WYDZIAŁ PRAWA

UNIWERYSTET W BIAŁYMSTOKU

KATEDRA PRAWA KONSTYTUCYJNEGO

GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

JAKO

ORGAN OCHRONY PRAWA DO PRYWATNOŚCI

Mgr Emilia Kuczma

Praca doktorska napisana pod kierunkiem

Prof. UwB dr hab. Grzegorza Kryszenia

Białystok 2016

SPIS TREŚCI

WSTĘP

Prywatność to w dzisiejszym świecie jedno z najcenniejszych dóbr człowieka. Daje każdemu poczucie niezależności, prawo do samostanowienia o sobie i swoim życiu na wielu płaszczyznach. Wielokrotnie nazywane i definiowane jest sumą różnych wartości składających się na rozumienie autonomiczności człowieka żyjącego w określonej rzeczywistości wobec innych jednostek, a także ich wspólnot oraz samego państwa i jego funkcjonariuszy[1].

Hegemonia informacji i rozwój różnorodnych form komunikowania się doprowadziły do wyodrębnienia z prawa do prywatności prawa do ochrony danych osobowych. W myśl zasady *ubi ius, ibi remedium* ochrona danych osobowych jawi się jako jeden z wielu środków realizacji szeroko rozumianego prawa do prywatności. Zakłada ochronę informacji dotyczących danej osoby, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o sobie[2].

Obecnie ochrona danych osobowych jest determinowana ciągłym rozwojem technologicznym. Informacja o osobie jest cenna we współczesnym świecie, stąd wymaga stałej ochrony. Z tego też względu istotne znaczenie ma precyzyjne, ustawowe uregulowanie tematyki ochrony danych osobowych. Kluczowe jest zagwarantowanie jednostce anonimowości oraz ochrony przed niechcianym i niekontrolowanym wykorzystywaniem informacji na jej temat, z równoczesnym zapewnieniem jej swobodnego funkcjonowania we współczesnej cywilizacji. Ochronie i kontroli muszą być poddane informacje gromadzone w większych i mniejszych zbiorach, a także procesy udostępniania i przekazywania danych zwłaszcza w systemach informatycznych. Zapewnienie skutecznej ochrony prywatności człowieka to obecnie priorytet państwa demokratycznego, a władze każdego kraju powinny dysponować odpowiednimi środkami, aby zagwarantować wszystkie wolności i prawa jednostki. Wymóg ten jest w pierwszej kolejności realizowany poprzez podejmowanie działań legislacyjnych kreujących m. in. normy zabezpieczające nienaruszalność życia prywatnego człowieka, wdrażanie mechanizmów oraz tworzenie instytucji, które stałyby na straży wolności osobistej i prywatności jednostki. Wypracowanie efektywnych metod regulacji ma służyć poprawie stanu ochrony danych osobowych oraz powinno wpływać na kształtowanie przyszłych postaw i świadomości społeczeństwa w zakresie ochrony prywatności.

---

[1] Zob. M. Jabłoński, *Prywatność jako przesłanka ograniczenia dostępu do informacji publicznej*, „Przegląd Prawa i Administracji" 2007, nr 86, s. 280.
[2] Por. wyrok TK z dnia 19 maja 1998 r., U5/97, OTK 1998, nr 4, poz. 46.

Począwszy od lat 70. XX wieku, po doświadczeniach w zakresie ochrony danych osobowych w Europie Zachodniej, posiadanie prawnych rozwiązań w tej materii stało się standardem. W Polsce kształtowanie skutecznych metod ochrony informacji osobowych było także od dawna przedmiotem rozważań doktryny prawa. Zgłębianie obszarów badawczych istniejących na pograniczu prawa konstytucyjnego czy administracyjnego, wraz z wpływem regulacji międzynarodowych, oddziaływało skutecznie na rozwój krajowych norm w zakresie bezpieczeństwa przetwarzania danych osobowych. Podstawę w zakresie ochrony prywatności i ochrony danych osobowych w Polsce stanowią obecnie przepisy Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.[3] oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[4] (dalej u.o.d.o.).

Ustawa o ochronie danych osobowych jest szczegółową regulacją odnoszącą się do ochrony danych osobowych. Po raz pierwszy w Polsce w jednym akcie prawnym ustawodawca kompleksowo unormował zagadnienia z obszaru ochrony danych osobowych człowieka, zdefiniował podstawowe pojęcia i instytucje odnoszące się do ochrony prywatności jednostki oraz wprowadził prawne mechanizmy kontroli i ochrony danych osób fizycznych. *Ratio legis* ustawodawcy było również powołanie organu, zgodnie z międzynarodowymi warunkami ochrony danych, stanowiącego zasadniczy element ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Zaistnienie Generalnego Inspektora Ochrony Danych Osobowych (w skrócie: GIODO) okazało się najistotniejszą gwarancją ochrony prywatności człowieka i ochrony jego danych osobowych w Polsce, tym bardziej że żaden inny organ państwowy nie posiadał wcześniej kompetencji w tym zakresie.

