gdy liczba internautów nie była znaczna, użytkownicy wewnątrz własnej struktury naciskali na przestrzeganie zasad netykiety. Obecnie, przy coraz większej liczbie użytkowników, niestety tracą na wartości.

Konkluzją powyższych rozważań może być stwierdzenie, że „porządek cyberprzestrzeni składa się w połowie z norm o charakterze prawnym i w takiej samej części z norm czysto etycznych. Te ostatnie tworzone są i sankcjonowane przez same cyberspołeczności, w ramach wypracowanych przez nie struktur i mechanizmów. Tworzą one oddolnie wypracowany, zwyczajowy, quasi-prawny porządek cyberprzestrzeni, który nazwać można *ius internet*, czerpiąc z rzymskiego źródłosłowania, gdzie pojęcie *ius gentium* służyło do określenia rodzącego się prawa międzynarodowego, opisywanego pierwotnie terminem prawo narodów. W dogmatyce prawa *ius* i *lex* są sobie przeciwstawiane. Pojęcie *ius* oznacza

[1446] Dane z portalu Webmaster: http://webmaster.net.pl/informacje/netykieta.php [10.01.2017].
[1447] J. Kulesza, *Ius…*, s. 38.

reguły zwyczajowe, przestrzegane z woli samych rządzonych, *lex* zaś to prawo »twarde«, stanowione przez suwerena do władania nad poddanymi. Wobec braku faktycznej i skutecznej władzy krajowych aparatów nad cyberprzestrzenią jesteśmy świadkami unikatowej jakości powstania prawa »cyber - narodów« w obszarach tworzonych przez nie cyberspołeczności”[1448]. Brak twardych reguł prawa powoduje, iż społeczności internetowe oddolnie wypracowują normy postępowania w przestrzeni wirtualnej. Wolnościowy, elastyczny i płynny charakter cyberprzestrzeni powoduje, iż łatwiej wprowadzać w nim *soft law* niż twarde reguły i sankcje. Wypracowanie międzynarodowego konsensusu skutkującego opracowaniem wielostronnej umowy międzynarodowej jest procesem trudnym i pracochłonnym. Łatwiej zatem reagować na szybko zmieniające się warunki technologiczne oddolnymi inicjatywami, rezolucjami i zaleceniami.

Cyberprzestrzeń jest miejscem, w którym czyha wiele zagrożeń związanych między innymi z dużym stopniem anonimowości. W przypadku wystąpienia naruszenia, często nie wiadomo, kim jest osoba po drugiej stronie komputera. W nieznacznej części portali posługujemy się własnym imieniem i nazwiskiem, w części ukrywamy się pod wirtualnym loginem, jednakże w większości przypadków surfujemy przez cyberprzestrzeń jako zupełnie anonimowe podmioty. Anonimowość wpływa na poczucie bezkarności. W cyberprzestrzeni nie widzimy realnego człowieka, lecz wyłącznie login. Nie zastanawiamy się nad konsekwencjami naszych wypowiedzi, nie przewidujemy, iż możemy ponieść odpowiedzialność karną za nasze niezgodne z prawem czyny. Rozwiązaniem mogłoby być przyjęcie obowiązkowych procedur identyfikacyjnych w cyberprzestrzeni.

Przestrzeń wirtualna powstała kilkadziesiąt lat temu, została jednakże spopularyzowana w latach dziewięćdziesiątych XX wieku. Wielu z nas było świadkami stopniowego postępu technologicznego, wynalezienia Internetu, komputera przenośnego czy smartfona. Jednakże obecne, młode pokolenia przyjmują cyberprzestrzeń za coś naturalnego, istniejącego od zawsze. Nie ulega wątpliwości, że przestrzeń wirtualna będzie się rozrastać, a dostęp do niej będzie coraz powszechniejszy. Nasuwa się pytanie, czy przy kilkumiliardowej liczbie użytkowników nie należałoby wprowadzić jakiegoś systemu identyfikacyjnego i elektronicznego numeru identyfikacyjnego na wzór numeru PESEL przypisanego indywidualnie od dnia „cyfrowego urodzenia” - od dnia pierwszej rejestracji, pierwszej czynności w cyberprzestrzeni, bądź w przypadku najmłodszych - faktycznie od momentu

[1448] Ibidem, s. 51.

urodzenia. Przyjęcie takiego rozwiązania byłoby niezwykle trudne. Przede wszystkim państwa musiałyby uzgodnić, jaki podmiot nadawałby taki elektroniczny numer identyfikacyjny, jakie dane byłyby w nim gromadzone kto miały dostęp, nadzorował i zarządzał przepływem wszystkich zgromadzonych w systemie danych. Zgromadzenie wszystkich danych w jednym systemie potencjalnie mogłoby niezwykle niebezpieczne, wprowadziłoby zagrożenie wycieku informacji, ataków hackerskich, inwigilacji przez władze różnych państw czy też naruszeniem wolności osobistych jednostek.

Ponadto, postawić należy pytanie, czy obowiązkowa rejestracja nie stanowiłaby nadmiernej inwigilacji, skutkującej naruszeniem naszej prywatności. Przyjęcie obowiązkowej, elektronicznej identyfikacji spowodowałoby, iż władza miałaby niegraniczony dostęp do każdego aspektu naszego życia: oglądanych filmów, przeglądanych stron internetowych, kupowanych w cyberprzestrzeni towarów. Tak dużej inwigilacji nie ma przecież w świecie realnym. Robiąc zakupy w sklepie spożywczym czy aptece jesteśmy anonimowi. Trudno zatem wyobrazić sobie sytuacje, że zakup jakiekolwiek przedmiotu *on-line*, przeglądanie konkretnej witryny internetowej powodowałby dopisanie tej informacji do elektronicznej bazy danych o naszej osobie. Wprowadzenie ścisłej identyfikacji każdego ruchu w przestrzeni cyfrowej byłoby również sprzeczne z wolnościowym i niezależnym charakterem cyberprzestrzeni i z całą pewnością spowodowałoby protesty cyberspołeczności.

Być może trafnym rozwiązaniem byłoby wprowadzenie nieco mniej inwazyjnych metod identyfikacji w cyberprzestrzeni. Na pewno zasadnym krokiem byłoby wprowadzenie obowiązku rejestracji w ściśle określonych przypadkach. Wspomniany wyżej „elektroniczny numer PESEL" mógłby identyfikować podmiot w relacjach z władzami państwowymi. Za pomocą takiego numeru moglibyśmy załatwić sprawę urzędową, złożyć wniosek, dokonywać opłat. Również korzystanie z prywatnych stron internetowych takich jak Facebook czy fora dyskusyjne mogłoby wiązać się z obowiązkiem weryfikacji elektronicznej. Na portalach internetowych często dochodzi do naruszenia wolności słowa, wypowiedzi obraźliwych, a nawet nawoływania do czynów przestępczych. W takich przypadkach szybka weryfikacja danych danej osoby pozwoliłaby na efektywne podjęcie odpowiednich działań. Podobnie w przypadku portali oferujących określone usługi czy towary.Istnienie obowiązku podania numeru identyfikacyjnego ułatwiłoby weryfikację wiarygodności kontrahenta oraz możliwość odnalezienie go i dochodzenie roszczeń w przypadku nieprawidłowego wykonania umowy. Musiałyby jednak zostać opracowane jasne procedury udostępniania tych danych osobowych ze zbioru danych.

Być może przyszłość przyniesie ciekawe, innowacyjne rozwiązanie identyfikacji w cyberprzestrzeni, które będzie zarówno chronić prywatność osoby, jak i umożliwiać jej bezpieczne poruszanie się w cyfrowym świecie. Może powstanie aplikacja, program bądź maszyna, która będzie miała za zadanie bezpieczne osadzenie człowieka w cybernetycznej przestrzeni, chroniąc przed zagrożeniami, kreując jego wirtualny byt. Biorąc zaś pod uwagę postęp techniczny, to rozwiązanie takie może pojawić się szybciej niż nam się wydaje. Zaledwie pięćdziesiąt lat temu wymysłem szaleńca wydawałaby się idea posiadania w kieszeni telefonu komórkowego czy karty płatniczej. System komputerowy statku kosmicznego, który wysłał człowieka na Księżyc miał mniej mocy obliczeniowej niż współczesny smartfon. Można śmiało zaryzykować stwierdzenie, że XXI wiek przyniesienie nieznaną, na tak wielką skalę, ewolucję technologiczną. Wyzwaniem dla prawników i całej społeczności międzynarodowej będzie stworzenie takiego systemu i procedur, które będą z jednej strony regulować, ale z drugiej strony wspomagać rozwój cyberprzestrzeni.

6.3 Rekonstrukcja prawa cyberprzestrzeni

W niniejszych rozważaniach często było stawiane pytanie, czy prawo cyberprzestrzeni zostanie wyodrębnione jako nowa gałąź prawa. Powstanie innych gałęzi prawa było procesem długofalowym, trwającym dekady, a nawet wieki. Czasochłonny proces kształtowania norm umożliwił wykształcenie się w piśmiennictwie spójnych założeń określonych gałęzi prawa. Regulacje krajowe, regionalne i międzynarodowe dotyczące prawa w cyberprzestrzeni są stosunkowo nowe. Powstały na przestrzeni zaledwie kilkudziesięciu - kilkunastu ostatnich lat. Przyjęte normy są jednak fragmentaryczne, niespójne i nierzadko regulują jedynie poszczególne, wybrane problemy. Dalszemu rozdrobnieniu sprzyja, niestety, brak głównego międzynarodowego organu czy instytucji, który w sposób kompleksowy regulowałby prawo w cyberprzestrzeni. Obecnie organizacje międzynarodowe oraz państwa na mocy umów wielostronnych starają się uregulować najistotniejsze zagadnienia. W dłuższej perspektywie rozwiązanie to nie zda egzaminu. Jak słusznie zauważa Jacek Janowski „w razie zaniechania wysiłków na rzecz wyodrębnienia i ujednolicenia prawnej regulacji stosunków informatycznych, nie będzie można zatrzymać rozpoczętego procesu partykularyzacji, rozczłonkowania i zróżnicowania odnośnych unormowań. Dziś rysuje się nie tylko

możliwość, ale i potrzeba wyodrębnienia prawa informatycznego, chociaż niekoniecznie na zasadzie nowej gałęzi prawa”[1449]. Jedynie ostatnie stwierdzenie może budzić sprzeciw. Wydaje się, że prawo cyberprzestrzeni - wcześniej czy później - wyłoni się jako oddzielna gałąź prawa (tak jak to miało miejsce chociażby z prawem kosmicznym czy z prawem ochrony środowiska). Utrzymanie *status quo* doprowadzi do zupełnego chaosu prawnego, a tym samym wzrostu zagrożeń w przestrzeni cyfrowej.

Technologia, a technologia informatyczna w szczególności, rozwija się w niesamowicie szybkim tempie. Rozwój cyberprzestrzeni jest jak „samonapędzająca się lawina”. Nie można jej zatrzymać, lecz należy spróbować skierować ją na właściwe tory prawne. Podobne wnioski wyciągają eksperci, podnosząc, że „tak jak niemożliwe jest odwrócenie zjawiska globalizacji ekonomicznej i informatycznej, tak nieunikniona okaże się perspektywa globalizacji prawa. Zagrożenia ekologiczne, przestępczość informatyczna, czy światowy terroryzm zapewne przełożą się, już się przekładają, na oczekiwane powołania jakiejś postaci ponadpaństwowego porządku prawnego. Nie powinno to jednak prowadzić po stronie teorii i filozofii prawa do podobnego roszczenia na rzecz utwierdzania takiego globalnego porządku poprzez jakąś nową koncepcję prawa, kultury prawa, kultury prawnej czy uniwersalnej etyki”[1450]. Przypomina się jednocześnie, że „rozważając zasadność wprowadzenia szczególnej regulacji prawnej cyberprzestrzeni, trzeba pamiętać, że jest to zawsze regulacja dodatkowa, powstająca na bazie istniejącego stanu prawnego”[1451].

Wychodząc z powyższych rozważań należy stwierdzić, że prawo cyberprzestrzeni nie może zatem powstać jako byt zupełnie oderwany od obowiązujących norm, zasad i zwyczajów. Wręcz przeciwnie, podwaliny prawa cyberprzestrzeni winny być zbudowane na obowiązujących już normach, zasadach i zwyczajach, które są ogólnie akceptowalne i ze względu na swoją naturę, mogą mieć zastosowanie również do działań w przestrzeni wirtualnej. Jacek Janowski wyraził pogląd, że: „abstrahując od zakresu regulacji określonych mianem prawa cyberprzestrzeni, można postulować zastosowanie go do unormowań stosunków nawiązywanych, utrzymywanych i modyfikowanych w cyberprzestrzeni”[1452]. W cyberprzestrzeni są obszary działalności człowieka, w których prawo zarówno krajowe, jak i międzynarodowe stosunkowo łatwo można zaimplementować. Nie ma na przykład potrzeby

[1449] J. Janowski, *Informatyka…*, s. 410.
[1450] A. Bator i in., *Integracja i globalizacja z perspektywy filozofii prawa*, [w:] J. Stelmach (red.), *Filozofia prawa wobec globalizmu*, Kraków 2003, s. 24-25.
[1451] K. Dobrzeniecki, *Lex informatica*, Toruń 2008, s. 84.
[1452] J. Janowski, *Informatyka…*, s. 417.

tworzenia zupełnie nowego prawa zobowiązań, lecz należy je zmodyfikować tak, by obejmowało kontrakty elektroniczne. Podstawowe zasady, tak jak *pacta sunt servanda* będą miały przecież zastosowanie zarówno w świecie realnym, jak i wirtualnym.

Istnieją jednak obszary prawa i obszary cyberprzestrzeni, w których użytkownik sieci porusza się niczym po „wirtualnym oceanie", na którym jedynie od czasu do czasu można natrafić na „legislacyjną wyspę". W doktrynie prezentowane jest zgodne stanowisko, że „nie wszystkie problemy związane z regulacją przestrzeni elektronicznej dadzą się rozwiązać przez odwołanie do tradycyjnych instrumentów prawnych. W niektórych obszarach, ściśle związanych ze specyfiką Internetu, a wyraźnie innych od znanych wcześniej mediów, konieczne jest wskazanie specyficznych rozwiązań. Jeśli jednak mowa o rozwiązaniach wspólnych dla całej aterytorialnej cyberprzestrzeni, jedno w stosunku do nich jest pewne: muszą one korespondować z tą jej wyjątkową cechą, muszą oderwać się od podstawowej dla regulacji prawnych zasady terytorialności i muszą być ponadgraniczne"[1453]. Brak jest holistycznych, spójnych ram prawnych regulujących kwestię własności intelektualnej, baz danych, cyberterroryzmu, pornografii dziecięcej w cyberprzestrzeni i wielu innych obszarów. Inne, częściowo zunifikowane, na przykład cyberprzestępczość, powinny być zmodernizowane.

Nie ulega jednak wątpliwości, że prawo cyberprzestrzeni będzie się stopniowo kształtować. Skoro nie można cofnąć rozwoju technologicznego, to należy stworzyć nowe bądź przekształcić stare normy postępowania tak, by były odpowiednie w przestrzeni o transgranicznym i transnarodowym charakterze. Rozwiązania przyjęte w prawie cyberprzestrzeni powinny jednak charakteryzować się kilkoma cechami. W pierwszej kolejności winny być neutralne technologicznie tak, by prawo odpowiadało postępującej technice i innowacyjnym rozwiązaniom. W drugiej - o ile to możliwe - powinno się czerpać z ogólnie przyjętych i akceptowalnych norm prawa, tak by nie doprowadzić do zjawiska „nadregulacji". Prawo cyberprzestrzeni należy tworzyć z udziałem sektora prywatnego oraz internautów. Ustanowienie reguł wzajemnej współpracy nie może odbyć się bez wszystkich aktorów wirtualnego obrotu, czy to w ujęciu horyzontalnym czy wertykalnym. Podejmowane prace nad stworzeniem prawa cyberprzestrzeni muszą mieć charakter systemowy i odnosić się nie tylko do kwestii technicznych, ale również prawnych, ekonomicznych, społecznych i

[1453] J. Kulesza, *Międzynarodowe…*, s. 351.

rozwojowych[1454]. Prawo powinno być również tworzone nie tylko z udziałem prawników, lecz również etyków, filozofów, twórców i specjalistów z branży IT.

Analiza omawianego zagadnienia prowadzi do przekonania, że szczególnie widoczna jest nieznaczna liczba norm traktatowych dotyczących cyberprzestrzeni, przy jednoczesnym, niemal całkowitym braku prawa zwyczajowego. W rezultacie należy odwołać się do ogólnych przepisów prawa międzynarodowego i jego interpretacji w kontekście przestrzeni wirtualnej, ponieważ cyberdziałalność jest relatywnie nowym zjawiskiem, to również odpowiednie normy polityczne i prawne dopiero się kształtują. Z czasem dojdzie do kodyfikacji właściwego prawa traktatowego i wykrystalizowania się prawa zwyczajowego, w taki sposób, by formalnie wytyczyć granice cyberaktywności. W międzyczasie cyberprzestrzeń będzie środowiskiem intensywnego i często wielokierunkowego rozwoju[1455].

W odniesieniu do cyberprzestrzeni mamy obecnie do czynienia z *law in action* (prawem w działaniu). Prawo międzynarodowe, regionalne i krajowe pozostają zawsze o krok za innowacjami technologicznymi. Dopiero przyszłe lata i dekady pozwolą, jak się wydaje, na wyodrębnienie się samodzielnej dziedziny międzynarodowego prawa cyberprzestrzeni. W chwili obecnej można jedynie domniemywać, kto będzie brał udział w jego tworzeniu oraz na jakich procedurach będzie się ona opierać. Nie można również wykluczyć, że wyłoni się zupełnie nowy byt prawny, coś na kształt prawa Unii Europejskiej, niemieszczący się w ścisłych granicach prawa międzynarodowego. Prawo unijne początkowo również budziło kontrowersję ze względu na swoją specyfikę i odrębności. Podstawowym pytaniem, które powinno się tu zadać nie będzie, czy powstanie międzynarodowe prawo cyberprzestrzeni, lecz raczej, jaką przybierze ono formę. Utrzymanie obecnego *status quo* jest niemożliwe. Prawo w cyberprzestrzeni może ulec samoregulacji, tworzyć się powoli na podwalinach *soft law* bądź zostać uregulowane przez kompetentną organizację międzynarodową. Praktyka pokaże, która z metod okażę się najbardziej efektywna i najkorzystniejsza.

[1454] J. Kulesza, *Międzynarodowe…*, s. 353.
[1455] M.N. Schmitt, L. Vihul The Nature of International Law Cyber Norms, "Tallinn Paper" 2014, nr 5, s. 30-31.

Podsumowanie

Stanisław Lem napisał: „Większość technologii ma świetlisty awers, ale życie dało im rewers - czarną rzeczywistość". Stwierdzenie to z całą pewnością można odnieść do cyberprzestrzeni. Wydaje się, że nie będzie zbyt śmiały wniosek, że wynalezienie Internetu jest jednym z największych osiągnięć ludzkości, które całkowicie zrewolucjonizowało drugą połowę XX wieku. Pojawienie się nowej przestrzeni działalności człowieka doprowadziło teoretyków i praktyków prawa do konkluzji, że obszar ten nie podlega łatwej regulacji i nie zawsze wpisuje się w dotychczasowe ramy prawne. Początkowo porównywano Internet do symbolicznego „Dzikiego Zachodu" jako przestrzeni „gdzie prawa nie ma lub trudno je egzekwować"[1456].