Problematyka ochrony prywatności posiada duże znaczenie praktyczne. Zagadnienie ochrony prywatności było i pozostaje we współczesnym świecie cały czas aktualne. Obecnie wysuwane są postulaty dyktatu prywatności niczym nieograniczonej, a z drugiej strony, pojawia się coraz więcej zagrożeń prywatności, uniemożliwiających pełną realizację tego prawa. Na tej podstawie uznałam za konieczną analizę działalności organu powołanego do ochrony prywatności w Polsce. Dotychczas pojawiające się publikacje opisują GIODO dość skromnie i raczej fragmentarycznie analizują problematykę odnoszącą się do pozycji tego organu czy podejmowanych przez niego działań. Z tego względu uznałam za niezbędne dokonanie w sposób całościowy i jednolity opisu pozycji, zasad funkcjonowania oraz zadań i

[3] Dz. U. z 1997 r. Nr 78, poz. 483; Dz. U. z 2001 r. Nr 28, poz. 319; Dz. U. z 2006 r. Nr 200, poz. 1471; Dz. U. z 2009 r. Nr 114, poz. 946.
[4] Dz. U. Nr 133, poz. 883 z późn. zm.

środków działania Generalnego Inspektora. Za punkt wyjścia przyjęłam analizę obszarów badawczych odnoszących się do pozycji ustrojowej GIODO istniejących na pograniczu prawa konstytucyjnego, administracyjnego, korzystając posiłkowo z regulacji międzynarodowych Ponadto chcę dowieść, iż pomimo realizacji przez GIODO części uprawnień w trybie administracyjnym, jest to organ w pełni zasługujący na pogłębioną analizę z perspektywy prawa konstytucyjnego, głównie z uwagi na realizację przez niego zadań i podejmowanie działań odnoszących się do płaszczyzny związanej z ochroną praw i wolności człowieka.

Określenie pozycji ustrojowej i zakresu działania organu ochrony prawa do prywatności, jakim jest GIODO, stanowi podstawowe założenie badawcze pracy. W doktrynie pojawiają się rozbieżności i sprzeczne poglądy co do określenia prawnej pozycji tego organu w polskim systemie organów państwowych. Jednym z celów pracy jest zatem kompleksowe opisanie działalności tego organu. Analiza zagadnień teoretycznych i praktycznych odnoszących do szczegółowego zakresu funkcjonowania Generalnego Inspektora Ochrony Danych Osobowych ma z kolei zaprezentować jego znaczenie wśród innych organów państwowych oraz wskazać istotę i potrzebę dalszego jego działania w zakresie ochrony prawa do prywatności człowieka w Polsce.

Praca jest podzielona na sześć rozdziałów.

Chcąc przybliżyć tematykę prawnej ochrony prywatności i ochrony danych osobowych pierwszy rozdział rozprawy jest poświęcony przedstawieniu w ogólnym zarysie genezy i istoty prawa do prywatności. Sfera prywatności jako odrębne dobro prawne zawiera w sobie wiele elementów występujących w obrębie szeroko pojętego życia prywatnego człowieka, a jednym z nich jest prawo do autonomii informacyjnej. Wydaje się zatem zasadne przedstawienie poglądów doktryny odnoszących się do prawa do prywatności, zdefiniowanie tego prawa i wskazanie oraz charakterystyka tych wspomnianych składowych, które je tworzą. W rozdziale tym podejmuję też próbę opisu ewolucji i rozwoju prawa do ochrony danych osobowych, a następnie wskazania zależności pomiędzy prawem do prywatności a ochroną danych osobowych.

Z uwagi na fakt, iż prawo do ochrony danych osobowych podlega ochronie w większości współczesnych systemów prawnych, w kolejnym rozdziale pracy zwracam uwagę na źródła prawnej ochrony danych osobowych o zasięgu międzynarodowym, w tym zwłaszcza europejskim, a także aspekty ochrony prywatności informacyjnej w wybranych państwach na świecie. Chcąc uporządkować i przybliżyć problematykę dotyczącą ochrony prywatności i ochrony danych osobowych w porządku chronologicznym opisuję i porównuję międzynarodowe akty prawne, które wyznaczyły standardy ochrony prywatności i ochrony

danych osobowych na świecie. W rozdziale tym zwracam także uwagę na proponowane zmiany w ustawodawstwie unijnym w zakresie ochrony danych osobowych stanowiące perspektywy ochrony danych osobowych w Unii Europejskiej oraz dokonuję charakterystyki instytucji Europejskiego Inspektora Ochrony Danych (w skrócie: EIOD). Moim zamiarem jest wykazanie, iż powołanie EIOD jako funkcjonującego na szczeblu ponadpaństwowym niezależnego organu odpowiedzialnego za nadzorowanie stosowania aktów wspólnotowych dotyczących ochrony danych osobowych w instytucjach i organach UE, było pozytywnym doświadczeniem w zakresie prawnej ochrony danych tak dla organów i instytucji wspólnotowych, jak również dla Unii Europejskiej oraz dla Polski, a jego działalność może stanowić wzór do naśladowania w tym zakresie dla odpowiednich organów krajowych.

W rozdziale trzecim kieruję uwagę na zagadnienia ochrony danych osobowych w polskim porządku prawnym. W pierwszej kolejności analizuję proces kształtowania się ochrony prawa do prywatności w polskim systemie prawnym, a następnie powstanie i wyodrębnienie prawa do ochrony danych osobowych. Dokonuję tu analizy regulacji z zakresu ochrony danych osobowych na gruncie przepisów Konstytucji RP z dnia 2 kwietnia 1997 r. oraz ustawy o ochronie danych osobowych, a także wyjaśniam podstawowe pojęcia i oraz definiuję kluczowe instytucje związane z ochroną danych osobowych w Polsce. Celem tego rozdziału jest dokonanie oceny ukształtowania problematyki ochrony autonomii informacyjnej, w stosunku do głównych idei i założeń prawa do prywatności i prawnych regulacji międzynarodowych w tym zakresie.

Przedmiotem rozważań w rozdziale czwartym jest określenie pozycji prawnoustrojowej Generalnego Inspektora Ochrony Danych Osobowych. Sformułowane w tym rozdziale tezy są istotne z punktu widzenia prawa konstytucyjnego i potwierdzają doniosłą pozycję GIODO w systemie organów państwowych w Polsce. Na wstępie jest dokonany podział i klasyfikacja organów państwowych w Polsce, tak aby możliwe było przedstawienie na tym tle specyfiki GIODO jako organu ochrony prywatności w tym systemie. Dokonując charakterystyki GIODO określam jego status jako organu państwowego, procedurę powołania, kwalifikacje osobiste i zawodowe wymagane od GIODO oraz zasady działania tego organu ze szczególnym uwzględnieniem zasady niezależności, zasady niepołączalności (*incompatibilitas*), zasady apolityczności, zasady ochrony immunitetowej oraz zasady kadencyjności GIODO. Przybliżam również działalność zastępcy GIODO i zasady działania oraz organizację Biura GIODO jako aparatu pomocniczego wspierającego GIODO w realizacji jego działań.

Rozdział piąty i szósty pracy poświęcony jest odpowiednio opisowi i analizie zadań oraz środków działania GIODO. Celowo dokonałam podziału i wyodrębniłam w pracy zadania oraz środki działania tego organu, wskazując, iż zadania to ogólne założenia i cele, które GIODO jako organ państwowy ma obowiązek spełniać na mocy ustawy o ochronie danych osobowych w trakcie swojej działalności, zaś środki działania to przewidziane prawem mechanizmy i narzędzia, w które został wyposażony ten organ do realizacji wyznaczonych przez ustawę celów związanych z ochroną prywatności człowieka.

W rozdziale piątym są przedstawione zadania GIODO. Szczegółowo jest opisany proces kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzony przez GIODO, z uwzględnieniem założeń i charakteru kontroli funkcjonalnej, jak też opisu działań kontrolnych dokonywanych przez GIODO.

W następnej kolejności przedstawiony jest proces notyfikacyjny, tj. opis procedury rejestracji zbiorów danych osobowych, prowadzenie przez Generalnego Inspektora rejestru zbiorów danych osobowych i administratorów bezpieczeństwa informacji wraz z udzielaniem informacji o zarejestrowanych zbiorach.

W rozdziale tym jest także przeanalizowana działalność GIODO w zakresie opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych oraz inicjowania i podejmowania przedsięwzięć o charakterze edukacyjno–informacyjnym w zakresie doskonalenia ochrony danych osobowych czy uczestniczenia Generalnego Inspektora w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

Ostatni rozdział pracy zawiera opis środków działania GIODO. Scharakteryzowane są rodzaje decyzji administracyjnych wydawanych przez GIODO i procedura wydawania decyzji administracyjnych w sprawach wykonania przepisów o ochronie danych osobowych, procedura rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych, a także uprawnienia egzekucyjne GIODO w procesie egzekucji świadczeń o charakterze niepieniężnym.

W dwóch ostatnich rozdziałach zawarte są ponadto informacje i analizy dotyczące efektywności działania GIODO w zakresie realizacji zadań i środków działania GIODO.

Aby wykazać znaczenie Generalnego Inspektora jako organu ochrony prawa do prywatności i ochrony danych osobowych na tle innych organów państwowych w Polsce, potrzebne było przeprowadzenie badań podstawowych o charakterze poznawczym dotyczących stanu prawa z użyciem metody dogmatyczno-prawnej. Metoda ta jest wykorzystana przeze mnie przede wszystkim podczas analizy międzynarodowych oraz

krajowych aktów prawnych odnoszących się do zagadnień związanych z ochroną prywatności i ochroną danych osobowych. W założeniu badania miały na celu szczegółowe i kompleksowe przedstawienie teoretycznych zagadnień rozprawy doktorskiej związanych z pozycją prawno-ustrojową GIODO jako organu ochrony prawa do prywatności i ochrony danych osobowych na tle pojawiających wielu uogólnień związanych z charakterystyka działania tego organu.

Wychodząc z założenia, iż kluczowym dla ukształtowania się prawa do prywatności i prawa do ochrony danych osobowych są czynniki genetyczne, metodą, z której również skorzystałam, była metoda historyczna. Dzięki jej zastosowaniu przedstawiłam ewolucję idei prawa do prywatności i mechanizmów jego ochrony na płaszczyźnie międzynarodowej i krajowej. Metoda ta okazała się również pomocna, by ukazać rozwój i kształtu zjawisk oraz instytucji, które bezpośrednio oraz pośrednio wpłynęły na obecną pozycję, zakres działania i efektywność pracy Generalnego Inspektora Ochrony Danych Osobowych.

Kolejną metodą subsydiarnie zastosowana w pracy jest metoda porównawcza, z której skorzystałam charakteryzując międzynarodowe regulacje prawne w zakresie prawa do prywatności i ochrony danych osobowych. Co więcej, metoda ta została przeze mnie użyta przy opisie instytucji Europejskiego Inspektora Ochrony Danych oraz polskiego GIODO, a także przy opisie proponowanych zmian w ustawodawstwie unijnym odnoszących się do ochrony danych osobowych.