Celem niniejszej dysertacji była weryfikacja aktualnego statusu cyberprzestrzeni w kierunku jej optymalnego uregulowania z wykorzystaniem prawa międzynarodowego, a w dalszej kolejności ustalenie, czy prawo międzynarodowe może udoskonalić rekonstrukcyjnie aktualny status cyberprzestrzeni. Realizacja wskazanego wyżej celu nastąpiła przez zbadanie poglądów teoretyków prawa, judykatury oraz przeprowadzenie analizy wielostronnych umów międzynarodowych, aktów prawnych organizacji międzynarodowych, dokumentów z zakresu tak zwanego *soft law* oraz reprezentatywnych przykładów prawa krajowego.

Cyberprzestrzeń trudno jest ująć w ramy prawne i definicyjne. Do tej pory nie przyjęto jednej uniwersalnej definicji tego terminu. Na ogół cyberprzestrzeń, nazywana również przestrzenią cyfrową lub wirtualną, jest uznawana za przestrzeń wymiany i przetwarzania danych oraz informacji za pomocą systemów technologii informacyjnych powiązanych na poziomie globalnym. Cyberprzestrzeni nie należy utożsamiać wyłącznie z Internetem (choć jest on jej głównym składnikiem), ponieważ jest to pojęcie szersze, obejmujące sieci telekomunikacyjne i systemy komputerowe. Cyberprzestrzeń ma specyficzną, jedyną w swoim rodzaju budowę. Brak w niej jednego centralnego miejsca przechowywania danych, fizycznego „centrum dowodzenia" czy ośrodka decyzyjnego. Do cech charakterystycznych cyberprzestrzeni zalicza się: plastyczność, płynność, obliczalność, terytorialność, dokładność, hipertekstowość, interaktywność, wirtualność, kompatybilność, otwartość, nieograniczoność,

[1456] Por. J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 9.

ponadnarodowość, wszechstronność, złożoność, sieciowość, przenikalność, konwergentność, konsolidację, automatyzację i totalność.

Należy przypomnieć, że Internet powstał jako sieć wojskowa w USA w latach sześćdziesiątych XX wieku, a prace nad rozwojem nowej technologii zostały przekazane ośrodkom akademickim, w których dominowały zdecentralizowane oddolne struktury. Dzięki temu rozwiązaniu cyberprzestrzeń przyjęła obecną formę i architekturę. Użytkownikami sieci są podmioty prywatne - osoby fizyczne i prawne, które pozbawione granic i balastu biurokratycznej hierarchiczności stworzyły zupełnie nowy obszar działalności człowieka - w części - odzwierciedlający realne życie. Tradycyjni aktorzy społeczności międzynarodowej stanęli w obliczu ogromnego wyzwania regulacji przestrzeni wirtualnej i podejmowanej w niej działalności ludzi oraz innych podmiotów, czyli głównie państw i korporacji, ale też organizacji terrorystycznych czy zorganizowanych grup przestępczych.

Zasadniczym problemem prawnym cyberprzestrzeni jest trudność ustalenia jurysdykcji właściwej. Wykonywanie kompetencji jurysdykcyjnej jest ściśle związane z określoną przestrzenią - terytorium - i zazwyczaj tam jest realizowane. Władztwo państwa ma wówczas charakter zupełny i wyłączny. Tymczasem w przestrzeni wirtualnej brak jest bezpośredniego odniesienia do tradycyjnie pojmowanego terytorium. Przestrzeń cyfrowa fizycznie w zasadzie nie istnieje, choć jest intensywnie wykorzystywana przez miliardy użytkowników z różnych zakątków globu. W odniesieniu do występków karnych można zastosować jedną z podstawowych reguł jurysdykcyjnych: zasadę jurysdykcji personalnej, skutkowej czy też miejsca popełnienia czynu. Jednakże przestrzeń wirtualna sprzyja wielomiejscowości wystąpienia skutków czynu, dlatego też wprowadza niepewność prawną co do możliwych konsekwencji naszych działań. Zauważać można wśród niektórych podmiotów trend do rozszerzania swoich granic jurysdykcyjnych. Rozważyć należałoby, czy nie dopuścić stosowania zasady jurysdykcji uniwersalnej w odniesieniu do najpoważniejszych przestępstw w cyberprzestrzeni, to jest pornografii dziecięcej czy cyberterroryzmu. Ochrona dzieci przed seksualnym wykorzystaniem oraz walka z terroryzmem wydaje się następować bezsprzecznie w interesie całej ludzkości. Nie mniej istotne są procesowe aspekty ścigania cyberprzestępców. Konieczna jest tu szeroko zakrojona współpraca państw między innymi w zakresie zbierania i zabezpieczenia dowodów, pomocy prawnej, wymiany informacji czy też międzynarodowych szkoleń.

W jurysdykcji cywilnej najbardziej trafnym rozwiązaniem w zakresie handlu elektronicznego jest zawarcie w umowie klauzuli jurysdykcyjnej. Rozstrzygnięcie takie jest zgodne z zasadą swobody umów oraz daje możliwość uniknięcia sporu kompetencyjnego. W innych przypadkach ustalenie jurysdykcji właściwej wiąże się z koniecznością zastosowania jednej z konwencji międzynarodowych, czyli odnowionej konwencji lugańskiej czy też rozporządzeń unijnych: 1215/2012, Rzym I lub Rzym II, które wprowadzają rozmaite łączniki jurysdykcyjne takie, jak miejsce zamieszkania powoda, konsumenta, miejsca wykonania umowy czy świadczenia usługi.

Tradycyjne kryterium terytorialności zupełnie nie znajduje zastosowania w nowej przestrzeni cyfrowej. Działalność człowieka w zdecentralizowanej i transgranicznej cyberprzestrzeni tworzy niepewność prawną wobec braku jasno zakreślonych reguł. Konsekwencją tych rozważań jest konkluzja, że specyficzna konstrukcja cyberprzestrzeni wymyka się spod klasycznych norm jurysdykcyjnych, dlatego też niezbędne jest opracowanie nowych zasad regulujących jurysdykcję w przestrzeni cyfrowej.

Sieć globalna, oprócz oczywistych, niewymiernych korzyści, determinuje liczne problemy i zagrożenia, nie tylko dla indywidualnych użytkowników, lecz również dla złożonych podmiotów państwowych i prywatnych. Infrastruktura krytyczna państwa sterowana przez systemy komputerowe musi podlegać szczególnej ochronie, a prowadzona już dzisiaj wojna informacyjna z czasem może przerodzić się w konflikt cybernetyczny. Firmy prywatne są również narażone na wycieki danych osobowych, ataki cyberprzestępców czy włamania do systemów bankowych. Część z zagrożeń zakwalifikować należy jako zupełnie nowe byty powstałe w cyberprzestrzeni i wyłącznie dla niej swoiste. Deliktami charakterystycznymi dla przestrzeni wirtualnej są na przykład hacking czy ataki DDoS. Zdecydowaną większość stanowią jednak czyny i zobowiązania, które transformowały z przestrzeni tradycyjnej do wirtualnej, gdyż wcześniej występowały i były odpowiednio regulowane w prawie międzynarodowym i krajowym. Przestępczość, wolność słowa, własność intelektualna czy zawieranie umów na odległość to tylko przykładowe obszary, w których zaistniała konieczność wypracowania nowych norm uwzględniających transgraniczny i ponadnarodowy charakter sieci globalnej. Okazało się bowiem, że stosowanie istniejących już rozwiązań jest niewystarczające lub zwyczajnie nieskuteczne albo też zbytnio rozszerza kompetencje poszczególnych państw.

Analiza cyberprzestrzeni z punktu widzenia postawionej w rozprawie tezy prowadzi do wniosku, że to właśnie prawo międzynarodowe jest najbardziej predysponowane do racjonalnego i użytecznego modelowania oraz harmonizacji regulacji krajowych dotyczących cyberprzestrzeni. Za stanowiskiem takim przemawia kilka argumentów. Przede wszystkim krajowe przepisy (i kultury) prawne są bardzo niejednolite, niejednokrotnie wzajemnie się wykluczają powodując znaczne trudności dochodzenia roszczeń w przypadku wystąpienia cyberczynnika. Obecnie państwa, wobec braku międzynarodowych regulacji oraz jednolitej praktyki, w sposób jednostronny próbują regulować treści zawarte w cyberprzestrzeni. Stan taki wprowadza niepewność obrotu oraz obawę użytkowników, że podejmowane przez nich czynności mogą wywołać skutki prawne w państwie na drugim końcu globu. Prowadzone są równocześnie próby rozciągnięcia jurysdykcji państwowej na wszelkie treści zawarte w sieci. Jedynie prawo międzynarodowe jest w stanie zharmonizować i ujednolicić obecny niekoherentny status prawny cyberprzestrzeni.

Analiza polityki państw oraz ich ustawodawstwa w odniesieniu do cyberprzestrzeni doprowadziła autorkę do licznych wniosków. Przede wszystkim znaczna większość państw w aktach prawnych dotyczących cyberprzestrzeni akcentuje konieczność intensywnej wielostronnej współpracy międzynarodowej, wymiany doświadczeń oraz informacji. Tendencja ta jest szczególnie widoczna w państwach wysoko rozwiniętych (zwłaszcza w kręgu europejskim), które charakteryzują się wysokim stopniem uzależnienia od nowych technologii. Wydaje się, że wynika to z dużej świadomości zagrożeń oraz z tego, że czyny cyberprzestępców, a zwłaszcza cyberterrorystów mają charakter transgraniczny. Co więcej, charakteryzuje je duża dynamika działań oraz intensywna zmienność metod przestępczych. Te czynniki wpływają na konieczność zacieśnienia współpracy i szybkiego informowania o nowych metodach działania sprawców. Z kolei państwa, które stały się ofiarami ataków, zdały sobie sprawę, że są zbyt małe bądź niedostatecznie silne, by skutecznie odeprzeć cyberatak albo zapobiec jego skutkom. Dlatego też szukają pomocy we współpracy międzynarodowej. Państwa poszkodowane zdają sobie sprawę, że wyłącznie odpowiednie przygotowanie techniczne może uniemożliwić lub chociaż znacznie zminimalizować skutki potencjalnego ataku. Na aprobatę zasługuje zatem strategia przyjęta przez Estonię, budującą „cyberrezerwę", swoistą ochotniczą armię informatyków, która podjęłaby działania obronne w przypadku wystąpienia cyberataku przeciwko państwu estońskiemu.

Zupełnie inne są motywy działania supermocarstw. Stany Zjednoczone w wydawanych przez siebie aktach prawnych stale podkreślają konieczność poszanowania

międzynarodowych standardów i współpracę międzynarodową. Szczegółowa analiza dokumentów prowadzi jednak do odmiennego przekonania. USA mają zamiar współpracować i pokojowo załatwiać spory w cyberprzestrzeni do czasu, gdy to jest dla nich korzystne lub obojętne ich interesom. W przypadku, gdy stroną konfliktu będą USA, zastrzegają sobie prawo użycia cyberoperacji do zakończenia trwającego konfliktu „na amerykańskich warunkach"[1457]. Przepis ten wydaje się być jednostronnym aktem usprawiedliwiającym bezprawne ataki, inwigilowanie i wykorzystanie cyberprzestrzeni do realizacji własnych celów. Inaczej do zagadnienia podchodzą Rosja i Chiny. Ich polityka w cyberprzestrzeni - przynajmniej oficjalnie - nakierowana jest bardziej na stosunki wewnątrzpaństwowe. Chiny od lat inwigilują i cenzurują w zakresie swych wpływów cyberprzestrzeń, zakazując dostępu do określonych treści, argumentując wszystko potrzebą ochrony obywateli przed działalnością wywrotową. W praktyce zakazane jest wszystko co niezgodne z polityką partii komunistycznej. Również Rosja - w oficjalnych dokumentach - podkreśla konieczność podniesienia konkurencyjności technologicznej rosyjskiej gospodarki w zakresie rozwiązań IT - tak, by uniezależnić się od technologii zachodnich. Dużą wagę przywiązuję się do cyberbezpieczeństwa, zwłaszcza w obliczu cyberprzestępczości oraz cyberterroryzmu. Tym, co z pewnością łączy wymienione wyżej mocarstwa jest gotowość do niezgodnego z prawem wykorzystywania cyberprzestrzeni do realizacji swoich celów. USA, Rosja i Chiny znajdują się w czołówce państw będących nie tylko ofiarami, ale również agresorami cyberataków. Rosja niemal na pewno wykorzystała „swoich" hakerów do pamiętnych ataków na Estonię i Gruzję. Z kolei ostatnie doniesienia prasowe wskazują, że mogło dojść do cyberwłamań i manipulacji wynikiem wyborczym w rywalizacji o urząd prezydenta USA pomiędzy Hilary Clinton i Donaldem Trumpem w 2016 roku. Jeżeli doniesienia te są zgodne z prawdą, to mamy do czynienia z jednym z najbardziej drastycznych, choć gołym okiem niewidocznym, przykładów ingerencji w stosunki wewnętrzne drugiego państwa, której prawo międzynarodowe publiczne kategorycznie zabrania.

W sferze prawa najistotniejszym chyba aktem prawnym wpływającym na harmonizację zagadnień cyberprzestępczości jest Konwencja o cyberprzestępczości. O jej doniosłym znaczeniu świadczy chociażby fakt przystąpienia do niej krajów spoza Rady Europy oraz wzorowanie ustawodawstw krajowych państw z innych regionów globu właśnie

[1457] Cyberstrategia Departamentu Obrony Stanów Zjednoczonych Ameryki, dokument wydany przez Sekretariat Obrony USA, kwiecień 2015, s. 5. Dokument dostępny on-line https://www.defense.gov/Portals/1/features /2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [10.10.2016].

na jej postanowieniach. W prawie unijnym kwestię cyberprzestępczości regulowała Decyzja ramowa nr 2005/222, która w obliczu nasilenia się zjawiska została uchylona Dyrektywą nr 2012/40 dotyczącą ataków na systemy informatyczne, wprowadzającą szereg nowych rozwiązań. Wskazane regulacje tworzą, jak się wydaje zalążek europejskiego ładu cybernetycznego, który (jako postulat autorki) być może rozwinie się w przyszłości.

Do obszarów, względem których winna nastąpić harmonizacja przepisów krajowych na poziomie międzynarodowym zaliczyć należy cyberprzestępczość, pornografię dziecięcą oraz zmasowane cyberataki. Rekomendowanym sposobem unifikacji norm prawnych w tym zakresie jest możliwie szeroka ratyfikacja Konwencji o cyberprzestępczości. Pomimo, że regulacje Rady Europy i Unii Europejskiej wprowadzają pożądane standardy, to jednak bez zakrojonej na szeroką skalę współpracy międzynarodowej nie da się osiągnąć znaczącej poprawy w walce z obrotem treściami pedofilskimi, podobnie jak z cyberterroryzmem czy przestępczością zorganizowaną. Zauważyć należy, że mimo coraz aktywniejszego wykorzystywania cyberprzestrzeni przez terrorystów brakuje na poziomie międzynarodowym jednego aktu, który poruszałby bezpośrednio zagadnienie cyberterroryzmu. Kwestią szczególnej wagi jest z pewnością wprowadzenie odpowiedniej międzynarodowej polityki w przedmiocie cyberataków. Przeprowadzane w ostatnich latach cyberataki na USA czy wspomniane Estonię i Gruzję ukazują potrzebę kwalifikacji tego typu czynów z punktu widzenia prawa międzynarodowego. Przyczynkiem do wprowadzenia zmian prawnych w zakresie cyberbezpieczeństwa z całą pewnością jest deklaracja złożona w czasie ubiegłorocznego szczytu NATO w Warszawie (w 2016 roku), w trakcie którego uznano, że ataki w cyberprzestrzeni mogą być uznane za naruszenie art. 5 Traktatu Północnoatlantyckiego. W związku z tym istnieje nagląca potrzeba zidentyfikowania i sklasyfikowania tego typu ataków w świetle prawa międzynarodowego. Obecnie brakuje jakichkolwiek norm wskazujących, kiedy cyberatak może być uznany za zbrojną napaść na państwo. Biorąc pod uwagę, że cybermocarstwa (takie, jak Chiny, Rosja czy USA) są krajami posiadającymi dostęp do broni jądrowej, potrzeba wypracowania jasnej klasyfikacji cyberataków staje się tym bardziej istotna.

Niezależnie od powyższego jednym z podstawowych sposobów wykorzystania przestrzeni cyfrowej jest handel elektroniczny. Kluczowe znacznie odegrały tu przyjęte przez UNCITRAL umowy modelowe, które mimo niewiążącego charakteru miały ogromny wpływ na unifikację krajowych porządków prawnych. Na podstawie umów modelowych w 68

krajach wprowadzono zmiany legislacyjne[1458]. Z kolei w Unii Europejskiej szczególną rolę w unifikacji prawa dotyczącego *e-commerce* odegrała dyrektywa Parlamentu Europejskiego i Rady nr 2000/31/WE z dnia 8 czerwca 2000 r. o handlu elektronicznym, która wprowadziła zasady świadczenia usług społeczeństwa informacyjnego, zawierania umów za pomocą środków elektronicznych oraz odpowiedzialności dostawców usług. Możliwość zawierania umów w cyberprzestrzeni nie doprowadziła *de facto* do wykształcenia się zupełnie nowego elektronicznego prawa zobowiązań. Dotychczasowe rozwiązania prawne zostały zastosowane bezpośrednio do umów elektronicznych, wprowadzając jedynie modyfikacje dotyczące specyfiki przestrzeni cyfrowej chociażby w zakresie miejsca i czasu zawarcia umowy. Optymalnym rozwiązaniem problemu multijurysdykcyjności w odniesieniu do handlu elektronicznego wydaje się wybór sądu właściwego za pomocą klauzuli jurysdykcyjnej zawartej w umowie bądź we wzorcu umownym. Większość porządków prawnych przyznaje szczególną ochronę praw konsumentów i dopuszcza możliwość dochodzenia swych praw przez sądem właściwym dla konsumenta. W przypadku zawierania umów dwustronnie profesjonalnych najtrafniejszym rozwiązaniem jest właśnie wybór prawa właściwego. Zauważyć należy, że obrót elektroniczny zmienił klasyczny model zawarcia umowy oparty na autonomii stron. Masowe umowy zawierane na odległość za pomocą wzorca kontraktowego zastąpiły tradycyjne umowy bezpośrednio negocjowane przez strony. Umowy adhezyjne w przestrzeni cyfrowej spowodowały przyśpieszenie stosunków kontraktowych, szeroki oraz masowy dostęp do świadczeń odpowiadających potrzebom nabywców. Możliwość modelowania stosunków przez strony umowy nie oznacza, że prawo międzynarodowe nie znajdzie tu zastosowania. Wręcz przeciwnie, potrzebne są wspólne harmonijne przepisy, które eliminowałyby liczne rozbieżności, a nawet sprzeczności regulacji krajowych. Prawo międzynarodowe winno również wskazać kierunek legislacyjny w odniesieniu do najnowszych nowinek technicznych takich, jak pieniądz wirtualny czy chmura obliczeniowa (ostatnie wydarzenia na tym polu dotkliwie to potwierdzają). Obecnie, międzynarodowe regulacje dotyczące handlu elektronicznego są rozproszone i fragmentaryczne, dlatego zasadne jest rozpoczęcie prac nad międzynarodowym aktem prawnym regulującym *e-commerce*. Akt ten winien rozstrzygać najistotniejsze zagadnienia związane z jurysdykcją, czasem, miejscem zawarcia i wykonania umowy, deliktami internetowymi, odpowiedzialnością za szkody i innymi newralgicznymi elementami elektronicznego obrotu handlowego.