ROZDZIAŁ I
PRAWO DO PRYWATNOŚCI A OCHRONA DANYCH OSOBOWYCH

1. Kształtowanie się idei prawa do prywatności

Człowiek od zawsze miał chęć nieskrępowanego decydowania o swojej osobowości, o swoim życiu i o swoich sprawach osobistych, bez obaw o negatywne reakcje ze strony społeczeństwa czy środowiska. Rozwój cywilizacyjny, w tym pojawienie się nowych mediów, urządzeń technicznych oraz rozwój tych dziedzin, które pozwalają na łatwe i szybkie gromadzenie, przetwarzanie i wykorzystywanie informacji, wymusiły znaczące zintensyfikowanie działań legislacyjnych mających na celu ochronę życia prywatnego człowieka. Postęp w sferze technologicznej powodował bowiem istotne zagrożenie dla prywatności jednostki. Konieczne stało się nakreślenie przez naukę sfer wolnych od ingerencji innych osób czy podmiotów. Posiadanie prawa do własnych decyzji i wiedzy pociągnęło za sobą stopniową jurydyzację tego pojęcia. Na przestrzeni lat pojawiło się wiele opracowań naukowych, których celem było przedstawienie istoty czy określenie przedmiotu prawa do prywatności. Ochrona prywatności znalazła także swój wyraz w orzecznictwie sądowym i w aktach prawnych, w tym także o randze konstytucyjnej. Doktrynalne próby określenia pojęcia prywatności wpływają na przyjmowane rozwiązania prawne, te natomiast wyznaczają granice rozważań teoretycznych. W ten sposób narodziła się nowa naukowa dyscyplina prawnicza - nauka o prywatności[5].

Prawo do ochrony życia prywatnego należy do pierwszej generacji praw człowieka[6]. Jako prawo fundamentalne podlega ochronie w większości współczesnych systemów prawnych oraz jest zagwarantowane w prawie międzynarodowym i polskim systemie prawnym[7]. Idea prawa do prywatności kształtowała się różnie w zależności od koncepcji

---

[5] Por. M. Jagielski, *Konstytucjonalizacja ochrony prywatności,* [w:] *Konstytucjonalizm a doktryny polityczno–prawne. Najnowsze kierunki badań*, red. R.M. Małajny, Katowice 2008, s. 262.

[6] Są to fundamentalne prawa obywatelskie i polityczne formułowane na przełomie XIX i XX w. pod wpływem koncepcji liberalnych. Akcentują one konieczność zachowania pewnego obszaru wolnego od ingerencji ze strony państwa, mają zatem charakter obronny i służą wzmocnieniu autonomii jednostki. Do praw jednostki pierwszej generacji obok prawa do ochrony prywatności zaliczyć także możemy: wolność słowa, równość wobec prawa, nietykalność osobistą, ochronę życia ludzkiego. Zob. P. Kuczma, *Prawa człowieka w zarysie,* Polkowice 2012, s. 19 i n.

[7] Ochrona prywatności należy do katalogu zasadniczych praw człowieka i tak jest traktowana m. in. w: Powszechnej Deklaracji Praw Człowieka, Międzynarodowym Pakcie Praw Cywilnych i Politycznych, Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności i w wielu aktach o zasięgu regionalnym. Zob. M. Pryciak, *Prawo do prywatności*, „Studnia Erasmiana Wratislaviensia" 2010, nr 4, s. 211.

głoszonych w nauce, od roli i intencji judykatury, a także od elastyczności interpretacyjnej dokonywanej względem przepisów obowiązującego prawa[8]. Sfera prywatności była rozmaicie określana i w różnym stopniu chroniona, na co wpływ miał upływ czasu, wzorce obowiązujące w społeczeństwie, czy poziom prawa w danym państwie. Zanim w świadomości ludzkiej oraz w obrocie prawnym pojawiła się koncepcja ochrony prawa do prywatności, w systemach prawnych państw istniały określone mechanizmy i instytucje zapewniające ochronę pewnych aspektów prywatności człowieka.

Formalno-prawna ochrona prywatności zrodziła się w okresie ostatnich stu lat, jednak samo pojęcie prywatności było już znane od starożytności w pismach politycznych, religijnych, antropologicznych, czy później socjologicznych[9]. Biorąc pod uwagę wszystkie te źródła łącznie, można zasadnie twierdzić o istnieniu teoretycznych i koncepcyjnych założeń pewnego pojęcia (myśli) o prywatności[10].

Źródeł prywatności można doszukiwać się ponadto w różnego rodzaju koncepcjach filozoficzno-prawnych. W zależności od zapatrywania się na prawo do prywatności, jedni badacze uważają, iż prywatność jest cechą nierozerwalnie związaną z człowiekiem, od zawsze jemu przypisaną, lecz nie zawsze uświadamianą. Na tej podstawie źródłem prawa do prywatności był już kodeks Hammurabiego, Biblia (głównie wyjątki ze Starego Testamentu) czy Koran. Wyjątkowe znaczenie, z punktu widzenia ochrony prywatności, według takiego postrzegania prywatności jest przypisywane greckiemu, następnie przejętemu przez Rzymian, podziałowi na sprawy publiczne i prywatne.

Inni badacze pojęcie prywatności wiążą z doktryną liberalizmu, a jej genezę upatrują w prawie natury i wolności (XVII i XVIII w.), gdy wolność człowieka była stanem pierwotnym i naturalnym, a ulegała ograniczeniom jedynie na zasadzie przyzwolenia. Koncepcja ta odrzucała upatrywania korzeni prywatności tak odlegle jak w pierwszym przypadku, podkreślając, że starożytny podział na sprawy prywatne i publiczne nie przystaje do współczesnego rozumienie prywatności, a łączy je jedynie tożsamość semantyczna[11]. W opinii przedstawicieli tej teorii genezy współczesnego rozumienia pojęcia „prywatność" można doszukiwać się w dziełach przedstawicieli prawa natury i „ojców liberalizmu", tj. Grocjusza, Hobbesa, J. Locke'a, Monteskiusza czy J.J. Rousseau[12]. Uważali oni, że prawo do

---

[8] J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002, s. 286.
[9] Zob. W.G. Staples, *Encyclopedy of Privacy.Volumes 1: A-M*, Greenwood Press, s. 404-405.
[10] *Ibidem*, s. 280.
[11] M. Jagielski, *Konstytucjonalizacja…*, s. 264.
[12] Zob. W.G. Staples, *op. cit.*, s. 405-406.

prywatności jest jednym z elementów katalogu praw osobistych, które skupiają się przede wszystkim wokół idei równości i wolności osobistej. Teoria ta uwzględniała już całkowitą zmianę postrzegania statusu jednostki wraz z uznaniem jej podmiotowości wobec państwa, co dało podstawy do ukształtowania się znanego współcześnie pojęcia prywatności.

Ogromny wkład w tym zakresie wnieśli liberałowie dziewiętnastowieczni jak: B. Constant i J. S. Mill. B. Constant był prekursorem pojęcia prywatności, poprzez ustanowienie niezwykle ważnej definicji wolności. Według niego wolność oznaczała przeciwstawienie się podporządkowaniu jednostki władzy ogółu. Jak pisał, „nasza wolność powinna się zasadzać na pokojowym korzystaniu z prywatnej niezależności”[13]. Prywatność B. Constant rozumiał natomiast jako intymność, odosobnienie lub zacisze domowe, a będąc zwolennikiem rozdziału pomiędzy sferą prywatną a publiczną każdej jednostki, optował za samookreśleniem się jednostki w obiektywnej rzeczywistości rozdziału tych dwóch sfer istnienia[14].

Sednem myśli J. S. Milla była zaś pewność, że szacunek dla prywatności jest podstawą wolności, a o człowieczeństwie ludzi stanowi ich zdolność wyboru. Omylność, prawo do błędu, stanowiące istotny składnik samodoskonalenia i w konsekwencji możność wyboru zarówno dobra, jak i zła, skłoniły go do przyznania, że państwo czasami powinno naruszyć prywatność jednostki gwoli wspierania np. bezpieczeństwa społecznego, sprawiedliwości, edukacji bądź higieny[15].

Sfera prywatności jako odrębne dobro prawne podlegające ochronie jest uznawane stosunkowo od niedawna. W języku prawnym i w języku prawniczym jako odrębna kategoria jurydyczna pojawiło się dopiero pod koniec XIX w[16]. Od tego momentu pojęcie prywatności, używane w różnych kontekstach, okazało się adekwatne do opisania pewnej sfery ludzkiego życia i współcześnie określenia, takie jak: „prawo do prywatności”, „sprawy prywatne”, „ochrona prywatności”, znajdują się w powszechnym obiegu.

Nie sposób jest w tym miejscu przytoczyć kompleksowo wszystkich stanowisk oraz dzieł doktryny, które traktują wyczerpująco o historii, istocie czy definicjach prawa do prywatności. Bezsprzecznie jednak należałoby uznać, iż żaden z krajów europejskich nie może na pewno poszczycić się takimi osiągnięciami w rozwoju prawnej koncepcji ochrony prywatności jak Stany Zjednoczone[17]. Zagadnienie prywatności zostały po raz pierwszy

---

[13] Za: B. Sobolewska, M. Sobolewski, *Myśl polityczna XIX i XX w. Liberalizm*, Warszawa 1978, s. 47.
[14] B. Szyszkowski, *Beniamin Constant. Doktryna polityczno- prawna,* Warszawa-Poznań-Toruń 1984, s. 155.
[15] I. Berlin, *John Stuart Mill i cele życia*, [w:] *Cztery eseje o wolności*, red. I. Berlin, Poznań 2000, s. 260.
[16] Zob. K. Motyka, *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach”, seria: Administracja i Zarządzanie 2010, nr 85, s. 11.
[17] J. Braciak, *Prawo do prywatności,* Warszawa 2004, s. 33.

przedstawione przez dwóch amerykańskich profesorów z Harvard University: L. D. Brandeisa i S. D. Warrena, którzy w opublikowali artykuł pt. „*The Right to Privacy*”[18]. Artykuł ten był poświęcony prywatności jako autonomicznej wartości, która przez każdego „cywilizowanego człowieka” jest najbardziej ceniona[19]. To oni przypomnieli, że odwieczną zasadą *common law* jest zapewnienie ochrony osobie i jej własności. Z uwagi na stałą ewolucję życia społecznego i nowe zagrożenia dla jednostki (możliwość utrwalania obrazu i głosu, rozwój prasy), wyrazili pogląd, że chociaż prawo zwykle podąża za tą ewolucją, to od czasu do czasu konieczna jest redefinicja tej ochrony i jej zakresu. Wskazywali, że *common law* powinno uznać zakres prawa do prywatności, dowodząc, że „istnieje wspólna, niewyrażona *expressis verbis* podstawa, którą jest prawo do prywatności służące ochronie nienaruszalnej osobowości”. Wspomniani autorzy określili je jako prawo do wyłączności, tajemnicy i samotności (w sformułowaniach *„right to be alone” oraz „my home is my castle”*). S.D. Warren i L.D. Brandeis postulowali, by sądy amerykańskie wydobyły z *common law* prawo do prywatności, przyznając prywatności ochronę jako wartości samoistnej (*per se*)[20]. Przyznali przy tym, że tak jak każde inne prawo, prawo do prywatności podlega ograniczeniom i nie może być podstawą np. do zakazu publikacji na tematy interesujące dla ogółu (zwłaszcza jeśli dotyczy to osób, które same z siebie uczyniły zainteresowanie innych) lub też ujawniania informacji w okolicznościach szczególnych przewidzianych przez prawo. Wyrazili również swoje przypuszczenie, że prawo nie będzie przewidywało odszkodowania za ustne rozpowszechnianie informacji odnoszących się do prywatności osoby, jeśli rozpowszechnianie to nie spowoduje szczególnej szkody.