[1458] Dane z oficjalnej strony internetowej UNCITRAL: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html [01.03.2017].

Ogromnym wyzwaniem jest wprowadzenie odpowiednich regulacji zagadnienia własności intelektualnej w cyberprzestrzeni. Nowe technologie informacyjne, a także aplikacje i programy komputerowe stanowią immanentną część przestrzeni cyfrowej, stąd też winny podlegać odpowiedniej ochronie. Własność intelektualna w przestrzeni wirtualnej ulega systematycznemu poszerzeniu oraz wzrostowi, a w prawie zarówno w międzynarodowym publicznym, jak i unijnym brak jest holistycznych unormowań odpowiadających współczesnym wyzwaniom. Postulowanym rozwiązaniem jest wprowadzenie jednego, generalnego aktu prawnego regulującego (bądź przynajmniej modelującego tymczasowo) prawo własności Intelektualnej w Unii Europejskiej. Konieczne jest również wprowadzenie regulacji dotyczących chmury obliczeniowej, programów *peer to peer* czy też ustalenie statusu prawnego stron internetowych, programów i aplikacji, opartych na zasadzie neutralności technologicznej.

Analiza inicjatyw międzynarodowych i regionalnych dotyczących cyberprzestrzeni pozwala przyjąć, że Organizacja Narodów Zjednoczonych, Rada Europy oraz Unia Europejska podejmują kroki w celu zwiększenia bezpieczeństwa sieci i systemów komputerowych, lecz ich efektywność pozostawia jeszcze wiele do życzenia. Czynnikiem negatywnie wpływającym na klarowność systemu jest fragmentacja i rozproszenie regulacji w wielu aktach prawnych, stąd też niezbędne jest stworzenie aktu prawnego, który unifikowałby przepisy dotyczące kluczowych zagadnień cyberprzestrzeni. Jednym z głównych problemów do uregulowania jest z całą pewnością brak wspólnej terminologii i definicji pojęciowych, które przyczyniłyby się do harmonizacji i jednakowej interpretacji pewnych działań w sieci. Ustanowienie takich regulacji musiałoby wiązać się z zapewnieniem neutralności technologicznej i elastyczności, tak by zakresem swym mogły one objąć powstające wciąż zagrożenia oraz rozwijającą się stale technologię.

Nowy ład prawny cyberprzestrzeni winien być zbudowany częściowo na podstawie istniejących źródeł prawa, lecz z czasem konieczne stanie się opracowanie zupełnie nowych standardów i kompleksowych ram prawnych dedykowanych przestrzeni wirtualnej. Uznanie cyberprzestrzeni za czwartą przestrzeń międzynarodową co do zasady mogłoby okazać się trafnym pomysłem. Mimo, że zarówno przestrzeń kosmiczna, Antarktyda i morze otwarte oparte są na łączniku terytorialnym, to przestrzeń wirtualna wykazuje wiele punktów stycznych z tymi przestrzeniami (a w szczególności z przestrzenią kosmiczną). Największym podobieństwem wszystkich wymienionych przestrzeni międzynarodowych jest wolność od wszelkiej suwerennej władzy, ale również niezawłaszczalność, wolny dostęp i postulat

pokojowego wykorzystania. Cyberprzestrzeń winna być wykorzystywana dla wspólnego dobra całej ludzkości, a każdy internauta powinien mieć dostęp do zgromadzonych w niej zasobów (wiedzy, informacji, edukacji, rynków zbytu). Rozważyć należy postulat, by przestrzeń cyfrową uznać, za nowe elektroniczne, globalne dobro wspólne.

Odrzucić należy propozycje zarządzania cyberprzestrzenią wyłącznie przez autoregulację. Oddolny sposób regulacji przestrzeni wirtualnej determinuje zbyt duże ryzyko nadużyć, a brak odpowiedniego autorytetu spowodować może nieefektywność stosowania sankcji w przypadku zachowań niezgodnych z ogólnie przyjętą „netykietą". Niemniej jednak system ten winien być stosowany pomocniczo, w myśl wolnościowego charakteru cyberprzestrzeni. Próby odgórnego narzucenia określonych rozwiązań przez państwa i bagatelizowanie cybernetycznej społeczności mogą doprowadzić do zbiorowych protestów, nie tylko w przestrzeni wirtualnej, lecz również w świecie realnym (jak miało to miejsce chociażby w odniesieniu do propozycji podpisania przez Polskę umowy ACTA). Wydaje się, że przy braku jasnych regulacji, prawo międzynarodowe winno być (metodologicznie) stosowane rekonstrukcyjnie, by udoskonalać aktualny status cyberprzestrzeni.

Przegląd obecnego stanu prawnego cyberprzestrzeni prowadzi do przekonania, że istnieje konieczność wprowadzenia zmian w systemie zarządzania Internetem. Sieć globalna powinna zostać z zasady umiędzynarodowiona i zdemokratyzowana, gdyż tylko takie podejście pozwoli na rozwój nie tylko samej cyberprzestrzeni, ale też opartego na wiedzy społeczeństwa informacyjnego[1459]. Rozproszenie i fragmentacja norm prawnomiędzynarodowych odnoszących się do cyberprzestrzeni pozwalają wnioskować, że powodem takiego stanu rzeczy jest brak jednego, centralnego ośrodka międzynarodowego, który miałby kompetencje do tworzenia prawa cyberprzestrzeni. Organ taki mógłby zostać utworzony jako zupełnie nowa, niezależna instytucja międzynarodowa bądź jako organizacja wyspecjalizowana w ramach ONZ (choć tu „dziedzictwo" ONZ nie gwarantuje „autorytetu efektywnościowego"). Niezależnie jednak od przyjętej formy, nowa instytucja do spraw cyberprzestrzeni winna być zbudowana na przejrzystych, demokratycznych zasadach oraz zapewniać reprezentację wszystkich najważniejszych podmiotów międzynarodowych i przedstawicieli społeczeństwa informacyjnego, w tym sektora prywatnego. Ustosunkowując się do kwestii sporów w cyberprzestrzeni, należy stwierdzić, że istniejące sądy i trybunały międzynarodowe już od lat stają w obliczu problemów prawnych związanych się z

[1459] J. Kulesza, *Międzynarodowe…*, s. 353.

działalnością człowieka w przestrzeni wirtualnej, a wydawane przez nie wyroki stanowią istotny wkład w kształtowanie się międzynarodowego prawa cyberprzestrzeni. Niemniej jednak, wydanie orzeczenia końcowego jest w międzynarodowych sądach i trybunałach procesem długotrwałym. Co więcej, można prognozować, że liczba spraw związanych z działalnością człowieka w cyberprzestrzeni będzie się lawinowo zwiększała. Wobec tego, w niedalekiej przyszłości pojawi się potrzeba powołania międzynarodowych organów oraz sądów arbitrażowych właściwych w sprawach cyberprzestrzeni, w których sędziowie swoimi wyrokami będą sprawnie wypełniać luki w prawie cyberprzestrzeni. Kluczowe jest tu jednak nie tyle prawo, ile podejście sędziów i sprawna, adekwatna procedura.

Rozwiązaniem, które winno zostać zrealizowane w najbliższej przyszłości jest opracowanie międzynarodowej konwencji ramowej o cyberprzestrzeni, która mogłaby zarysować ogólne ramy prawne cyberprzestrzeni, a następnie wskazać zasady, normy i procedury ułatwiające bardziej szczegółowe regulacje w przyszłości. Musi bowiem pojawić się globalne rozwiązanie ustalające podstawowe zasady zarządzania cyberprzestrzenią, współpracy państw oraz zainteresowanych podmiotów społecznych. Przyjmowanie kompletnego prawa pozytywnego jest procesem długotrwałym i bardzo pracochłonnym to też wypracowanie konwencji ramowej może pozwolić na bieżące budowanie adekwatnych rozwiązań prawnych niehamując zasadniczo głównego procesu prawotwórczego (gwarantuje to zbieżność treściowa konwencji ramowej z rozłożoną w czasie długotrwałą kodyfikacją).

Nie mniej istotne w kształtowaniu się prawa cyberprzestrzeni jest wykorzystanie ogólnych zasad prawa, zwyczaju międzynarodowego oraz - pomocniczo - orzecznictwa i judykatury. Znaczący wpływ na stosunki prawne w przestrzeni cyfrowej może wywrzeć też *soft law*. Jak wskazano powyżej stanowienie prawa pozytywnego na poziomie międzynarodowym jest długotrwałe i pracochłonne. W sytuacji zaś, gdy brak jest twardych zasad, to właśnie „prawo miękkie" może stać się swoistym „drogowskazem" tworząc podwaliny pod formułujące się traktatowe prawo cyberprzestrzeni (wskazuje kierunki rozwoju, poddaj epod dyskusje merytoryczne treści i stanowi układ odniesienia do praktyki). Zgodna praktyka państw i innych podmiotów może z kolei w przyszłości doprowadzić do wykształcenia się norm zwyczajowych na przykład zasady wolności i niezawłaszczalności cyberprzestrzeni (co może zostać dostrzeżone i potwierdzone w orzecznictwie).

W ten sposób został nakreślony scenariusz optymistyczny. Czy zrealizuje się? Czy w takim właśnie kształcie? Trudno przewidzieć, ale można założyć, obserwując przy tym

analitycznie (wedle formuły „*law in action*”). Mottem mogą być tu słowa Marco Polo, który stwierdził, że: „Gdy nie ma dokąd zawrócić, trzeba iść naprzód”. Nie można cofnąć rozwoju technologicznego i rewolucji cyfrowej, którą spowodowało pojawienie się i upowszechnienie cyberprzestrzeni. Konieczne jest zatem przyjęcie nowej metody i zmiana podejścia do uregulowania sieci globalnej. Wydaje się, że obecnie podejmowane próby dostosowania prawa do szybko rozwijających się technologii są nieefektywne. Prawo międzynarodowe publiczne winno pełnić rolę wzorca (swoistego „metra” z Sèvres) wskazującego drogę ustawodawcom krajowym. Charakterystyka cyberprzestrzeni ukazała bowiem, że jest to obszar, którego nie można wprost porównać do żadnego innego bytu, z jakim prawo musiało się mierzyć na przestrzeni wieków. Cyberprzestrzeń potrzebuje tu więc elastycznej metody regulacji, a prawem, które jest najbardziej predysponowane do podjęcia tego wyzwania jest prawo międzynarodowe publiczne.

BIBLIOGRAFIA I NETOGRAFIA

Wykaz aktów normatywnych

Prawo polskie

Akty prawa powszechnie obowiązującego

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. z 1997 r., nr 78 poz. 483
2. Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny, Dz. U. z 1964 r., nr 16, poz. 93
3. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz. U. z 1994 r., nr 24, poz. 83
4. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny, Dz. U. z 1997 r., nr 88, poz. 553 z późn. zm.
5. Ustawa o podpisie elektronicznym z dnia 18 września 2001 r., Dz. U. z 2001 r., nr 130, poz. 1450 z późn. zm.
6. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz. U. z 2002 r., nr 156, poz. 1301
7. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. z 2007 r., nr 89, poz. 590 ze zm.
8. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz. U. z 2011 r., nr 199 poz. 1175
9. Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r., Dz. U. z 2014 r., poz. 1514
10. Ustawa z dnia 26 września 2014 r. o ratyfikacji Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzonej w Lanzarote w dniu 25 października 2007 r., Dz. U. z 2014 r., poz. 1623
11. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz. U. z 2016 r., poz. 1579

Prawo wspólnotowe

Prawo pierwotne

1. Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana), Dz. Urz. UE 2012 C 326
2. Karta Praw Podstawowych Unii Europejskiej, Dz. Urz. UE 2012 C 326

Prawo wtórne

1. Dyrektywa Rady nr 93/83/EWG z dnia 27 września 1993 r. w sprawie koordynacji niektórych zasad dotyczących prawa autorskiego oraz praw pokrewnych stosowanych w odniesieniu do przekazu satelitarnego oraz retransmisji drogą kablową, Dz. Urz. WE L 248 z dnia 06.10.1993 r.
2. Dyrektywa Parlamentu Europejskiego i Rady nr 96/9/WE z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych, Dz. Urz. WE L z dnia 27.03.1996 r.
3. Dyrektywa Parlamentu Europejskiego i Rady nr 2000/31/WE z dnia 8 czerwca 2000 r., w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz. Urz. UE L 178 z dnia 17.07.2000 r.
4. Dyrektywa Parlamentu Europejskiego i Rady nr 2000/46/WE z dnia 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, Dz. Urz. WE L 275 z dnia 27.10.2000 r.
5. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 45/2001 z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnych przepływie takich danych, Dz. Urz. UE L 8 z dnia 12.01.2001 r.
6. Rozporządzenie Rady (WE) nr 44/2001 z dnia 22 grudnia 2000 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, Dz. Urz. L 12 z dnia 16.01.2001 r.
7. Dyrektywa Parlamentu Europejskiego i Rady nr 2001/29/WE z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, Dz. Urz. WE L 167 z dnia 22.06.2001 r.
8. Decyzja ramowa Rady 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, Dz. Urz. WE L 149 z dnia 02.06.2001 r.
9. Dyrektywa Parlamentu Europejskiego i Rady 2002/65/WE z dnia 23 września 2002 r. dotycząca sprzedaży konsumentom usług finansowych na odległość oraz zmieniająca dyrektywę Rady 90/619/EWG oraz dyrektywy 97/7/WE i 98/27/WE, Dz.Urz. L 271 z dnia 09.10.2002 r.
10. Dyrektywa Parlamentu Europejskiego i Rady nr 2004/48/WE z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej, Dz. Urz. WE L 157 z dnia 30.04.2004 r.
11. Decyzja Parlamentu Europejskiego i Rady 854/2005/WE z dnia 11 maja 2005 r. w sprawie ustanowienia wieloletniego programu wspólnotowego na rzecz promowania bezpieczniejszego korzystania z Internetu i nowych technologii sieciowych, Dz. Urz UE L 149 z dnia 11.06.2005 r.
12. Dyrektywa Parlamentu Europejskiego i Rady 2006/115/WE z dnia 12 grudnia 2006 r. w sprawie prawa najmu i użyczenia oraz niektórych praw pokrewnych prawu autorskiemu w zakresie własności intelektualnej, Dz. Urz. UE L 376 z dnia 27.12.2006 r.
13. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 864/2007 z dnia 11 lipca 2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych Rzym II, Dz. Urz. L 199 z dnia 31.07.2007 r.
14. Decyzja Rady z 15.10.2007 r. dotycząca podpisania Konwencji lugańskiej o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń w sprawach cywilnych i handlowych (2007/712/WE), Dz. Urz. UE z 2007 r., nr. K 339

15. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I), Dz. Urz. L 177 z dnia 04.07.2008 r.
16. Dyrektywa Komisji 2008/63/WE z dnia 20 czerwca 2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych (Wersja skodyfikowana) (Tekst mający znaczenie dla EOG), Dz. Urz. L 162 z dnia 21.06.2008 r.
17. Dyrektywa Parlamentu Europejskiego i Rady nr 2008/95/WE z dnia 22 października 2008 r. mająca na celu zbliżenie ustawodawstw państw członkowskich odnoszących się do znaków towarowych, Dz. Urz. UE L. z dnia 08.11.2008 r.
18. Decyzja ramowa 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych, Dz.Urz.UE L 328 z dnia 6.12.2008. r.
19. Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych, Dz. Urz. UE L 265 z dnia 11.10.2011 r.
20. Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE, Dz. Urz. L 267 z dnia 10.10.2009 r.
21. Dyrektywa Parlamentu Europejskiego i Rady nr 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz. Urz. UE L 337 z dnia 18.12.2009 r.
22. Dyrektywa Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej, Dz. Urz. L 337 z dnia 18.12.2009 r.
23. Decyzja ramowa Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów, Dz. Urz. UE L 328 z dnia 15.12.2008 r.
24. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 30 września 2010 r. w sprawie ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE L 218/8 z dnia 14.08.2013 r.
25. Dyrektywa Parlamentu Europejskiego i Rady nr 2011/77/UE z dnia 27 września 2011 r. dotycząca zmiany dyrektywy 2006/116/WE w sprawie czasu ochrony prawa autorskiego i niektórych praw pokrewnych, Dz. Urz. UE L 265 z dnia 10.11.2011 r.
26. Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady, Dz. Urz. UE L 304 z dnia 22.11.2011 r.
27. Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i

wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW, Dz. Urz. UE L 335 z dnia 17.12.2011 r.
28. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, Dz. Urz. L 351 z dnia 20.12.2012 r.
29. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 Tekst mający znaczenie dla EOG, Dz. Urz. L 165 z dnia 18.06.2013 r.
30. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. w sprawie ataków na systemy informatyczne i uchylającą decyzję ramową Rady 2005/222/WSiSW, Dz.Urz. UE L 218/8 z dnia 14.08.2013 r.
31. Dyrektywa Parlamentu Europejskiego i Rady 2014/61/UE z dnia 15 maja 2014 r. w sprawie środków mających na celu zmniejszenie kosztów realizacji szybkich sieci łączności elektronicznej, Dz. Urz. UE L 155 z dnia 23.05.2014 r.
32. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS), Dz. Urz. L 257 z dnia 28.08.2014 r.
33. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. U. L 119 z dnia 4.05.2016 r.