W owym czasie nie było jednak możliwe ustalenie zakresu przestrzennego tego prawa, stąd też należy uznać brak jednoznacznej jego definicji. W Stanach Zjednoczonych przyjęto zatem tak w doktrynie jak i w judykaturze, że na prywatność składają się cztery wielkie kompleksy zagadnień, tj.: wolność słowa i religii, prawo do decydowania o własnym życiu i zdrowiu, prawo do ochrony informacji biograficznej oraz prawo do intymności życia

---

[18] S. D. Warren, L. D. Brandeis, *The Right to Privacy*, „Harvard Law Review”, 1890, Vol. 4, s. 193-220. Artykuł był odpowiedzią autorów, na ich zdaniem nadmierne i krępujące relacjonowanie przez bostońska prasę życia prywatnego D. Warrena, przede wszystkim spotkań towarzyskich organizowanych przez jego żonę, córkę senatora Thomasa Francisa Bayarda; Zob. W.G. Staples, *op. cit.*, s. 463.

[19] Zob. M. Safjan, *Prawo do ochrony życia prywatnego,* [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, red. L. Wiśniewski, Warszawa 1997, s. 127; J.H.Moor, *The Ethics of Privacy Protection*, “Library Trends”, Summer & Fall 1990, s. 70-72.

[20] W. Sokolewicz, *Prawo do prywatności,* [w:] *Prawa Człowieka w Stanach Zjednoczonych*, red. L. Pastusiak, Warszawa 1985, s. 252.

osobistego[21]. Są to główne zagadnienia, wokół których toczy się w tym kraju dyskusja naukowa i praktyka sądowa i które wyznaczają teren konfrontacji prywatności z aspektami życia.

Koncepcja prawa do prywatności, która jest punktem wyjścia dla tworzonych nowożytnie koncepcji ochrony danych osobowych, ma także silne korzenie w prawie anglosaskim. Niektórzy badacze prawa brytyjskiego twierdzą, iż w przeciwieństwie do innych instytucji tego prawa, ta koncepcja powstała na kontynencie amerykańskim, a następnie została przejęta przez prawo brytyjskie[22]. Model konstytucjonalizacji prawa do prywatności na gruncie brytyjskim jest specyficzny, z uwagi chociażby na brak konstytucji pisanej w Wielkiej Brytanii. W brytyjskim *common law* koncepcja ochrony prywatności z kolei nigdy nie zyskała powszechnego uznania (mimo iż to na orzeczenia sądów angielskich powoływali się m. in. S. D. Warren i L.D. Brandeis). Nie jest tam traktowana jako wartość samodzielna i podlega ochronie z wykorzystaniem tradycyjnych dla brytyjskiego *common law* instrumentów prawnych.

Pierwsze próby określania prawa do prywatności i elementów go tworzących w prawie anglosaskim pojawiły się na długo przed opublikowaniem przełomowego artykułu o prawie do prywatności S. D. Warrena i L. D. Brandeisa. Jako przykład można wskazać regulację ustawy o sędziach pokoju z 1361 r., która przewidywała karę aresztu dla „podglądaczy" i podsłuchiwaczy". Podobne przesłanki leżały u podstaw instytucji miru domowego, mocno osadzonego w tradycji angielskiej. Co więcej, na uwagę zasługuje też ujęcie prawa do prywatności połączone z koncepcją prawa własności. W 1741 r. w sprawie *Pope vs. Curl*, w której chodziło o publikację przez księgarza listów od osobistości znanych w świecie literatury, Lord Kanclerz stwierdził, że słowa są własnością piszącego, a rozpowszechnianie korespondencji bez zgody autora narusza jego prywatność. Także później, Sir James Fitzjames Stephen w polemice z poglądami J.S. Milla stwierdził, iż „uznanie istnienia jakiegoś «prawa» autonomii osobistej, bez względu na to, jak będziemy je rozumieć, zawsze zawiera w sobie prawo do prywatności, choć ścisłe określenie obszaru prywatności nie jest możliwe. Prywatność powinna jednak być respektowana zarówno przez legislatorów, jak i opinię publiczną"[23].

---

[21] J. Braciak, *Prawo do prywatności*. *Praktyczne i teoretyczne problemy współczesnego państwa*, „Zeszyty Luksemburskie" 2012, nr 1, s. 77.
[22] Zob. L. Kański, *Prawo do prywatności, nienaruszalność mieszkania i tajemnicy korespondencji*, [w:] *Prawa człowieka. Model prawny*, red. R. Wieruszewski, Wrocław 1991, s. 322-323.
[23] J. Braciak, *Prawo do prywatności…,* s. 31-32.