Prawo międzynarodowe

1. Karta Narodów Zjednoczonych, Dz. U. z 1947 r., nr 23, poz. 90
2. Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r., Dz. U. z 2000 r., nr 87, poz. 970
3. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz. U. z 1993 r., nr 61, poz. 284
4. Konwencja genewska o ochronie osób cywilnych podczas wojny (IV konwencja genewska) z dnia 12 sierpnia 1949 r., Dz. U. z 1956 r., nr 38, poz. 171
5. Konwencja o morzu pełnym sporządzona w Genewie dnia 29 kwietnia 1958 r., Dz. U. z 1963, nr 33, poz. 187
6. Układ w sprawie Antarktydy podpisany w Waszyngtonie dnia 1 grudnia 1959 r., Dz. U. z 1961 r., nr 46, poz. 237
7. Konwencja o uznawaniu i wykonywaniu zagranicznych orzeczeń arbitrażowych, sporządzona w Nowym Jorku dnia 10 czerwca 1958 r., Dz. U. z 1962 r., nr 9, poz. 41
8. Układ o zasadach działalności państw w zakresie badań i użytkowania przestrzeni kosmicznej łącznie z Księżycem i innymi ciałami niebieskimi, sporządzony w Moskwie, Londynie i Waszyngtonie dnia 27 stycznia 1967 r., Dz. U. z 1968 r., nr 14, poz. 82

9. Konwencja o ustanowieniu Światowej Organizacji Własności Intelektualnej, sporządzona w Sztokholmie dnia 14 lipca 1967 r., Dz. U. z 1975 r., nr 9, poz. 49
10. Konwencja Wiedeńska o Prawie Traktatów sporządzona w Wiedniu dnia 23 maja 1969 r., Dz. U. z 1990 r., nr 74, poz. 439
11. Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, sporządzona w Hadze dnia 16 grudnia 1970 r., Dz. U. z 1972 r., nr 25, poz. 181
12. Konwencja o przedawnieniu w międzynarodowej sprzedaży towarów, sporządzona w Nowym Jorku dnia 14 czerwca 1974 r., Dz. U. z 1997 r., nr 45, poz. 282
13. Konwencja o rejestracji obiektów wypuszczonych w przestrzeń kosmiczną, otwarta do podpisania w Nowym Jorku dnia 14 stycznia 1975 r., Dz. U. z 1979 r., nr 5, poz. 22
14. Międzynarodowy Paktu Praw Obywatelskich i Politycznych uchwalony w Nowym Yorku dnia 16 grudnia 1966 r., Dz. U. z 1977 r., nr 38, poz. 167
15. Konwencja o prawie właściwym dla zobowiązań umownych, otwarta do podpisu w Rzymie dnia 19 czerwca 1980 r., Dz. Urz. UE C 169, z dnia 08.07.2005 r.
16. Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r., Dz. U. z 2003 r., nr 3, poz. 25
17. Konwencja w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 10 grudnia 1984 r., Dz. U. z 1989 r., nr 63, poz. 378
18. Konwencja berneńska o ochronie dzieł literackich i artystycznych z dnia 9 września 1986 r. (obecnie obowiązujący tekst – Akt paryski Konwencji berneńskiej o ochronie dzieł literackich i artystycznych sporządzony w Paryżu dnia 24 lipca 1971 r.), Dz. U. z 1990 r., nr 82 poz. 474
19. Konwencja Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów, sporządzona w Wiedniu dnia 11 kwietnia 1980 r., Dz. U. z 1997 r., nr 45, poz. 286
20. Konwencja Narodów Zjednoczonych o prawie morza, sporządzona w Montego Bay dnia 10 grudnia 1982 r., Dz. U. z 2002 r., nr 59, poz. 534
21. Porozumienie ustanawiające Światową Organizację Handlu (WTO), sporządzone w Marakeszu dnia 15 kwietnia 1994 r., Dz. U. z 1995 r., nr 98, poz. 483
22. Traktat Światowej Organizacji Własności Intelektualnej o Prawie Autorskim, sporządzony w Genewie dnia 20 grudnia 1996 r., Dz. U. z 2005 r., nr 3, poz. 12
23. Traktat WIPO o artystycznych wykonaniach i fonogramach, sporządzony w Genewie dnia 20 grudnia 1996 r., Dz. U. z 2004 r., nr 41, poz. 375
24. Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r., Dz. U. z 2005 r., nr 18 poz. 158
25. Konwencja o cyberprzestępczości sporządzona w Budapeszcie w dniu 23 listopada 2001 r., Dz. U. z 2014 r., poz. 1514
26. Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu dnia 28 stycznia 2003 r., Dz. U. z 2015 r., poz. 730
27. Konwencja o ochronie dzieci przed seksualnym wykorzystaniem i niegodziwym traktowaniem w celach seksualnych sporządzona w Lanzarote dnia 25 października 2007 r., Dz. U. z 2015 r., poz. 608
28. Konwencja o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń sądowych w sprawach cywilnych i handlowych podpisana w Lugano w dniu 30 października 2007 r., Dz. Urz. UE L 147 z dnia 10.06.2009 r.

Prawo innych państw

1. The Code Of Civil Procedure of India, 1908 (Act No. 5 of 1908)
2. Gesetz über Urheberrecht und verwandte Schutzrechte von 09.09.1965
3. Holenderski kodeks karny (1881, amended 1994)
4. Austriacki kodeks karny (österreichisches StGB - 1974)
5. Nouveau Code de procédure civile z dnia 1 stycznia 1976 r., Nouveau Code de Procédure Civile z dnia 1 stycznia 1976 r.,
6. Canadian Criminal Code (R.S.C, 1985, c. C-46)
7. Ustawa o nieautoryzowanym dostępie do komputera nr 128 z 1999 r. (Japonia)
8. Estoński Kodeks Karny z dnia 06.06.2001 (RT I 2001, 61, 364). Wejście w życie 01.09.2002.
9. Niemiecki Kodeksu Postępowania Cywilnego, Zivilprozessordnung (ZPO) Opublikowany 5 grudnia 2005 (Bundesgesetzblatt (BGBl., Federal Law Gazette)
10. An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)
11. Zasadniczy Akt o Cyberbezpieczeństwie Ustawa nr 104 z 2014 r. (Japonia)
12. Protecting Canadians from Online Crime Act (S.C. 2014, c. 31)
13. Cybersecurity Enhancement Act of 2014, P.L. 113-274
14. The National Cybersecurity Protection Act of 2014, Public Law 113-282.
15. Cyber Privacy Fortification Act of 2015. H.R. 104
16. Data Security Act of 2015, H.R. 2205
17. Consumer Privacy Protection Act of 2015, H.R. 2977
18. Cyberthreat Sharing Act of 2015, S. 456

Dokumenty

1. "Zielony Dokument" dotyczący ochrony małoletnich i poszanowania godności ludzkiej w usługach informacyjnych i audiowizualnych, COM(96) 483 final
2. 65 Yearbook of the Institute of International Law z 1993 r.
3. Action Plan 2010-2015 for Canada's Cyber Security Strategy, Canada 2013
4. Amerykańska Deklaracja Praw i Obowiązków Człowieka z kwietnia 1948 r.
5. Biała Księga Komisji Wspólnot Europejskich, Wzrost, konkurencyjność, zatrudnienie (Growth, Competitivness and Employment) 1993
6. Canada's Cyber Security Strategy. For a stronger and more prosperous Canada, Canada 2010
7. Council of Europe, Computer - Realated Crime: Recommendation No. R (89)9 on computer - related crime and final report of the European Committee on Crime Problems, Strasburg 1989
8. Cyber Security Development Action Plan 2016 - 2017, Ministry of Defence of Georgia Cyber Security Bureau, Tbilisi 2016

9. Cyber Security Strategy 2014-2020, Ministry of Economic Affairs and Communication, Tbilisi 2014
10. Cybercrime Convention, Explanatory Report, Budapeszt 2001
11. Cyberstrategia Departamentu Obrony Stanów Zjednoczonych Ameryki, Sekretariat Obrony USA, kwiecień 2015
12. Doktryna Cyberbezpieczeństwa Rzeczpospolitej polskiej 2015, Biuro Bezpieczeństwa Narodowego dnia 22 stycznia 2015
13. ENISA Stategy 2016-2020, Heraklion 2016
14. Europejski Bank Centralny Report on electronic, Frankfurt am Main 1998
15. Europejski Bank Centralny, Virtual Currency Schames, Frankfurt am Main 2012
16. Europol, Cybercrime: improving international cooperation. GCCS2015 - Parallel session 4. Discussion paper, Haga 2015
17. Komunikat Komisji dla Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno - Społecznego i Regionów na temat nielegalnej i szkodliwej treści w Internecie, COM(96) 487
18. Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 20 czerwca 2014 r. Sprawozdanie końcowe z realizacji strategii bezpieczeństwa wewnętrznego UE w latach 2010-2014, COM(2014)0365
19. Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 22 listopada 2010 r. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpiecznej Europy na lata 2010-2014, COM(2010)0673
20. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 31 marca 2011 r. w sprawie ochrony krytycznej infrastruktury informatycznej. Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni, COM(2011)163
21. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22 maja 2007 r. w kierunku ogólnej strategii zwalczania cyberprzestępczości, COM(2007)0267
22. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Komunikat dotyczący realizacji wieloletniego wspólnotowego programu wspierania bezpiecznego korzystania z Internetu i nowych technologii sieciowych (Bezpieczny Internet +), COM/2006/0661 końcowy
23. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie jednolitego rynku telekomunikacyjnego [COM(2013) 634 final z 11.9.2013 - nieopublikowany w Dzienniku Urzędowym]
24. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 30 marca 2009 r. w sprawie ochrony krytycznej infrastruktury informatycznej. Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności, COM(2009)0149
25. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 19 maja 2010 r. zatytułowany Europejska agenda cyfrowa, COM(2010) 245
26. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 11 marca 2014 r. Otwarta i bezpieczna Europa: realizacja założeń, COM(2014)0154

27. Komunikat Komisji do Rady i Parlamentu Europejskiego z dnia 28 marca 2012 r. w sprawie zwalczania przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością, COM(2012)0140
28. Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno – Społecznego oraz Komitetu Regionów dotyczącego „i2010 – Europejskie społeczeństwo informacyjne na rzecz rozwoju wzrostu i zatrudnienia" COM (2005) 229 końcowy
29. Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 31 maja 2006 r. Strategia na rzecz bezpieczeństwa społeczeństwa informacyjnego - Dialog, partnerstwo i przejmowanie inicjatywy, COM(2006)0251
30. Komunikat Komisji Wspólnot Europejskich W kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r., COM(2007)267
31. Komunikat Komisji z dnia 10 maja 2005 r. Program haski: dziesięć priorytetów na najbliższe pięć lat. Partnerstwo na rzecz odnowy europejskiej w dziedzinie wolności, bezpieczeństwa i sprawiedliwości, COM(2005)0184
32. Międzynarodowa Strategia Cyberbezpieczeństwa. Dobrobyt, Bezpieczeństwo i Otwartość w Sieciowym Świecie, Akt wydany przez Prezydenta Stanów Zjednoczonych Ameryki, Waszyngton 2011
33. Narodowa Strategia Bezpieczeństwa USA, Akt wydany przez Prezydenta Stanów Zjednoczonych Ameryki, Waszyngton Luty 2015
34. National Security Concept of the Russian Federation, Zatwierdzone dekretem Prezydenta nr 24 z dnia 10 stycznia 2000 r.
35. OECD Digital Economy Outlook 2015, Paryż 2015
36. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013
37. Powszechna Deklaracja Praw Człowieka, przyjęta i proklamowana rezolucja Zgromadzenia Ogólnego ONZ nr 217 A (III) w dniu 10 grudnia 1948 r.
38. Program Sztokholmski - Otwarta i bezpieczna Europa dla Dobra i Ochrony Obywateli, Dz. Urz. UE C 115 z 04.05.2010 r.
39. Projekt rezolucji Parlamentu Europejskiego z dnia 4 marca 2014 r. w sprawie śródokresowego przeglądu programu sztokholmskiego
40. Ramowa konwencja Narodów Zjednoczonych w sprawie zmian klimatu, sporządzona w Nowym Jorku dnia 9 maja 1992 r., Dz. U. z 1996 r., nr 53, poz. 238
41. Raport CERT Polska z 2012. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne
42. Raport Najwyższej Izby Kontroli, Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP
43. Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/51/628)] 51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law, New York 1996
44. Resolution adopted by the General Assembly, Creation of a global culture of cybersecurity and the protection of critical information infrastructures, A/RES/58/199 z 30.01.2004
45. Resolution adopted by the General Assembly, Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, A/RES/45/121 z 15.12.1990 r.
46. Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP)), Dz. U. C 93 z 09.03.2016 r.
47. Rezolucja Parlamentu Europejskiego z dnia 2 kwietnia 2014 r. sprawie śródokresowego przeglądu programu sztokholmskiego (2013/2024(INI))

48. Rezolucja Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony (2012/2096(INI)), Dz. U. C 419 z 16.12.2015 r.
49. Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2016 r. w sprawie wdrażania wspólnej polityki bezpieczeństwa i obrony (na podstawie sprawozdania rocznego Rady dla Parlamentu Europejskiego na temat wspólnej polityki zagranicznej i bezpieczeństwa), (2016/2067(INI))
50. Rules concerning information, data and intellectual property - ESA/C/89/95 rev. 1.
51. Russia's National Security Strategy to 2020, 12 maja 2009, nr. 537.
52. Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016
53. Strategia Cyberbezpieczeństwa Gruzji na lata 2012 - 2015
54. Strategic Plan of the Commonwealth Telecommunications Organisation (CTO) for the period 2016 – 2020.
55. The Seul Declaration for the Future of the Internet Economy, Seul 2008
56. Ustawa modelowa UNCITRAL o handlu elektronicznym 1996
57. Ustawa modelowa UNCITRAL o podpisach elektronicznych 2001
58. Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 7 lutego 2013 r. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, JOIN(2013)01

Orzecznictwo

Międzynarodowy Trybunał Karny dla byłej Jugosławii

1. Wyrok Międzynarodowego Trybunału Karnego dla byłej Jugosławii z dnia 15 lipca 1999 r., Procecutor przeciwko Tadić, sygn. akt IT-94-1-A

Stały Trybunał Sprawiedliwości Międzynarodowej

1. Wyrok Stałego Trybunału Sprawiedliwości Międzynarodowej, z dnia 7 września 1927 r., sprawa "Lotus" Francja przeciwko Turcji, sygn. akt P.C.I.J. Ser. A, nr 10

Europejski Trybunał Sprawiedliwości

1. Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 16 lipca 2009 r., w sprawie Infopaq International A/S przeciwko Danske Degblades Forening, sygn. akt C-5/08

Trybunał Sprawiedliwości Unii Europejskiej

1. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 7 grudnia 2010 r. w sprawach połączonych C-585/08, Peter Pammer przeciwko Reederei Karl Schluter

GmbH & Co KG, oraz C-144/09, Hotel Alpenhof GesmbH przeciwko Oliverowi Hellerowi, ECR [2010] I-0000
2. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 9 czerwca.2011 r. w sprawie Electrosteel Europe SA przeciwko Edil Centro, SpA, sygn. akt C-87/10
3. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 12 lipca 2011 r., w sprawie L'Oreal S.A. i inni przeciwko eBay International AG i inni, sygn. ak. C-324/09, ECR [2010] I-0000
4. Trybunału Sprawiedliwości Unii Europejskiej z dnia 25 października 2011 r. w sprawach eDate Advertising GmbH przeciwko X (C0509/09) oraz Robert Martinez przeciwko MGN Limited (C-161/10), ECR [2011] I-000Wyrok
5. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 3 kwietnia 2014 r., w sprawie Hi Hotel HCF SARL przeciwko Uwe Spoering, sygn. akt C-387/12
6. Wyrok Trybunału Sprawiedliwości Unii Europejskiej, z dnia 13 maja 2014 r., w sprawie Google Spain SL i Google Inc, sygn. akt C-131/12

Europejski Trybunał Praw Człowieka

1. Wyrok Europejskiego Trybunału Praw Człowieka z dnia z 8 lipca 1986 r., w sprawie Lingens przeciwko Austrii, skarga nr 9815/82
2. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 23 września 1994 r., w sprawie Jersild przeciwko Danii, skarga nr 15890/89
3. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 18 października 2005 r., w sprawie Laurent Perrin przeciwko Wielkiej Brytanii, skarga nr 5446/03
4. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 7 marca 2006 r. w sprawie Evans przeciwko Wielkiej Brytanii, skarga nr 6339/05
5. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 grudnia 2008 r., w sprawie K.U. przeciwko Finlandii, skarga nr 2872/02
6. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10 marca 2009 r., w sprawie Times Newspapers Ltd przeciwko Wielkiej Brytanii, skarga nr 3002/03 oraz 233676/03
7. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10 maja 2011 r. w sprawie Mosley przeciwko Wielkiej Brytanii, skarga nr 48009/08
8. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 16 lipca 2013 r. w sprawie Smolczewski i Węgrzynowski przeciwko Polsce, skarga nr 33846/07
9. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10 października 2013 r. w sprawie Delfi przeciwko Estonii skarga nr 64569/09

Orzeczenia sądów krajowych innych państw

1. Wyrok Sądu Najwyższego USA, z dnia 10 kwietnia 1929 r., United States ex rel. Claussen przeciwko Day, 279 U.S. 398, 401
2. Wyrok Sądu Najwyższego USA, z dnia 20 marca 1984 r., w sprawie Calder przeciwko Jones 465 U.S. 783(1984)
3. Wyrok Apple Computer Inc. przeciwko Microsoft Corp.709 F.Supp. 925, 10 U.S.P.Q.2d (BNA) 1677 (N.D. Cal. 1989), oraz wyrok Lotus Develompment Corporation przeciwko Borland International Inc., 516 U.S. 233 (1996)

4. Wyrok Sądu Rejonowego dla Okręgu Connecticut, z dnia 17 kwietnia 1996 r., Inset Systems, Inc. przeciwko Instruction Set, Inc., sygn. akt 937 F. Supp. 161 (D. Conn. 1996)
5. Wyrok Sądu Apelacyjnego Szóstego Okręgu, z dnia 22 lipca 1996 r., w sprawie Compuserve, Inc. przeciwko Patterson, o sygn. 89 F.3d 1257
6. Wyrok Sądu Okręgowego dla Wschodniego Missouri, z dnia 19 sierpnia 1996 r., Maritz przeciwko Cybergold, 947 F, sygn. akt Supp. 1328 E.D. Mo.1996
7. Wyrok Sądu Rejonowego w Minesocie, z dnia 11 grudnia 1996 r., w sprawie Minnesota przeciwko Granite Gate Resorts, sygn. akt 658 N.W.2d, 718
8. Wyrok Sądu Rejonowego Zachodniej Pensylwanii, z dnia 16 stycznia 1997 r., w sprawie Zippo Manufacturing Co. przeciwko Zippo Dot Com, Inc., o sygn. akt. 952 F. Supp. 1119 (W.D. Pa. 1997)
9. Wyrok Sądu Apelacyjnego House of Lords (1997) z dnia 10 kwietnia 1997 r. w sprawie R. przeciwko Governor of Brixton Prison and another, ex parte Levin (1996) 4 All ER 350, All ER 289
10. Wyrok Sądu Rejonowego w Arizonie, z dnia 2 grudnia 1997 r,, w sprawie Cybersell Inc. przeciwko Cybersell Inc. o sygn. No. 3:00-CV-1268-R (N.D. Tex., N. Div. Mar. 20, 2001)
11. Orzeczenie Sądu Okręgowego w Paryżu z dnia 20 października 2000 r., w sprawie Anit-Semitism LICRA przeciwko Yahoo! Inc., sygn. akt No RG 00/05308
12. Wyrok Sądu Rejonowego w Kansas, z dnia 5 lutego 2002 r. w sprawie Rainy Day Books, Inc. przeciwko Rainy Day Books & Café, L.L.C, o sygn. 186 F.Supp.2d 1158 (2002)
13. Wyrok Sądu Apleacyjnego Piątego Okręgu, z dnia 31 grudnia 2002 r., w sprawie Revell przeciwko Lindov, o sygn. 317 F 3d 467 (2002)
14. Wyrok Sądu Kasacyjnego we Francji, z dnia 9 grudnia 2003 r., Cour de cassation nr 01-03225
15. Wyrok Sądu Apelacyjnego Dziewiątego Obwodu USA z dnia 12 stycznia 2006 r., Wyrok Yahoo! przeciwko La Ligue Contre le Racisme et l'Antisémitisme, 2006 WL 60670 (9th Cir. 2006) C-00-21275 JF
16. Wyrok Cour d'appel w Paryżu, z dnia 27 września 2006 r., nr 04-20185
17. Wyrok Trybunału Sprawiedliwości z dnia 22 grudnia 2010 r. Bezpečnostní softwarová asociace - Svaz softwarové ochrany przeciwko Ministerstwo Kultury, sygn. akt C-393/09

Wykaz literatury

1. Adamski A., *Cyberprzestępczość - aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4
2. Adamski A., *Podstawy jurysdykcji cyberprzestępstw w prawie porównawczym*, [w:] T. Jasudowicz, M. Balcerzak (red.), *Księga pamiątkowa ku czci Profesora Jana Białocerkiewicza,* t. 2, Toruń 2009
3. Adamski A., *Prawo karne komputerowe*, Warszawa 2000
4. Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001
5. Akińcza J., *Stalking - zjawisko, odpowiedzialność karna*, „Jurysta" 2012, nr 12

6. Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15
7. Aleksandrowicz T.R., K. Liedel, *Społeczeństwo informacyjne - sieć - cyberprzestrzeń. Nowe zagrożenia*, [w:] K. Liedel, P. Piasecka, T.A. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna pokój i terroryzm w epoce informacji*, Warszawa 2014
8. Arguilla J., D. Ronfeldt, *The Advent of Netwar*, [w:] J. Arguilla, D. Ronfeldt (red.), *Networks and Netwars. The Future of Terror, Crime and Militancy*, Santa Monica 2009
9. Babis H., *Internet*, [w:] E. Cała-Wacinkiewicz (red.), *Encyklopedia zagadnień międzynarodowych*, Warszawa 2011
10. Bagdan-Kurluta K., *Podmioty prawa międzynarodowego*, [w:] B. Wierzbicki (red.), *Prawo międzynarodowe publiczne*, Białystok 2001
11. Balcerzyk J. (red.), *Dobra osobiste w XXI wieku. Nowe wartości, zasady, technologie*, Warszawa 2012
12. Bar G., D. Klimas, *Treść cyfrowa w obrocie konsumenckim*, [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
13. Bar G., *Elektroniczne świadczenie w obrocie profesjonalnym*, Wrocław 2012
14. Baranowska M. B., *Bitcoin. Nowa waluta i nowe wyzwania dla organów ścigania,* „Studia prawnoustrojowe" 2016, t. 31
15. Barcik J., *Akt terrorystyczny i jego sprawca w świetle prawa międzynarodowego i wewnętrznego*, Warszawa 2004
16. Barcik J., *Charakter prawny ACTA w prawie międzynarodowym i prawie Unii Europejskiej,* „Studia Prawnicze KUL" 2013, nr 3
17. Barcik J., *Dostęp do dokumentów Unii Europejskiej: na kanwie negocjacji umowy ACTA*, „Państwo i Prawo" 2013, z. 1
18. Barcik J., *Międzynarodowe prawo morza*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne,* wyd. 2, Warszawa 2014
19. Barcik J., *Nowe formy podmiotowości prawnomiędzynarodowej na przykładzie partnerstw publiczno-prywatnych*, [w:] K. Karski (red.), *Kierunki rozwoju współczesnego prawa międzynarodowego*, Warszawa 2015
20. Barcik J., *Zagadnienia ogólne*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2014
21. Barlow J.P., *Deklaracja Niepodległości Cyberprzestrzeni*, przekład J. Staniszewski [w:] „Magazyn Internetowy WWW" 2000, listopad
22. Barta J., R. Markiewicz, *Oprogramowanie open source w świetle prawa. Między własnością a wolnością*, Kraków 2005
23. Barta J., R. Markiewicz, *Prawo autorskie i prawa pokrewne*, Warszawa 2014
24. Barta J., R. Markiewicz, *Prawo cyberprzestrzeni i stare konwencje*, „Rzeczpospolita" 1997, 15 listopada
25. Barta J., R. Markiewicz. *Prawo autorskie*, Warszawa 2016
26. Bator A. i in., *Integracja i globalizacja z perspektywy filozofii prawa*, [w:] J. Stelmach (red.), *Filozofia prawa wobec globalizmu*, Kraków 2003
27. Bednarek J., A. Andrzejewska, *Cyberświat - możliwości i zagrożenia*, Warszawa 2009
28. Bekkers V., B.J. Koops, S. Nouwt (red.) *Emerging Electronic Highways: New Challenges for Politics and Law*, Haga-Boston-Londyn 1995
29. Benoliel D., *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistomology*, "California Law Review" 2004, nr 92
30. Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2

31. Białkowski M., *Niszczenie danych i programów komputerowych,* „Gazeta Sądowa" 2002, nr 7/8
32. Białocerkiewicz J., *Prawo międzynarodowe publiczne. Zarys wykładu*, Toruń 2007
33. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI w. - zarys problematyki*, Warszawa 2011
34. Biczysko-Pudełko K., *Znaczenie soft law dla regulacji cloud computing,* [w:] *Media elektroniczne. Współczesne problemy prawne,* K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
35. Biegel S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Cambridge (Massachusetts) 2001
36. Bielak-Jomaa E., *Źródła prawa ochrony danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba i in., *Prawo ochrony danych osobowych*, Warszawa 2013
37. Bienias M., *Prawo właściwe i jurysdykcja w usługach świadczonych drogą elektroniczną*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2012 , nr 4
38. Bienias T., *Internet*, Kraków 1998
39. Bierzanek R., *Zarys historii prawa międzynarodowego*, [w:] R. Bierzanek, J. Symonides (red.), *Prawo międzynarodowe publiczne*, Warszawa 2005
40. Błażiwska N., *Konwencja UNICITRAL o wykorzystywaniu komunikacji elektronicznej w kontraktach międzynarodowych a ustawodawstwo ukraińskie*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych*, Warszawa 2008
41. Bohaczewski M., *Jurysdykcja krajowa w sprawie o naruszenie praw własności intelektualnej w internecie na tle orzecznictwa francuskiego*, [w:] A. Sztoldman (red), *Prawo wobec innowacji technologicznych*, Warszawa 2013
42. Boister N., *An Introduction to Transnational Criminal Law*, Oxford 2012
43. Bolechów B., *Sieci przeciwko hierarchiom - wyzwanie dla suwerenności państw*, [w:] Z. Leszczyński, S. Sadowski (red.), *Suwerenność państwa we współczesnych stosunkach międzynarodowych*, Warszawa 2005
44. Bollee S., B. Haftel, *Les nouveaux (des) equilibres de la competence internationale en matiere de cyberdelits apres l'arret eDateAdvertising et Martinez*, "Recueil Dalloz" 2012, nr 20
45. Bonnici M., J. Pia, *Self - regulation in cyberspace*, "Information Technology & Law Series" 2008, nr 16
46. Brenner S. W., B. Jaap Koops, *Approaches to Cybercrime Jurisdiction*, "Journal of High Technology Law" 2004, t. 1
47. Broadhurst R., K. Kwang, R. Choo, *Cybercrime and online safety in cyberspace*, [w:] C.J. Smith, S.X. Zgang, R. Barberet (red.), *Routledge Handbook of International Criminology*, Londyn-Nowy York
48. Bryła J., *Wkład Unii Europejskiej w rozwój międzynarodowego reżimu kosmicznego*, „Rocznik Integracji Europejskiej" 2015, nr 9
49. Brzozowska M., *Ochrona danych osobowych w sieci*, Wrocław 2012
50. Brzozowska M., *Ochrona danych osobowych w sieci*, Wrocław 2012 Balcerzyk J. (red.), *Dobra osobiste w XXI wieku. Nowe wartości, zasady, technologie,* Warszawa 2012
51. Brzozowski A., *Komentarz do art. 66^1 k.c,* [w:] K. Pietrzykowski (red.), *Kodeks cywilny. Komentarz. Art. 1-449^{10}*, t. 1, Warszawa 2015
52. Bukowski S., *Ataki hackerskie, Próba analizy prawno - karnej*, „Gazeta Sądowa" 2003, nr 7/8
53. Całus A., *Szansa unifikacji prawa właściwego dla zobowiązań z "deliktów elektronicznych" w ramach Unii Europejskiej*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych. Materiały z konferencji*, Warszawa 2008

54. Cassese A., *International Criminal Law*, Oxford 2003
55. Cassese A., *International Law*, Oxford 2005
56. Chałubińska-Jentkiewicz K., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015
57. Chałubińska - Jentkiewicz K., *Własność intelektualna jako szczególny rodzaj własności w „sieci",* [w:] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015
58. Chałubińska - Jentkiewicz K., *Wstęp,* [w:] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015
59. Chałubińska-Jentkiewicz K., M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015
60. Chałubińska-Jentkiewicz K., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015
61. Chmura R., *Kodeks Internetu*, [w:] R. Skubisz (red.), *Internet 2000 prawo - ekonomia-kultura*, Lublin 2000
62. Chrabonszczewska E., *Bitcoin - nowa wirtualna globalna waluta?*, „Zeszyty Naukowe Kolegium Gospodarki Światowej SGH" 2013, nr 40
63. Cieślak M., *Polskie prawo karne. Zarys systemowego ujęcia*, Warszawa 1994
64. Clough J., *Principles of cybercrime*, New York 2010
65. Cłapka F., *Internet jako wyzwanie dla współczesnych systemów prawa*, [w:] E. Galewska, S. Kotecka (red.), *X-lecie Księga pamiątkowa z okazji dziesięciolecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego - Blok Prawa Komputerowego*, Wrocław 2012
66. Collier M., *Estonia: Cyber Superpower*, "Transitions Online" 2007, nr 12/18
67. Cyman D., *Elektroniczne instrumenty płatnicze a bezpieczeństwo uczestników rynku finansowego*, Warszawa 2013
68. Cyman D., *Pojęcie pieniądza i kierunki jego rozwoju*, [w:] Z. Ofiarski (red.), *XXV lat przeobrażeń w prawie finansowym i prawie podatkowym - ocena dokonań i wnioski na przyszłość*, Szczecin 2014
69. Czapielewski M., *Cyberterroryzm jako element społeczeństwa informacyjnego (na przykładzie Estonii),* [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioły, J. Kisielińskiego, K. Rakchela (red.), Warszawa 2009
70. Czaplicki K., *Kradzież tożsamości w Internecie*, [w:] G. Szpor (red.), *Internet. Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011
71. Czapliński W., A. Wyrozumska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2014
72. Czechowski R., P. Sienkiewicz *Przestępcze oblicza komputerów,* Warszawa 1993
73. Czekalska J., *Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych*, „Państwo i Prawo" 2004, nr 11
74. Czosseck C., R. Ottis, A. Talihärm, *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*, "International Journal of Cyber Warfare and Terrorism", t. 1, nr 1
75. Czyżak M., *Strategie zwalczania cyberterroryzmu - aspekty prawne*, [w:] A. Podraza (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013
76. Dereń J., A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa 2004
77. Dobrzeniecki K., *Autonomiczne prawo cyberprzestrzeni: mit czy rzeczywistość?*, [w:] O. Bogucki, S. Czepita (red.), *System prawny a porządek prawny*, Szczecin 2008

78. Dobrzeniecki K., *Lex informatica*, Toruń 2008
79. Dobrzeniecki K., *Prawo a etos cyberprzestrzeni*, Toruń 2004
80. Draczyk Ł., *Strona internetowa w świetle prawa autorskiego*, „Prace z Prawa Własności Intelektualnej" 2015, z. 2 (128)
81. Drzewicki K., *Idea wspólnego dziedzictwa ludzkości a prawa człowieka*, „Przegląd Stosunków Międzynarodowych" 1982, nr 1/3
82. Dubber M.D., *Comparative Criminal Law*, [w:] M. Reimann, R. Zimmermann (red.), *The Oxford Handbook of Comparative Law*, Oxford 2006
83. Duda M., *Przestępstwa z nienawiści. Studium prawnokarne i kryminologiczne*, Podlewska J., O. Trocha, *Ochrona prawna małoletnich - kierunki przemian prawa i postępowania karnego, zagadnienia wybrane*, „Dziecko Krzywdzone" 2012, nr 2(39)
84. Dziura Ł., *Internet ostoją wolności słowa, czyli jak regulować, aby nie zaszkodzić*, [w:] *Prawa człowieka. Współczesne zjawiska, wyzwania, zagrożenia - Materiały konferencyjne*, t. 2., A. Kalisz (red.), Sosnowiec 2015
85. Ereciński T., *Kilka uwag o tzw. jurysdykcji koniecznej*, [w:] L. Ogiełła, W. Popiołek (red)., *Księga pamiątkowa Profesora Maksymiliana Pazdana*, Kraków 2005
86. Ervin S., *Law in a Vacuum: The Common Heritage Doctrine in Outer Space Law*, "Boston Collage International and Comparative Law Review" 1984, t. 7, nr 2
87. Fajgielski P., *Przetwarzanie danych osobowych w serwisach społecznościowych - wybrane aspekty prawne*, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016
88. Fajgielski P., *Rozwój technologii informacyjnych i komunikacyjnych oraz związanych z nimi zagrożeń - wybrane aspekty prawne*, [w:] R. Wieruszewski (red.), *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010
89. Ferenc-Szydełko E. (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2014
90. Fischer B., *Przestępstwa komputerowe, ochrona informacji. Aspekty prawno – kryminalistyczne*, Kraków 2000
91. Fischer B., *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich*, Warszawa 2010
92. Flisak D., *Utwór multimedialny w prawie autorskim*, Warszawa 2008
93. Frączek B., *Pieniądz elektroniczny - próby zdefiniowania i sklasyfikowania*, „Bank i Kredyt" 2004, nr 4
94. Gadecki B., *Ochrona podwodnego dziedzictwa kultury*, „Państwo i Prawo" 2015, nr 9
95. Gadkowski T., *Koncepcja wspólnego dziedzictwa ludzkości w międzynarodowym prawie morza*, „Prace Instytutu Nauk Społecznych WSI" 1986, nr 6
96. Gadkowski T., *Prawo do wspólnego dziedzictwa ludzkości,* [w:] *Prawa człowieka. Model prawny*, R. Wieruszewski (red.), Wrocław 1991
97. Gajda A., S. Gajda, *Prawne aspekty ścigania użytkowników sieci P2P w Polsce*, [w:] J. Kosiński (red.), *Internetowe naruszenia własności intelektualnej*, Szczytno 2015
98. Galicki Z., *Rozwój zasad odpowiedzialności międzynarodowej za działania kosmiczne*, [w:] A. Wasilkowski (red.), *Działalność kosmiczna w świetle prawa międzynarodowego*, Warszawa 1991
99. Garlicki L., *Polskie prawo konstytucyjne*, Warszawa 2003
100. Giaro M., *Zawarcie umowy w trybie aukcji internetowej*, Warszawa 2014
101. Gienas K., *Cyberprzestępczość*, „Jurysta" 2003, nr 12
102. Gilas J., *Prawo międzynarodowe*, Toruń 1995
103. Giles K., *Russia's Public Stance on Cyberspace Issues*, [w:] C. Chosseck, R. Ottis, K. Ziolkowski (red.), *2012 4th International Conference on Cyber Conflict*, Talin 2012

104. Gizicki W., *Państwo wobec cyberterroryzmu*, [w:] A. Podraza (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013
105. Golat R., *Internet - aspekty prawne*, Warszawa 2003
106. Gołaczyński J. (red.), *Jurysdykcja, uznawanie orzeczeń sądowych oraz ich wykonywanie w sprawach cywilnych i handlowych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012. Komentarz*, Warszawa 2015
107. Gołaczyński J., *Umowy elektroniczne - próba definicji*, [w:] J. Gołaczyński (red.), *Umowy elektroniczne w obrocie gospodarczym*, Warszawa 2005
108. Gołaczyński J., *Umowy elektroniczne w prawie prywatnym międzynarodowym*, Warszawa 2007
109. Gołaczyński J., *Umowy elektroniczne w prawie wybranych państw*, [w:] J. Gołaczyński (red.), *Umowy elektroniczne w obrocie gospodarczym*, Warszawa 2005
110. Gołaczyński J., *Wpływ rozporządzenia eIDAS na polskie prawo prywatne. Wybrane zagadnienia,* [w:] *Media elektroniczne. Współczesne problemy prawne,* K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
111. Gończ E., *Jak chronić środowisko naturalne?,* [w:] Z. Brodecki (red.), *Ochrona środowiska*, Warszawa 2015
112. Goździaszek Ł., *Cywilnoprawne granice swobody wypowiedzi w Internecie*, Warszawa 2015
113. Góralczyk W., S. Sawicki, *Prawo międzynarodowe publiczne w zarysie*, Warszawa 2007
114. Góralczyk W., S. Sawicki, *Prawo międzynarodowe publiczne w zarysie.* Warszawa 2013
115. Góralczyk W., S. Sawicki, *Prawo międzynarodowe publiczne w zarysie*, Warszawa 2015
116. Góreczny N., *Wtórny rynek cyfrowych kopii programów komputerowych. Wprowadzenie do obrotu i wyczerpanie prawa w kontekście cyfrowej dystrybucji*, „Zeszyty Naukowe Prawa Własności Intelektualnej Uniwersytetu Śląskiego" 2013, z. 1
117. Górska A., *Bezpieczeństwo a aterytorialność cyberprzestrzeni*, „Prace Naukowe Wyższej Szkoły Bankowej w Gdańsku" 2014, t. 33
118. Górski M., *Zagadnienia wprowadzające*, [w:] M. Górski (red.) *Prawo ochrony środowiska*, Warszawa 2009
119. Gregor B., M. Stawiszyński, *e-Commerce*, Bydgoszcz - Łódź 2002
120. Gronkowska B., T. Jasudowicz, *Prawa człowieka i ich ochrona*, Toruń 2005
121. Grzelak A., T. Ostropolski, *Współpraca wymiarów sprawiedliwości w sprawach karnych i współpraca policyjna,* t. 9, cz. 1, Warszawa 2011
122. Grzelak M., K. Lidel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski - zarys problemu*, „Bezpieczeństwo narodowe" 2012, nr 22
123. Guo J., A. Chow, *Virtual Money System: a Phenomenal Analysis*, [w:] 10th IEEE International Conference on E-Commerce Technology (CEC 2008)/5th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services, IEEE, Waszyngton 2008
124. Gvosdev N. K., *The Bear Goes Digital. Russia and Its Cyber Capabilities*, [w:] D.S. Reveron (red.), *Cyberspace and national security. Threats, Opportunities and Power in a Virtual World*, Waszyngton 2012
125. Hałuszczak M., *Wybrane problemy cloud computing z perspektywy polskiej regulacji ochrony danych osobowych*, „Zeszyty Naukowe Prawa Własności Intelektualnej Uniwersytetu Śląskiego" 2013, z. 1
126. Hang L.Q., *Online Dispute Resolution System: The Future of Cyberspace Law*, "Santa Clara Law Review" 2001, t. 41, nr 3