Wszystkie te oraz inne próby definiowania prawa do prywatności na gruncie anglosaskim wskazują, iż jest to zagadnienie interpretowane różnorodnie, a wiele składowych elementów stanowi o jego istocie. Chociaż termin „prywatność" znajdował się i nadal znajduje w wielu aktach prawnych na świecie, to rdzennie pochodzi on właśnie od angielskiego słowa „*privacy*". „*Privacy*" odnosi się do określenia intymności, odosobnienia, zaciszy, odcięcia (się) od świata, unikania rozgłosu czy utrzymania czegoś w tajemnicy[24]. Takie ujęcie prywatności jest nierozerwalnie związane z wolnością, intymnością i indywidualnym statusem jednostki, dając bardzo szeroką możliwość interpretacyjną w zakresie definicji dóbr chronionych w obrębie prywatności człowieka.

Poza Ameryką i systemem anglosaskim, także i kraje niemieckojęzyczne poszczycić się mogą w historii próbami wskazania praw i wartości składających się na pojęcie prywatności jednostki. Nie negując wpływu, jaki artykuł S. D. Warrena i L.D. Brandeisa wywarł na rozwój prawnej ochrony życia prywatnego, należy jednak zauważyć, że w doktrynie niemieckiej już w XVII czy XIX w. można było spotkać publikacje poświęcone kategorii praw znanych jako „prawa osobistości" (np. dzieła K. Garaisa, O. Gierkego, J. Kohlera). Idee tam głoszone wniosły pionierski wkład w rozwój prawa do prywatności, gdyż stały się inspiracją dla wykształconego później „prawa do swobodnego rozwoju osobowości" (*allgemeines Persönlichkeitsrechte*), które jest - mocno rzecz upraszczając - innym ujęciem prawa do prywatności. J. Kohler głosił, iż „jednostce trzeba pozwolić, by była aktywna, tj. by mogła realizować swoje pragnienia i ujawnić światu swą osobowość, albowiem kultura może rozkwitać tylko wówczas, gdy każdy może się swobodnie rozwijać poddając swe umiejętności własnej woli". Definiował swoje prawo jako prawo żądania, aby osoba uznana była za pełnowartościową, moralną i duchową osobowość i by była chroniona w swym niewzruszonym roszczeniu o byt i rozwój[25].

Pomimo jednak poparcia dla idei ogólnego prawa do osobowości czołowych przedstawicieli doktryny, niemiecki ustawodawca odrzucił konstrukcję prawnej ochrony osobowości i nie umieścił w uchwalonym w 1868 r. ogólnoniemieckim kodeksie cywilnym Bürgerliches Gesetzbuch BGB (poza prawem do nazwiska i „dobrami życiowymi" jak: życie, zdrowie, wolność, nietykalność cielesna i inne niż własność) prawa do ochrony dóbr

---

[24] *Oxford Wordpower. Słownik angielsko-polski z indeksem polsko-angielskim*, Oxford University Press 1997, red. J. Philips, s. 596.

[25] Zob. M. Lijowska, *Koncepcja ogólnego prawa osobistości w niemieckim i polskim prawie cywilnym*, „Kwartalnik Prawa Prywatnego" 2001, z. 4, s. 718-720.

osobistych[26]. Także w orzecznictwie, z uwagi na zbyt dużą możliwość interpretacyjną i nieprecyzyjność określeń, co zagrażało bezpieczeństwu obrotu prawnego, rezygnowano z możliwości uznania ogólnego prawa do osobowości[27].

Niemiecka koncepcja ochrony prywatności jednostki zaistnieć mogła realnie dopiero po II wojnie światowej. Ogromne znaczenie dla koncepcji prawa do osobowości miało uchwalenie Ustawy Zasadniczej RFN w 1949 r., chociaż niemiecka ustawa, podobnie jak amerykańska, nie zawiera bezpośredniego odwołania do prywatności. Podstawą do wyinterpretowania prawa do prywatności w Niemczech jest art. 2 Ustawy Zasadniczej, stwierdzający, że „1. Każdy ma prawo do swobodnego rozwoju swej osobowości, o ile nie narusza praw innych i nie staje w sprzeczności z porządkiem konstytucyjnym albo nakazami moralności. 2. Każdy ma prawo do życia i nietykalności cielesnej. Wolność osobista jest nienaruszalna. Wkraczać w te prawa wolno jedynie na podstawie ustawy". W orzecznictwie Federalnego Trybunału Konstytucyjnego określenia zawarte w art. 2 Ustawy Zasadniczej (zwłaszcza swobodnego rozwoju osobowości - *die freie Entfaltung seiner Persönlichkeit*) stały się podstawą wypracowania całej konstytucyjnej koncepcji ochrony prywatności w Niemczech.

Także wydanie 25 maja 1954 r. przez Trybunał Związkowy orzeczenia, w którym Trybunał jednoznacznie opowiedział się za koncepcją *allegemeines Persönlichkeitsrechte,* było przełomowe. W orzeczeniu tym, które przeszło do historii jako *casus Leserbrief* (list czytelnika), Trybunał uznał, że listy i inne prywatne zapiski nie mogą być publikowane bez zgody autora, nawet jeśli nie wykazują cech decydujących o uznaniu ich za utwór w rozumieniu prawa autorskiego[28]. Uznanie ogólnego prawa do osobowości doprowadziło zatem do rozszerzenia nie tylko jego zakresu, ale i środków ochrony prawnej.