127. Hardy I.T, *The Proper Legal Regime for Cyberspace*, "University of Pittsburgh Law Review" 1994, nr 55
128. Hert P. de, *Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - whose Sovertrignty is at stake*?, [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, „Information Technology & Law Series" 2006, t. 11
129. Hirschson D., T. Lewis, *European E-cash rules at the front*, „ITLR" 2001, nr 5
130. Hofmański P., *Komentarz do art. 122 k.k.* [w:] M. Filar (red.), *Kodeks karny. Komentarz*, Warszawa 2010
131. Hofmokl J., *Internet jako nowe dobro wspólne*, Warszawa 2009
132. Holland H.B., *The Failure of The Rule of Law in Cyberspace?: Reorienting The Normative Debate on Borders and Territorial Sovereignty*, "The John Marshall Journal of Computer & Information Law" 2005, t. 24, nr 1
133. Hołda Z., *Prawa człowieka. Wiadomości wstępne* [w:] J. Hołda, Z. Hołda, D. Ostrowska, J.A. Rybczyńska, *Prawa człowieka. Zarys wykładu*, Warszawa 2014
134. Hołyst B., J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1
135. Hołyst B., *Kryminologia*, Warszawa 2007
136. Hołyst B., *Podsłuchiwanie i inwigilacja użytkowników mediów elektronicznych w kontekście bezpieczeństwa informacyjnego*, „Prokuratura i Prawo" 2015, nr 3
137. Hołyst B., *Policja na świecie*, Warszawa 2013
138. Hołyst B., *Terroryzm*, t. 1, Warszawa 2011
139. Huczkowski M., *Ochrona autorskich praw osobistych w powszechnym prawie międzynarodowym*, Warszawa 2013
140. Inkster N., *China in Cyberspace*, [w:] D.S. Reveron, *Cyberspace and national security. Threats, Opportunities and Power in a Virtual World*, Waszyngton 2012
141. Jabłoński M., K. Wygoda, *Prawa człowieka w komunikacji elektronicznej*, [w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003
142. Jacyszyn J., S. Zakrzewski, *Podpis elektroniczny jako element systemu zabezpieczenia danych w sieci*, cz. 2, „Rejent" 2001, nr 11
143. Jagielska M., I. Rauch, *Klauzule abuzywne w umowach standardowo zawieranych przez Internet*, [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
144. Jagiełło D., *Cyberterroryzm*, „Edukacja Prawnicza" 2015, nr 5
145. Jaishankar K., *Identity related Crime in the Cyberspace: Examining Phishing and its impact*, "International Journal of Cyber Criminology" 2008, t. 2, nr 1
146. Jakubski K.J., *Przestępczość komputerowa - zarys problematyki*, „Prokuratura i Prawo" 2006, nr 12
147. Janowicz R., *Pieniądz elektroniczny w wybranych krajach - charakterystyka, główne funkcje i zastosowanie*, „Bank i Kredyt" 2005, nr 1
148. Janowicz R., R. Klepacz, *Pieniądz elektroniczny na świecie. Istota i zastosowanie elektronicznej portmonetki*, Warszawa 2002
149. Janowski J., *Cybernetyzacja prawa*, [w:] E. Gulewska, S. Kotecka (red.), *X-lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego*, Warszawa 2012
150. Janowski J., *Informatyka prawa. Zadania i znaczenie w związku z kształtowaniem się elektronicznego obrotu prawnego*, Warszawa 2011
151. Janowski J., *Kontrakty elektroniczne w obrocie prawnym*, Warszawa 2008

152. Janowski J., *Podpis elektroniczny w obrocie prawnym*, Warszawa 2007
153. Janyst T., *Charakter prawny wirtualnych pieniędzy i formy ich regulacji. Analiza prawnoporównawcza*, [w:] A. Sztoldman (red.), *Prawo wobec innowacji technologicznych*, Warszawa 2013
154. Jaroszek A., *Prawo właściwe dla umów konsumenckich zawieranych przez Internet*, Warszawa 2009
155. Jastrzębski M., *Międzynarodowe i polskie standardy wolności wypowiedzi a postanowienia umowy ACTA*, [w:] M. Jastrzębski, T. Kuczur (red.), *Bezpieczeństwo państwa a wolność jednostki. Wybrane aspekty prawne i polityczne*, Toruń 2013
156. Jeżewski M., *Uniwersalna jurysdykcja karna w prawie międzynarodowym*, „Kwartalnik Prawa Publicznego" 2003, nr 2
157. Johnson D.R., D. Post, *Law and Borders - The Rise of Law in Cyberspace*, „Stanford Law Review" 1996, t. 48, nr 5
158. Joyner J., *Comparing Transatlantic Versions of Cybersecurity*, [w:] D.S. Reveron, *Cyberspace and national security. Threats, Opportunities and Power in a Virtual World*, Waszyngton 2012
159. Kacker U., T. Saluja, *Online Arbitration For Resolving E-Commerce Disputes. Gateway to The Future*, "Indian Journal of Arbitration Law" 2014, t. 3, nr 1
160. Kamiński I.C., Z. Warso, *Czy można zniknąć z Google'a? Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos i Mario Costeja González* (C-131/12), [w:] D. Bychawska-Sinarska, D. Głowacka (red.), *Wirtualne media - realne problemy*, Warszawa 2014
161. Kańciak A., *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8
162. Karavas V., G. Teubner, *The Horizontal Effect of Fundamental Rights on 'Private Parties' within Autonomous Internet Law*, "German Law Journal" 2003, nr 4 (12)
163. Karpiuk M., *Ochrona danych osobowych na gruncie regulacji Unii Europejskiej*, [w:] M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015
164. Karpiuk M., *Prawo do prywatności w warunkach nowych technologii,* [w:] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015
165. Karska E. (red.), *Prawa dziecka w prawie międzynarodowym*, Warszawa 2014
166. Karska E., *Dorobek Konferencji Rewizyjnej Statutu MTK ze szczególnym uwzględnieniem poprawki definiującej zbrodnię agresji*, „Kwartalnik Prawa Publicznego" 2010, nr 10/3
167. Karska E., *Karna jurysdykcja krajowa a międzynarodowa*, [w:] J. Kolasa (red.), *Współczesne sądownictwo międzynarodowe. Wybrane zagadnienia prawne*, t. 2, Wrocław 2010
168. Karska E., *Subsydiarność uchwał organizacji rządowych i pozarządowych w jurysdykcji międzynarodowych trybunałów karnych*, Wrocław 2009
169. Karski K., *Problem Statutu korporacji ponadnarodowych w prawie międzynarodowym (globalizacja a podmiotowość prawa międzynarodowego)*, [w:] E. Dynia (red.), *Nauka prawa międzynarodowego u progu XX wieku. Materiały pokonferencyjne*, Rzeszów 2003
170. Karwala D., *Dostępność przekazów internetowych jako podstaw jurysdykcji krajowej*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych. Materiały z konferencji*, Warszawa 2008

171. Kaspersen H.W.K., *Jurisdiction in the Cybercrime Convention*, B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, nr 11
172. Kasprzak W. - *Zagrożenie bezpieczeństwa cyfrowego Polski na przykładzie cyberwojny w Estonii*, „Studia prawnoustrojowe" 2016, t. 31
173. Kasprzak W.A., *Ślady cyfrowe. Studium prawno - kryminalistyczne,* Warszawa 2015
174. Kępa L., *Ochrona danych osobowych w praktyce*, Warszawa 2014
175. Kiedrowicz-Wywiał A., *Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6
176. Kilian W., *Umowy elektroniczne w prawie międzynarodowym*, [w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003
177. Klimas D., *Obowiązki informacyjne przedsiębiorców w umowach B2C e-commerce - wybrane aspekty*, [w:] E. Galewska (red.), *Wybrane aspekty prawa nowych technologii: publikacja studenckiego koła naukowego „Blok prawa komputerowego",* cz. 3, Wrocław 2015
178. Klimas D., *Odpowiedzialność licencjodawcy za wady programu komputerowego w prawie autorskim i prawie zobowiązań,* [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
179. Kocot W.J., *Wpływ Internetu na prawo umów*, Warszawa 2004
180. Konarski X., *Obowiązki pośredników internetowych w związku z rozpowszechnianiem bezprawnych treści,* [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
181. Koops B.J., S. Brenner, *Cybercrime jurisdiction - an introduction,* [w:] B.J. Koops, S.W. Brenner (red.), *Cybercrime and Jurisdiction. A global survey,* "Information Technology & Law Series" 2006, nr 11
182. Korns S.W., J.E. Kastenberg, *Georgia's Cyber Left Hook*, "Parameters", Winter 2008-2009 Issue
183. Korus K., *Oświadczenie woli w postaci elektronicznej i podpis elektroniczny*, [w:] M. Chudzik i in. (red.), *Prawo handlu elektronicznego*, Bydgoszcz-Kraków 2005
184. Kosińska J., *Prawnokarna problematyka stalkingu*, „Prokuratura i Prawo" 2008, nr 10
185. Kosiński J., *Cyberprzestępczość*, [w:] W. Jasiński (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013
186. Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015
187. Kosiński J., *Wstęp*, [w:] J. Kosiński (red.), *Internetowe naruszenia własności intelektualnej 2015*, Szczytno 2016
188. Kościółek A., *Wpływ rozporządzenia eIDAS na skuteczność elektronicznych pism procesowych w postępowaniu cywilnym,* [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
189. Kot D., M. Świerczyński, *Prawo właściwe i jurysdykcja krajowa dla stosunków gospodarczych w Internecie*, [w:] J. Barta, R. Markiewicz, *Handel elektroniczny. Prawne problemy*, Kraków 2005
190. Kotarba W., *Ochrona własności intelektualnej*, Warszawa 2012
191. Kotecka S., *Aukcja elektroniczna w polskim prawie zamówień publicznych i nowych unijnych dyrektywach zamówieniowych*, „Monitor Prawniczy" 2005, nr 6, dodatek „Prawo Mediów Elektronicznych" nr 2
192. Kowal J. (red.), *Wstęp do Internetu*, Wrocław 2000
193. Kowalczuk-Szymańska M., O. Sztejnert-Roszak, *Naruszenia praw autorskich w Internecie,* Warszawa 2011

194. Kowalik P., D. Wociór, *Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego*, [w:] A. Balicki, P. Barta, M. Byczkowski i in., *Ochrona danych osobowych w sektorze publicznym*, Warszawa 2016
195. Kowalik-Bańczyk K., *Sposoby regulacji handlu elektronicznego w prawie wspólnotowym i międzynarodowym*, Kraków 2006
196. Kowalska S., *Prawa człowieka a terror i terroryzm*, Kalisz 2008
197. Kramska M., *Międzynarodowe i europejskie standardy ochrony genomu ludzkiego a preimplantacyjna diagnostyka genetyczna*, „Prawo i medycyna" 2011, nr 3
198. Krekora-Zając D., *Istota i charakter prawny danych genetycznych*, „Prawo i medycyna" 2015, nr 4
199. Krzysztofek M., *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy" 2012, nr 9
200. Kulesza J., *Ius internet. Między prawem a etyką*, Warszawa 2010
201. Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010
202. Kulesza J., *Odpowiedzialność państw za podejmowane w cyberprzestrzeni działania zagrażające międzynarodowemu pokojowi i bezpieczeństwu*, „Studia Prawno – Ekonomiczne" 2011, t. 83
203. Kulesza J., *Projekt Ramowej Konwencji Internetu*, „Państwo i Prawo" 2009, z. 10
204. Kulik M., *Zmiana przepisów dotyczących przedawnienia wprowadzone ustawą z dnia 20 lutego 2015 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*, „Annales Universitatis Mariae Curie - Skłodowska" 2016, t. 63
205. Kułaga Ł., *Przestrzeń kosmiczna - jako wspólne dziedzictwo ludzkości. Kontrowersje wokół Porozumienia regulującego działalność państw na Księżycu i innych ciałach niebieskich*, [w:] Z. Galicki, T. Kamiński, K. Myszona - Kostrzewa, *Wykorzystanie przestrzeni kosmicznej. Świat - Europa - Polska*, Warszawa 2010
206. Kun-Buczko M., *Prawo międzynarodowe publiczne. Zarys problematyki*, Białystok 2011
207. Kun-Buczko M., *Zagadnienia wstępne*, [w:] M. Kun-Buczko, *Prawo międzynarodowe publiczne. Zarys problematyki*, Białystok 2011
208. Kun-Buczko, M. Wenclik, *Międzynarodowa ochrona praw człowieka*, [w:] M. Kun - Buczko, *Prawo* M. *międzynarodowe publiczne. Zarys problematyki*, Białystok 2011
209. Kunicki I., *Podmioty procesu*, [w:] W. Broniewicz, A. Marciniak i in., *Postępowanie cywilne w zarysie*, Warszawa 2014
210. Kurek R., *Alternatywne waluty wirtualne*, „Annales Universitatis Mariae Curie - Skłodowska" 2014, t. 48, nr 3
211. Kurowski W., *Mafia 2.0. Jak organizacje przestępcze kreują wartość w erze cyfrowej*, Warszawa 2015
212. Kurzępa E., *Ochrona baz danych*, [w:] B. Kurzępa, E. Kurzępa, *Ochrona własności intelektualnej. Zarys problematyki*, Toruń 2010
213. Lach A., *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3
214. Lach A., *Przestępczość komputerowa*, [w:] A. Grzelak (red.), *Europejskie Prawo Karne*, Warszawa 2012
215. Lachow I., C. Richardson, *Terrorist use of the internet. The real story*, "Joint Force Quarterly" 2007, nr 45
216. Lakomy M., *Polityka cyberbezpieczeństwa Sojuszu Północnoatlantyckiego*, „Przegląd Zachodni" 2013, nr 4
217. Lerdeux G., *La competence internationale des tribunaux francais en matiere de cyberdelits*, „Recueil Dalloz" 2010, nr 19
218. Lessig L., *Wolna kultura*, Warszawa 2005

219. Levy P., *Drugi potop*, [w:] M. Hopfinger (red.) *Nowe media w komunikacji społecznej w XX wieku. Antologia*, Warszawa, 2002
220. Levy P., *Drugi potop*, „Magazyn Sztuki" 1997, nr 1/2
221. Lewandowski K., *Big Four - Kluczowe aspekty globalnej polityki Internetu*, [w:] A. Andrzejewska, J. Bednarski, S. Ćmiel (red.), *Człowiek w świecie rzeczywistym i wirtualnym. Wybrane patologie społeczno - wychowawcze w cyberprzestrzeni*, Jozefów 2013
222. Lichocki E., *Cyberterroryzm państwowy i niepaństwowy - początki, skutki i formy*, [w:] M.J. Malinowski (red.), *Ewolucja terroryzmu na przełomie XX i XXI wieku*, Gdańsk 2009
223. Lisowska Z., *Ochrona prawa do wizerunku w Internecie*, [w:] E. Galewska (red.), *Wybrane aspekty prawa nowych technologii: publikacja studenckiego koła naukowego „Blok prawa komputerowego",* cz. 3, Wrocław 2015
224. Littlejohn Shinder D., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci,* Gliwice 2004
225. Litwiński P., *Nowe rozporządzenie ogólne w sprawie ochrony danych osobowych i jego wpływ na społeczeństwo informacyjne. Wybrane zagadnienia,* [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
226. Loiseau H., L. Lemay, *Canada's Cyber Security Policy: a Tortuous Path Toward a Cyber Security Strategy*, [w:] E. Ventre (red.), *Cyber Conflict. Competing National Perspectives*, Londyn 2012
227. Lubasz D., *Handel elektroniczny. Bariery prawne*, Warszawa 2013
228. Lubasz D., K. Witkowska, *Europejska reforma ochrony danych osobowych z perspektywy pełnomocnika przedsiębiorcy,* [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
229. Łukaszuk L., *Działalność związana z kosmosem a międzynarodowa ochrona własności intelektualnej - wybrane zaganiania,* [w:] J. Menkes, *Prawo Międzynarodowe. Księga pamiątkowa prof. Renaty Szafarz*, Warszawa 2007
230. Łukaszuk L., *Prawo kosmiczne - z europejskiej perspektywy. Kierunki rozwoju i dziedziny zastosowania,* [w:] Z. Galicki, T. Kamiński, K. Myszona - Kostrzewa, *Wykorzystanie przestrzeni kosmicznej. Świat - Europa - Polska,* Warszawa 2010
231. Łukaszuk L., *Współpraca i spory międzynarodowe na morzach. Wybrane zagadnienia prawa, polityki morskiej i ochrony środowiska*, Warszawa 2009
232. Macedo S., *Universal Jurisdiction. National Courts and the Prosecution of Serious Crimes under International Law* [za:] M. Znojek, *Kilka uwag o zarzutach podnoszonych wobec jurysdykcji uniwersalnej*, „Kwartalnik Prawa Publicznego" 2007, nr 3
233. Machała W., *Licencja mieszana? Prawnoautorskie aspekty obrotu programami komputerowymi stworzonymi z wykorzystaniem oprogramowania o otwartym kodzie*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej" 2010, z. 1
234. Machanowski J., *Stan i perspektywy rozwoju międzynarodowego prawa polarnego (próba systematyzacji)*, [w:] K. Lankosz (red.), *Aktualne problemy prawa międzynarodowego we współczesnym świecie. Księga pamiątkowa poświęcona pamięci Profesora Mariana Iwanejko*, Kraków 1995
235. Machowska A., *Postępowanie cywilne*, [w:] A. Machowska, K. Wojtyczek (red.) *Prawo francuskie*, t. 1 Kraków 2004
236. Machowski J., *Problemy prawne ochrony środowiska*, Warszawa 2000

237. Machowski J., *Stan i perspektywy rozwoju międzynarodowego prawa polarnego (próba systematyzacji)*, [w:] K. Lankosz (red.), *Aktualne problemy prawa międzynarodowego we współczesnym świecie. Księga pamiątkowa poświęcona pamięci Profesora Mariana Iwanejko*, Kraków 1995
238. Machowski P., *Komentarz do art. 66 k.c.*, [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks Cywilny Komentarz*, Warszawa 2016
239. Maciejewska-Szałas M., *Forma pisemna i elektroniczna czynności prawnych. Studium prawnoporównawcze*, Warszawa 2014
240. Maciejewska-Szałas M., *Podpis elektroniczny w prawie Wielkiej Brytanii*, „Gdańskie Studia Prawnicze" 2011, t. 26
241. Mackiewicz P., M. Musiał, *Rozwój wirtualnych systemów monetarnych*, „Nauki o finansach - Financial sciences" 2014, nr 1(18)
242. Madison M.J., *The Narratives of Cyberspace Law (or, Learning From Casablanca)*, "Columbia Journal of Law & the Arts" 2004, nr 27(2)
243. Makowski A., *Arktyka - wspólne dziedzictwo czy wspólny problem?*, „Prawo Morskie" 2008, nr 24
244. Makowski A., *Koncepcja wolności mórz w działalności wojskowej mocarstw morskich na wszechoceanie*, [w:] U. Jackowiak, I. Nakielska, P. Lewandowski (red.), *Współczesne problemy prawa. Księga pamiątkowa dedykowana profesorowi Jerzemu Młynarczykowi*, Gdynia 2011
245. Marchini R., *Cloud computing: A Practical Introduction to the Legal Issues*, Londyn 2010
246. Marczewska - Rytko M. (red.), *Demokracja elektroniczna. Kontrowersje i dylematy*, Lublin 2013
247. Mariański M., *Problematyka kwalifikacji prawnej wirtualnej waluty we Francji*, „Państwo i Prawo" 2015, nr 10
248. Markiewicz R., *Internet i prawo autorskie - wykaz problemów i propozycje ich rozwiązań*, „Prace z Prawa Własności Intelektualnej" 2013, z. 2 (121)
249. Marszałkowska-Krześ E., *Właściwość sądu*, [w:] E. Marszałkowska - Krześ (red.), *Postępowanie cywilne*, Warszawa 2013
250. Marszelewski M., *Zapłodnienie post mortem w europejskim prawie porównawczym. Przyczynek do oceny polskiej ustawy o leczeniu niepłodności*, „Prawo i medycyna" 2015, nr 4
251. Masuda Y., *Managing in the Information Society*, Oxford 1990
252. Mączyński J., *Globalne społeczeństwo informacyjne. Wybrane kwestie adaptacyjne*, [w:] L. W. Zacher (red.), *Rewolucja informacyjna i społeczeństwo. Niektóre trendy, zjawiska i kontrowersje*, „Transformacje" 1997
253. Mednis A., *Prywatność od epoki analogowej do cyfrowej - czy potrzebna jest redefinicja?*, [w:] *Prywatność a jawność - bilans 25-lecia i perspektywy na przyszłość*, A. Mednis (red.), Warszawa 2016
254. Mefford A., *Lex informatica: Foundations of Law on the Internet*, "Indiana Journal of Global Legal Studies" 1997, t. 5, nr 1
255. Menkes J., *Stała suwerenność państw nad bogactwami naturalnymi a wspólne dziedzictwo ludzkości (analiza porównawcza)*, „Państwo i Prawo" 1990, nr 11
256. Menthe D.C., *Jurisdiction in Cyberspace: A Theory of International Spaces*, "Michigan Telecommunications and Technology Law Review" 1998, t. 4, nr 1
257. Meyer P., *Outer Space and Cyberspace: A Tale of Two Security Realms*, [w:] A.M. Osula, H. Rõigas (red.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Talin 2016

258. Michalak A., *Przegląd cywilnoprawnych instrumentów ochrony portali internetowych*, „Przegląd Prawa Handlowego" 2010, nr 4
259. Michałkiewicz E., Milczarek E., *Prawo do prywatności w dobie Internetu*, „Prawo Mediów Elektronicznych" 2015, nr 2
260. Michałowska G., *Ochrona praw człowieka w Radzie Europy i w Unii Europejskiej*, Warszawa 2007
261. Molenda-Kropielnicka E., *Cloud Computing - zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej" 2013, z. 1 (119)
262. Moore E.S., *Cyber jurisdiction*, "Virginia Lawyer Magazine", kwiecień 2002
263. Morcom C., *Trade Marks and the Internet: Where Are We Now?*, "European Intellectual Property Review" 2012, t. 34
264. Mostownik P., M. Niedźwiedź, *Druga konwencja lugańska o jurysdykcji oraz uznawaniu i wykonywaniu obcych orzeczeń w sprawach cywilnych*, „Kwartalnik Prawa Prywatnego" 2006, z. 4
265. Mozgawa M., P. Kozłowska-Kalisz, *Pornografia dziecięcia w świetle badań empirycznych (aspekty prawnokarne)*, [w:] M. Mozgawa, *Pornografia*, Warszawa 2011
266. Murray A.D., *Regulation and Rights in Networked Space*, "Journal of Law and Society" 2003, t. 30, nr 20
267. Myszona-Kostrzewa K., *Kierunki rozwoju międzynarodowego prawa kosmicznego*, [w:] K. Karski, *Kierunki rozwoju współczesnego prawa międzynarodowego*, Warszawa 2015
268. Niewęgłowski A., M. Chrzanowski, *Internet a prawo autorskie*, Lublin 2016
269. Poźniak-Niedzielska M. (red.), *Ochrona niematerialnego dziedzictwa kulturalnego*, Warszawa 2015
270. Nowak J.S., G. Bliźniuk (red.), *Społeczeństwo informacyjne: doświadczenie i przyszłość*, Katowice 2006
271. Nowicka A., *Prawnoautorska i patentowa ochrona programów komputerowych*, Warszawa 1995
272. Nowicka A., *Prawnoautorska ochrona programów komputerowych - regulacja polska i jej unijny wzorzec w świetle orzecznictwa Trybunału Sprawiedliwości*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2015, t. 77, z. 2
273. Nowicki M., *Zobowiązania Polski dotyczące ochrony klimatu wynikające z międzynarodowych i unijnych negocjacji,* [w:] M. Lipińska (opr.) *Ochrona klimatu szansą dla gospodarki i społeczeństwa. Materiały z konferencji zorganizowanej przez Komisję Środowiska we współpracy z Instytutem na rzecz Ekorozwoju*, Warszawa 2010
274. Nowina-Konopka M., *Istota i rozwój społeczeństwa informacyjnego*, [w:] M. Witkowska, K. Cholawo-Sosnowska (red*.), Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006
275. Noyes J.E., *The Common Heritage of Mankind: Past, Present, and Future*, "Denver Journal of International Law & Policy" 2012, nr 447
276. Okoń Z., *Licencja czy sprzedaż? Wyczerpanie prawa dystrybucji programów komputerowych w prawie UE*, [w:] K. Flaga - Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016
277. Ostropolski T., *Jurysdykcja uniwersalna w prawie międzynarodowym*, „Studia Prawno - - Europejskie" 2004, t. 7
278. Ostropolski T., *Zapobieganie sporom o jurysdykcję w Unii Europejskiej i ich rozstrzyganie*, [w:] A. Grzelak (red.), *Europejskie prawo karne*, Warszawa 2012
279. Osula A.M., H. Rõigas, *Outer Space and Cyberspace: A Tale of Two Security Realms* [w:] C. Chosseck. R. Ottis. K. Ziolkowski (red.), *2012 4th International Conference on Cyber Conflict*, Talin 2012

280. Oxman B.H., *Jurisdiction of States*, [w:] R.L. Bindschedler, T. Buergenthal (red), *Encyclopedia of Public International Law*, t. 3, Amsterdam 1997
281. Padzik J., *Piractwo morskie: historyczna ciągłość i zmiana*, „Bezpieczeństwo narodowe" 2013, nr I(25)
282. Paland O., *Bürgerliches Gesetzbuch*, Monachium 1998
283. Perkowski M., E. Szadkowska, *Umiędzynarodowienie organizacji pozarządowych we współczesnym prawie międzynarodowym*, „Problemy Współczesnego Prawa Międzynarodowego i Porównawczego" 2013, t. 11
284. Perkowski M., *Koncepcja „non-state actors" a umiędzynarodowienie regionów*, „Białostockie Studia Prawnicze" 2012, z. 12
285. Perkowski M., *Kształtowanie się podmiotowości prawa międzynarodowego*, [w:] J. Menkes (red.), *Prawo międzynarodowe. Księga pamiątkowa prof. Renaty Szafarz*, Warszawa 2007
286. Perkowski M., *Samostanowienie a Partnerstwo Wschodnie Unii Europejskiej: przyczynek do dyskusji*, „Polski Rocznik Praw Człowieka i Prawa Humanitarnego" 2010, nr 1
287. Pieńkos J., *Prawo międzynarodowe publiczne*, Kraków 2004
288. Piotrkowska A., *Koncepcja i formy pieniądza elektronicznego*, „Acta Universitatis Lodziensis Folia Oeconomica" 2014, nr 1(299)
289. Płachta M., *Konflikty jurysdykcyjne w sprawach karnych: pojęcie, geneza i środki zaradcze*, „Prokuratura i Prawo" 2010, nr 11
290. Płachta M., *Konflikty jurysdykcyjne w sprawach karnych: propozycja rozwiązania w Unii Europejskiej*, „Studia Europejskie" 2010, nr 2
291. Podraza A., *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeńswa międzynarodowego w XXI wieku*, [w:] A. Podraza (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013
292. Podrecki P., *Podział i rodzaje umów w Internecie*, [w:] *Prawo Internetu*, Warszawa 2004
293. Podrecki P., *Zawarcie umowy w sieci Internet*, [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007
294. Polański P., *Ochrona stron internetowych jako programów komputerowych.* [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
295. Polański P.P., *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warszawa 2014
296. Polański P.P., *Wprowadzenie do konwencji ONZ o kontraktach elektronicznych*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych*, Warszawa 2008
297. Polański P.P., *Zarys autonomicznego prawa Internetu*, „Studia Iuridica" 2006, nr 45
298. Polčák R., *Introduction to ICT law (selected issues)*, Brno 2007
299. Polkowska M., *Prawo kosmiczne w obliczu nowych problemów współczesności*, Warszawa 2011
300. Pollaud - Dulian F., *Competence internationale. Contrefacon. Internet. Droits voisins de l'artiste interprete*, "Revue trimestrielle de droit commercial" 2011, nr 2
301. Pollitt M., *Cyberterrorism - Fact or Fancy?*, "Computer Fraud & Security", luty 1998
302. Popiołek W., *Prawo właściwe dla umownych zobowiązań elektronicznych w konwencji rzymskiej i projekcie rozporządzenia Rzym I*, [w:] J. Gołaczyński (red.), *Kolizyjne aspekty zobowiązań elektronicznych. Materiały z konferencji*, Warszawa 2008
303. Posyniak J., *Bitcoin a aktualne uregulowania prawne środków płatniczych w Polsce*, [w:] Z. Ofiarski (red.), *XXV lat przeobrażeń w prawie finansowym i prawie podatkowym - ocena dokonań i wnioski na przyszłość*, Szczecin 2014

304. Pruszczyński T., *Streaming i sharing jako najszybciej rozwijające się gałęzie piractwa. Zagadnienia kryminologiczne i prawnokarne*, [w:] W. Dadak, M. Słobosz (red.), *Przestępczość przeciwko prawom własności intelektualnej*, Kraków 2016
305. Przyjemska J., *Granice wolności słowa w Internecie w wybranych systemach prawnych*, [w:] A. Biłgoraski (red.), *Wolność wypowiedzi i jej granice. Analiza wybranych zagadnień*, Katowice 2014
306. Pudełko M., *Prawdziwa histori@ Internetu*, Piekary Śląskie 2013
307. Pyć D., *Prawo oceanu światowego. Res usus publicum*, Gdańsk 2011
308. Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016
309. Radwański Z., *Aukcja i przetarg po nowelizacji*, „Monitor Prawniczy" 2004, nr 8
310. Raszkowska M., I. Malinowska, *Stalking jako problem społeczny*, „Przegląd Policyjny" 2013, nr 2
311. Rau Z., *Przestępczość zorganizowana w Polsce i jej zwalczanie*, Kraków 2002
312. Reidenberg J.R., *Lex Informatica: The Formulation of Information Policy Rules through Technology*, „Texas Law Review" 1998, t. 76, nr 3
313. Reinbothe J., M. Prat, S. von Lewinski, *The New WIPO Treaties: A first Résumé,* "European Intellectual Property Review" 1997, nr 7
314. Rodziewicz P., *Komentarz do art. 25*, [w:] J. Gołaczyński, *Jurysdykcja, uznawanie orzeczeń sądowych oraz ich wykonywanie w sprawach cywilnych i handlowych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012. Komentarz*, Warszawa 2015
315. Rogowski M., *Arbitraż w przedmiocie nazw domen internetowych na podstawie Uniform Domain Resolution Policy*, „Rynek - Społeczeństwo - Kultura" 2014, nr 2(10)
316. Rohrmann C.A., *The Dogmatic Function of Law as a Legal Regulation Model for Cyberspace*, "Anuario Brasileiro De Direito Internacional" 2008, t. 1
317. Rosłan G., M.P. Stolarski, *Cyfrowa waluta Bitcoin - nowe zagrożenie dla systemu finansowego*, cz. 2, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie" 2014, nr 2(27)
318. Roszyk A., *Świat przyjmuje walutę bitcoin*, „Prawo i podatki" 2015, nr 121
319. Rowe H., *Electronic Commerce and Consumers*, "International Business Lawyer" 1998, nr 4
320. Rybiałek M., *Ewolucja środków płatności (zapłaty): od pieniądza gotówkowego do pieniądza elektronicznego*, „Studia Prawnicze" 2012, z. 4 (192)
321. Ryfa J., *Waluty wirtualne - problem zdefiniowania i klasyfikacji nowego środka płatniczego*, „Nauki o Finansach Financial Studies" 2014, nr 2(19)
322. Schmidt A., H. Franken, *Law as code*, [w:] H. Snijders, S. Weatherill (red.), *E-commerce law. National and Transnational Topics and Perspectives code as law - general remarks on legal requirements engineering*, Haga 2003
323. Schmitt M.N., L. Vihul, *The Nature of International Law Cyber Norms*, "Tallinn Paper" 2014, nr 5
324. Schmitt M.N., *Tallinn Manual on the International law applicable to the cyber warfare*, Cambridge 2013
325. Schwabach A., *Internet and the Law: technology, society and compromises*, Santa Barbara 2014
326. Scott C., *Regulation in the Age of Governance: The Rise of the Post Regulatory State*, [w:] J. Jordana, D. Levi-Faur (red.), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance*. Cheltenham 2004
327. Shaw M.N., *International Law*, Cambridge, 2008
328. Shaw M.N., *Prawo międzynarodowe*, Warszawa 2006

329. Shaw M.N., *Prawo międzynarodowe*, Warszawa 2011
330. Sieber U., *Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions*, [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, nr 11
331. Siejka P., *Naruszenie tajemnicy korespondencji zagrożeniem bezpieczeństwa informacji*, [w:] Sitek M., I. Niedziółka, A. Ukleja, *Wymiary ochrony informacji i polityki bezpieczeństwa. Państwo - Prawo - Społeczeństwo*, Józefów 2014
332. Siemaszko A. (red.), *Stalking w Polsce - rozmiary - formy - skutki -. Raport z badania nt. uporczywego nękania*, „Archiwum Kryminologii" 2010, t. 32
333. Sienkiewicz P., H. Świeboda, *Sieci teleinformatyczne jako instrument państwa - zjawisko walki informacyjnej*, [w:] M. Madej, M. Trelikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009
334. Sienkiewicz P., *Od cybernetyki Wienera do cybernetycznej przestrzeni* [w:] *10 wykładów*, Warszawa 2005
335. Sienkiewicz P., *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2015, t. 9, nr 13
336. Sienkiewicz P., *Prognozowanie rozwoju globalnego społeczeństwa informacyjnego: wizje i scenariusze*, [w:] A. Szewczyk, E. Kot (red.), *Fenomen Internetu*, t. 1, Szczecin 2008
337. Sienkiewicz P., *Teoria rozwoju społeczeństwa informacyjnego*, [w:] L. H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno - kulturowe*, Kraków 2002
338. Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni*, [w:] T. Jemioła, J. Kiesielnicki, K. Rajchel (red.), *Cyberterroryzm - nowe wyzwania XXI wieku*, Warszawa 2009
339. Sienkiewicz P., *Wizje i modele wojny informacyjnej*, [w:] L.H. Haber, *Społeczeństwo informacyjne - wizja czy rzeczywistość ?,* t.1, Kraków 2004
340. Sieńczyło-Chlabicz J., *Prawo własności intelektualnej*, Warszawa 2011
341. Siuda P., *Prywatność w Internecie - zarys perspektywy krytycznej*, „Kultura-Media-Teologia" 2015, nr 20
342. Siwicki M., *Cyberprzestępczość*, Warszawa 2013
343. Siwicki M., *Jurysdykcja krajowa w sprawach z zakresu prawa autorskiego w „chmurach obliczeniowych" w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1215/2012*, „Europejski Przegląd Sądowy" 2016, nr 1
344. Siwicki M., *Karalność mowy nienawiści w Internecie - aspekty prawnoporównawcze*, „Palestra" 2007, nr 5-6
345. Siwicki M., *Kradzież tożsamości - pojęcie i charakterystyka zjawiska*, cz. 1, „Edukacja Prawnicza" 2009, nr 11
346. Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011
347. Siwicki M., *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajemnicy telekomunikacyjnej w chmurach obliczeniowych*, „Prokuratura i Prawo" 2015, nr 5
348. Siwicki M., *Podstawy określenia jurysdykcji w sprawach cyberprzestępstw w UE*, „Europejski Przegląd Sądowy" 2013, nr 9
349. Siwicki M., *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęciu prawnoporównawczym*, cz. 1, „Europejski Przegląd Sądowy" 2011, nr 9
350. Siwicki M., *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęciu prawnoporównawczym*, cz. 2, „Europejski Przegląd Sądowy" 2011, nr 10

351. Skwarzyński M., *Przestępstwa uzyskania programu komputerowego - art. 278 § 2 k.k.*, „Palestra" 2010, nr 3
352. Słok M., *Regulacje prawnomiędzynarodowe dotyczące handlu organizmami modyfikowanymi genetycznie*, [w:] J. Menkes (red.), *Prawo międzynarodowe. Księga pamiątkowa prof. Renaty Szafarz*, Warszawa 2007
353. Smart U., *The Stalking Phenomenon: Trends in European and International Stalking and Harassment Legislation*, "European Journal of Crime, Criminal Law and Criminal Justice" 2001, t. 9, nr 3
354. Smith G., *Internet Law and Regulation*, Londyn 1997
355. Smus T.R., *Spełnienie świadczeń pieniężnych za pomocą pieniądza elektronicznego*, Warszawa 2010
356. Sołodow D., *Regulacje prawne dotyczące bezpieczeństwa w sieci Internet (na przykładzie prawa internetowego Federacji Rosyjskiej)*, „Studia prawnoustrojowe" 2016, t. 31
357. Spang-Hansen H., *Cybercrime and Jurisdiction in Denmark*, [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, nr 11
358. Srogosz T., *Międzynarodowe prawo lotnicze i kosmiczne*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne,* Warszawa 2014
359. Srogosz T., *Obszary podbiegunowe*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2014
360. Srogosz T., *Terytorium*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2014
361. Srokosz W., *Istota prawna pieniądza elektronicznego*, „Prawo Bankowe" 2002, nr 12(64)
362. Srokosz W., *Prawo a rozwój elektronicznych środków płatniczych w XXI wieku*, [w:] Z. Ofiarski (red.), *XXV lat przeobrażeń w prawie finansowym i prawie podatkowym - ocena dokonań i wnioski na przyszłość*, Szczecin 2014
363. Stanek J., *Patentowanie genów ludzkich*, Warszawa 2016
364. Stańczyk J., *Pojęcie wspólnego dziedzictwa ludzkości w prawie międzynarodowym*, „Państwo i Prawo" 1985, z. 9
365. Stosio A., *Umowy zawierane przez Internet*, Warszawa 2002
366. Symonides J., *Terytorium w prawie międzynarodowym*, [w:] R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Warszawa 2005
367. Szczotka J., *Przepisy szczególne dotyczące niektórych utworów*, [w:] M. Poźniak - Niedzielska (red.), *Prawo autorskie i prawa pokrewne*, Bydgoszcz-Warszawa-Lublin 2007
368. Szostek D., M. Świerczyński, *Wybór prawa właściwego dla zobowiązań z umów elektronicznych zawieranych w postaci elektronicznej,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2007, z. 100
369. Szostek D., *Pieczęć elektroniczna i jej możliwość wykorzystania w prawie polskim*, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016
370. Szostek D., *Prawne aspekty podpisu elektronicznego*, [w:] J. Barta, R. Markiewicz, *Handel elektroniczny. Prawne problemy*, Kraków 2005
371. Sztobryn K., *Ochrona programów komputerowych w prawie własności intelektualnej w Unii Europejskiej*, Warszawa 2015
372. Śledzińska-Simon A., *Decyzja ramowa w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii*

Europejskiej, [w:] R. Wieruszewski (red.) *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010
373. Świerczyński M., *Internet a nowe prawno prywatne międzynarodowe*, [w:] G. Szpor, W.R. Wiewiórski (red.), *Internet. Prawno - informatyczne problemy sieci, portali i e-usług*, Warszawa 2012
374. Świerczyński M., *Jurysdykcja krajowa i prawo właściwe a Internet,* [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007
375. Świerczyński M., *Komentarz do art. 7,* [w:] J. Gołaczyński (red.), *Jurysdykcja, uznawanie orzeczeń sądowych oraz ich wykonywanie w sprawach cywilnych i handlowych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012. Komentarz*, Warszawa 2015
376. Świerczyński M., M. Kolesiński, *Wybór prawa obcego w internetowych wzorcach umownych a ochrona konsumenta,* [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
377. Świerczyński M., *Podpis elektroniczny*, [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007
378. Taczkowska J., *Kategorie wypowiedzi i ich ochrona*, Warszawa-Poznań 2008
379. Tadeusiewicz R., *Wychowywanie dla cyberprzestrzeni jednym z warunków zapobiegania cyberuzależnieniom*, [w:] E. Mastalerz, K. Pytel, H. Noga (red.), *Cyberuzależnienia: przeciwdziałanie uzależnieniom od komputera i Internetu*, Kraków 2007
380. Targosz T., *Pieniądz elektroniczny*, [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007
381. Tarnacki R., *Korzystanie z obszaru jako realizacja zasady wspólnego dziedzictwa ludzkości w świetle Konwencji NZ o prawie morza*, „Prawo Morskie" 2007, nr 23
382. Tarnogórski R., *Konwencja o cyberprzestępczości - międzynarodowa odpowiedź na przestępczość ery informacyjnej*, [w:] M. Madej, M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa Polski*, Warszawa 2009
383. Tokarczyk R., *Prawo amerykańskie*, Warszawa 2011
384. Torbus A., *Umowa jurysdykcyjna w systemie międzynarodowego postępowania cywilnego*, Toruń 2012
385. Traple E. (red.), *Ochrona gry komputerowej. Aktualne wyzwania prawne*, Warszawa 2015
386. Trelikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Trelikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009
387. Urbas G., P. Grabosky, *Cybercrime and Jurisdiction in Australia,* [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, nr 11
388. Vattel E. de, *Prawo narodów, czyli zasady prawa naturalnego zastosowane do postępowania i spraw narodów i monarchów*, Warszawa 1958
389. Ventre D., *Cyberspace in Japan's New Defence Strategy*, [w:] D. Ventre (red.) *Cyber Conflict. Competing National Perspectives*, Londyn 2012
390. Vogler J., *Global Commons Revisited,* "Global Policy" 2012, t. 3, nr 1
391. Vogler J., *The Global Commons*, Toronto 1995
392. von Stein J., The *International Law and Politics of Climate Change: Ratification of the United Nations Framework Convention and the Kyoto Protocol*, "The Journal of Conflict Resolution" 2008, t. 52, nr 2

393. Walden I., *Cybercrime and Jurisdiction in United Kingdom*, [w:] B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A global survey*, "Information Technology & Law Series" 2006, nr 11
394. Warylewski J., *Pornografia - próba definicji*, [w:] M. Mozgawa (red.), *Pornografia*, Warszawa 2011
395. Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9
396. Wasiński M., *Jurysdykcja legislacyjna państwa w prawie międzynarodowym publicznym*, „Państwo i Prawo" 2002, nr 3
397. Wąsek A., M. Kulik, *Zasady odpowiedzialności karnej (art. 1-12)*, [w:] M. Filar (red.), *Kodeks karny. Komentarz*, Warszawa 2010
398. Weitz K., *Jurysdykcja krajowa w postępowaniu cywilnym*, Warszawa 2005
399. Weitz K., *Kilka uwag na temat jurysdykcji krajowej w sprawach z czynów niedozwolonych w prawie europejskim*, „Roczniki Nauk Prawnych" 2006, t. 16
400. Wejman F., *Wprowadzenie do cywilistycznej problematyki ustawy o podpisie elektronicznym*, „Prawo Bankowe" 2002, nr 2
401. Wierzbicki P., *Metody zawierania umów z wykorzystaniem wzorców kontraktowych w Internecie - analiza wybranych orzeczeń*, [w:] E. Galewska (red.), *Wybrane aspekty prawa nowych technologii*, Wrocław 2013
402. Wiśniewski S., *Prawnoautorska kwalifikacja gier komputerowych - program komputerowy czy utwór audiowizualny?* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej" 2012, z. 1
403. Witkowska M., K. Cholawo-Sosnowska (red*.), Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006
404. Wnukiewicz-Kozłowska A., *Prawo międzynarodowe wobec wyzwań współczesnej medycyny*, [w:] E. Dynia (red.), *Prawo międzynarodowe i wspólnotowe wobec wyzwań współczesnego świata*, Rzeszów 2009
405. Wojtasik Ł., *Materiały dla uczestników konferencji wojewódzkich realizowanych w ramach kampanii "Dziecko w sieci" i programu UE "Safer Internet Action Plan" w latach 2006-2016*
406. Woluniuk L., *Cyberterroryzm jako element cywilizacji informacyjnej*, [w:] M. Zuber (red.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i reagowanie kryzysowe*, Wrocław 2006
407. Wouwer J.J. van de, F. Lambert, *European Trajectories in Space Law 2007*, Luksemburg 2008
408. Wrona A., *Cyberpornografia i cyberseks*, [w:] J. Bednarek, A. Andrzejewska (red.), *Cyberświat - możliwości i zagrożenia*, Warszawa 2009
409. Wróbel W., A. Zoll, *Polskie prawo karne. Część ogólna*, Kraków 2010
410. Wydro K.B., *Internet dziś – stan i wykorzystanie*, [w:] A. Szewczyk, E. Krok (red.), *Fenomen Internetu*, t. 1, Szczecin 2008
411. Zalisko M., *Instrumenty prawne w obszarze współpracy sądowej w sprawach cywilnych i handlowych w Unii Europejskiej*, Warszawa 2013
412. Załucki M., *Śmierć a dane w systemach teleinformatycznych - przyczynek do dyskusji*, [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016
413. Znojek M., *Kilka uwag o zarzutach podnoszonych wobec jurysdykcji uniwersalnej*, „Kwartalnik Prawa Publicznego" 2007, nr 3
414. Zwolińska A., *Wpływ projektu dyrektywy o treściach cyfrowych na ich pojęcie - wnioski de lege lata i de lege ferenda*, [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2016

415. Żak D.G., *Wybrane formy naruszeń prawa własności intelektualnej w Internecie*, [w:] D. Żak, *Własność intelektualna w sieci*, Lublin 2014
416. Żak K., *Środki ochrony zamawiającego program komputerowy. Odpowiedzialność twórcy za usterki utworu*, Warszawa 2015
417. Żylicz M., *O początkach międzynarodowego prawa kosmicznego*, [w:] Z. Galicki, T. Kamiński, K. Myszona-Kostrzewa, *Wykorzystanie przestrzeni kosmicznej. Świat - Europa - Polska*, Warszawa 2010

Netografia

Akty prawa innych państw

1. Australijski kodeks karny http://www.austlii.edu.au/au/legis/vic/consol_act/ca195882/s21a.html
2. Malaysia Computer Crimes Act 1997, http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf
3. Nouveau Code de procédure civile z dnia 1 stycznia 1976 r., Nouveau Code de Procédure Civile z dnia 1 stycznia 1976 r., https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070716

Dokumenty

1. CCRCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2007/CCPCJ/Resolution_16-2.pdf
2. Center for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey, California, White Paper. *Cyberterror: prospects and implemenations*, October 1999
3. Comprehensive Study on Cybercrime. Undoc 2013, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBER CRIME _STUDY_210213.pdf,
4. Cooperation against cybercrime: Progress made in 2012 – A brief review of Council of Europe activities, Dokument dostępny online na oficjalnej stronie internetowej Rady Europy http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Docs2013/cyber%20AS%20review2012_flyer_v6.pdf
5. Council of the European Union Revised Draft Code of Conduct for Outer Space Activities, Bruksela 2010, http://www.consilium.europa.eu/uedocs/cmsUpload/st14455.en10.pdf
6. *Cybersecurity strategy September 2015*, National Center of Incident Readiness and Stategy for Cybersecurity, http://www.nisc.go.jp/eng/index.html

7. Dokument *Basic tips for investigators and prosecutors for requesting electronic/digital data/evidence from foreign jurisdictions*, https://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf
8. Dokument Cyber Defence Plagde dostępny na oficjalnej stronie NATO: https://nato.usmission.gov/cyber-defense-pledge
9. Dokument *Cyber Security Strategy for Germany:*
10. Dokument *Cybersecurity Strategy 2014* dostępny na oficjalnej stronie internetowej Ministerstwa Gospodarki i Komunikacji Republiki Estonii: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_ version.pdf
11. *ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.* http://www.un.org/en/ecosoc/docs/2004/resolution%202004-26.pdf
12. ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identityrelated crime. http://www.un.org/en/ecosoc/docs/2007/resolution%202007-20.pdf,
13. Europe and the Global Information Society, Recomendations of the Bangerman Group to the European Council, http://www.epractice.eu/files/media/media_694.pdf
14. F. Pocara, *Sprawozdanie objaśniające Konwencję o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń sądowych w sprawach cywilnych i handlowych, podpisaną w Lugano w dniu 30 października 2007 r.*, http://bip.ms.gov.pl/Data/Files/_public/bip/lugano/raport pocara_2.pdf
15. Growth, Competitiveness and Employment. The Challenges and Ways Forward into 21st Century Dokument dostępny online: http://www.cvce.eu/content/publication/1997/10/13/b0633a76-4cd7-497f-9da1-4db3dbbb56e8/publishable_en.pdf
16. *How Censorship Works in China: A Brief Overview*, Human Rights Watch https://www.hrw.org/reports/2006/china0806/3.htm
17. Internet Law & Policy Forum, Survey of International Electronic and Digital Signature Initiatives: http://www.ilpf.org/groups/survey.htm#overview
18. ITU Global CybersecurityAgenda (GCA) High - Level Experts Group (HLEG) Report of the Chairman of HLEG, http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf,
19. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Wykorzystanie potencjału chmury obliczeniowej w Europie", http://eur–lex.europa.eu/ LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:PL:PDF
20. Komunikat Komisji, Europa 2020 Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, KOM(2010)2020, http://ec.europa.eu/eu2020/pdf/1_PL_ACT_part1_v1.pdf
21. National Security Concept of Georgia http://csbd.gov.ge/bureau.php?lang=en
22. Oświadczenie Ministra Finansów w sprawie bitcoin http://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/dokumenty/stenogram/oswiadczenia/klima/3001oa.pdf
23. Projekt SISSDEN: https://sissden.eu/
24. Raport Gemius E-commerce w Polsce, https://www.gemius.pl/files/reports/E-commerce-w-Polsce-2015.pdf

25. Raport http://iab.org.pl/badania-i-publikacje/raport-strategiczny-iab-polska-internet-2010/
26. Raport http://iab.org.pl/wp-content/uploads/2014/08/raport_iab_2013.pdf
27. Raport Norton 2013: http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf
28. Raport The 2015 Global Retail E-Commerce Index, https://www.atkearney.com/documents/10192/5691153/Global+Retail+E-Commerce+Keeps+On+Clicking.pdf/abe38776-2669-47ba-9387-5d1653e40409
29. Raport „E-commerce w Polsce 2015. Gemius dla e-Commerce" dostępny online https://www.gemius.pl/files/reports/E-commerce-w-Polsce-2015.pdf
30. Report of the Working Group on Internet Governance. Château de Bossey June 2005, http://www.wgig.org/docs/WGIGREPORT.pdf
31. *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World,* https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf
32. Strategia Militarna Chin, https://news.usni.org/2015/05/26/document-chinas-military-strategy
33. Tekst *ITU Toolkit for Cybercrime Legislation*, http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf
34. Tekst Warsaw Summit Communiqué, https://nato.usmission.gov/warsaw-summit-communique/
35. The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security- strategy-final.pdf
36. UNCITRAL „Model Law on Electronic Commerce", United Nations, New York 1997
37. Zielona Księga Living and Working in Information Society. People First, http://europa.eu/rapid/press-release_IP-96-688_en.htm?locale=en

Wykaz literatury

1. Bauer J.M., *Internet Governance: Theory and First Principles*, https://www.researchgate.net/profile/Johannes_Bauer3/publication/228800513_Internet_Governance_Theory_and_First_Principles/links/09e4150fee13f84c8a000000.pdf
2. Broome J., *Comonwealth, State Boundaries in Crime and Justice*, http://www.aic.gov.au/media_library/conferences/outlook99/broome.pdf
3. Danning D., *Testimony before the Special Oversight Panel on Terrorism. Committee on Armed Services*, U.S. House of Representatives, 23.05.2000, http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf
4. Dwivedi S., *Jurisdictional Issues in Cyber Crime*. [online] Academia.edu. http://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime
5. Gercke M., *Internet - related identity theft*, Strasburg, 2007 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022% 20 nov% 2007.pdf

6. J. Skarżyńska - Sernaglia, *Stalking w Polsce - występowanie i charakterystyka zjawiska*, Artykuł dostępny na http://psychologia.net.pl/artykul.php?level=415
7. Johnson D.R., D.G. Post, *The New 'Civic Virtue' of the Internet: A Complex Systems Model for the Governance of Cyberspace*, "Review of the Institute for Information Studies" 1998, http://www.temple.edu/lawschool/dpost/Newcivicvirtue.html,
8. Lashkari B. R., *Issue of jurisdiction under cyber law in India*, Racolblegal, http://racolblegal.com/issue-of-jurisdiction-under-cyber-law-in-india/
9. Ogilvie E., *Cyberstalking*, artykuł dostępny online na oficjalnej stronie internetowej Australian Institute of Criminology http://www.aic.gov.au/documents/4/7/A/%7B47A7FA60-8EBF-498A-BB9E-D61BC512C053%7Dti166.pdf
10. R. O'Connell, *A Typology of Child Cybersexploitation and Online Grooming Practices*, Lancashire 2003, http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf
11. Tadeusiewicz R., Internet i prawo, http://winntbg.bg.agh.edu.pl/skrypty/0037/cz0-r1.pdf
12. *Tak działa scarewere! Poznaj swojego wroga*, http://www.komputerswiat.pl/jak-to-dziala/2011/03/tak-dziala-scareware-poznaj-swojego-wroga.aspx
13. The Guardian http://www.theguardian.com/uk/2001/feb/11/tracymcveigh.martinbright
14. Watkins B., *The Impact of Cyber Attacks on the Private Sector*,http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf
15. Weinberg M., *The criminal jurisdiction of the Federal Court*, http://www.austlii.edu.au/au/journals/NSWBarAssocNews/2008/53.pdf

Strony internetowe

1. Oficjalna strona internetowa bazy aktów prawnych Unii Europejskiej: www.eur-lex.europa.eu
2. Oficjalna strona internetowa Biura Bezpieczeństwa Narodowego RP: www.bbn.gov.pl
3. Oficjalna strona internetowa Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi: www.ccdcoe.org
4. Oficjalna strona internetowa CERT: www.cert.org
5. Oficjalna strona internetowa Creative Commons: www.creativecommons.pl,
6. Oficjalna strona internetowa Crypto-Currency Market Capitalizations: www.coinmarketcap.com
7. Oficjalna strona internetowa Cybersecurity Gateway: www.groups.itu.int/cybersecurity-gateway
8. Oficjalna strona internetowa Cyberterrorism Project: www.cyberterrorism-project.org
9. Oficjalna strona internetowa Cybsecurity.org: www.cybsecurity.org/cyber-exe-gruzja-2015
10. Oficjalna strona internetowa Dziennika Internautów Biznes i Prawo: www. di.com.pl
11. Oficjalna strona internetowa ENISA: www.enisa.europa.eu
12. Oficjalna strona internetowa Europolu: www.europol.europa.eu
13. Oficjalna strona internetowa Forum Zarządzania Internetem. www.intgovforum.org
14. Oficjalna strona internetowa Gazety Prawnej: www.biznes.gazetaprawna.pl
15. Oficjalna strona internetowa Human Rights Watch www.hrw.org
16. Oficjalna strona internetowa Internet Governance: www.internetgovernance.org

17. Oficjalna strona internetowa Internet Live Stats: www.internetlivestats.com
18. Oficjalna strona internetowa Internet World Stats: www.internetworldstats.com/stats.htm
19. Oficjalna strona internetowa Interpolu: www.interpol.int
20. Oficjalna strona internetowa ITU: www.itu.int
21. Oficjalna strona internetowa JProjektu BIC: www.bic-trust.eu
22. Oficjalna strona internetowa kanadyjskiego Ministerstwa Bezpieczeństwa: www.publicsafety.gc.ca
23. Oficjalna strona internetowa Komisji Europejskiej: www.ec.europa.eu
24. Oficjalna strona internetowa misji amerykańskiej NATO: www.nato.usmission.gov
25. Oficjalna strona internetowa National Center of Incident Readiness and Stategy for Cybersecurity: www.nisc.go.jp
26. Oficjalna strona internetowa NATO: www.nato.int
27. Oficjalna strona internetowa Newsweek Polska: www.newsweek.pl
28. Oficjalna strona internetowa OECD: www.oecd.org
29. Oficjalna strona internetowa Projektu CAPITAL: www.capital-agenda.eu/default.aspx?page=home
30. Oficjalna strona internetowa Projektu COMIFIN: www.tssg.org/projects/comifin
31. Oficjalna strona internetowa Projektu Cybercrime@IPA: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp
32. Oficjalna strona internetowa Projektu ETCETERA: www.etcetera-project.eu
33. Oficjalna strona internetowa Projektu GLACY: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/GLACY/GLACY_en.asp
34. Oficjalna strona internetowa Projektu ILLBuster: www.illbuster-project.eu
35. Oficjalna strona internetowa Projektu NISHA: www.nisha-network.eu
36. Oficjalna strona internetowa Projektu WOMBAT: www.wombat-project.eu
37. Oficjalna strona internetowa Rady Europy: www.coe.int
38. Oficjalna strona internetowa słownika komputerowego i encyklopedii informatycznej wwww.i-slownik.pl
39. Oficjalna strona internetowa Statista: www.statista.com
40. Oficjalna strona internetowa The Guardian: https://www.theguardian.com
41. Oficjalna strona internetowa TVN24 http://www.tvn24.pl
42. Oficjalna strona internetowa UNCITRAL: www.uncitral.org
43. Oficjalna strona internetowa Webmaster: www.webmaster.net.pl
44. Oficjalna strona internetowa World Wide Web Size: www.worldwidewebsize.com
45. Oficjalna strona internetowa WSIS: www.itu.int/net
46. Oficjalna strona internetowa WTO: www.wto.org

Spis rysunków

Spis tabel