Według S. Stömholma prawoznawstwo niemieckie odegrało w wypracowaniu prawnej koncepcji prywatności rolę bliską tej, która była udziałem prawników amerykańskich[29]. Wydaje się jednak, że niemiecka koncepcja nie była tożsama w stosunku do amerykańskiej, (chociaż widoczne są pewne podobieństwa), stąd słuszniej byłoby mówić o koncepcji prawa do prywatności i prawa do osobowości, jako że wyrastały z zupełnie odmiennego podłoża systemów prawnych.

---

[26] Zob. K. Styrna-Bartman, E. Tuora - Schwierskott, *Niemiecki Kodeks Cywilny. Przepisy §1- 432 niemieckiego kodeksu cywilnego z wyjaśnieniami w tłumaczeniu na język polski,* Regensburg 2014, s. 12 i n.

[27] B. Kordasiewicz, *Cywilnoprawna ochrona prawa do prywatności*, „Kwartalnik Prawa Prywatnego" 2000, z. 1, s. 21.

[28] BGHZ 13, 334.

[29] Autor podkreśla, co prawda, iż chodzi o teoretyczną koncepcję, gdyż praktyczną jej realizacja nie nastąpiła przed końcem II wojny światowej. Za: L. Kański, *Prawo…*, s. 324.

Analizując początki i rozwój koncepcji prawa do prywatności warto także przybliżyć francuską idee prawa do prywatności. Francuskie piśmiennictwo rozwój koncepcji prawa do prywatności datuje w 1791 r., tj. wraz z uchwaleniem pierwszej francuskiej konstytucji. Wśród licznych gwarancji wolności obywatelskich konstytucja z 1791 r. wymieniała m. in swobodę prasy, ograniczoną jednak przez zakaz głoszenia „kalumnii i oszczerstw dotyczących życia prywatnego”[30]. Wraz z uchwaleniem w 1789 r. Powszechnej Deklaracji Praw Człowieka i Obywatela zagwarantowano każdemu obywatelowi prawo do „wolnego przekazywania myśli i opinii”, co z kolei doprowadziło do rozwoju w rewolucyjnej Francji prasy, a na przestrzeni kolejnych lat przyniosło wręcz lawinę nowo powstałych tytułów, w tym dzienników, a także pism salonowych i pism bulwarowych. Pisma bulwarowe korzystając z wolności słowa i wolności prasy publikowały sensacje niejednokrotnie opisując soczystym językiem wydarzenia towarzyskie wyższych sfer, co skłoniło do debat na tematy zakresu swobód dziennikarskich oraz zakresu informacji publicznej i prywatnej[31].

Francuskie *droits de la personnalite* pojawiło się w XIX w. i zostało ono ostatecznie sformułowane jako zespół norm chroniących nazwisko, wizerunek i prywatną sferę życia człowieka. Do tego czasu sądy udzielały ochrony prywatnej sfery życia człowieka, interpretując art. 675 Kodeksu Napoleona („Jeden z sąsiadów nie może bez zgody innego urządzać w murze wspólnym żadnego okna lub jakiegokolwiek innego otworu, chociażby o oszkleniu nieprzeźroczystym”) oraz art. 1382 Kodeksu Napoleona, przewidujący naprawienie szkody wyrządzonej innej osobie przez naruszenie tajemnicy listów, nadużycie nazwiska czy nieuprawnioną publikację wizerunku („Wszelki czyn, wyrządzający drugiej osobie szkodę, obowiązuje tego, kto się go dopuścił, do jej naprawienia”). Pierwsza wielka kodyfikacja prawa cywilnego nie zawierała jednak jeszcze żadnych postanowień co do zadośćuczynienia za krzywdy osobiste i szkody niemajątkowe[32]. Dopiero ustawa o prawie prasowym uchwalona w 1868 r. przewidywała sankcję grzywny za opublikowanie materiałów zawierających informacje z życia prywatnego osób trzecich[33]. Kolejne próby reform w zakresie prawa do prywatności nastąpiły w XX w. W 1920 r. przygotowano reformę kodeksu

---

[30] Rozwój prawnej ochrony życia prywatnego miał jednak swój rodowód dużo wcześniej, wraz z rozwojem przywilejów szlacheckich we Francji, które obejmowały m. in. zakaz sporządzania publicznej dokumentacji obciążeń majątkowych, mogącej naruszyć „dobrą sławę wielce szanowanych rodzin”. Przepis ten jednak dotyczył tylko najwyżej urodzonych a nie wszystkich obywateli Francji.

[31] Zob. A. Corbain, *Kulisy*, [w:] *Historia życia prywatnego. Tom 4: Od rewolucji francuskiej do I wojny światowej,* red. M. Perrot, Ossolineum 2006, s. 469-470.

[32] S. M. Grzybowski, *Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego*, Warszawa 1957, s. 33-34.

[33] Zob. Casus Rachel (uznawany przez doktrynę za pierwszą francuską sprawę, w której prywatność została objęta ochroną na gruncie prawa deliktowego), casus Mickiewicz, casus Dumas czy casus Moittesier.

cywilnego, która nie weszła jednak w życie, a następnie w 1944 r. nowelizację prawa prasowego, która z kolei nie usatysfakcjonowała zwolenników reform prawa do prywatności, gdyż tylko ograniczała się do zmian przepisów o zniesławieniu. Poważniejsze zmiany wprowadziła dopiero ustawa o wzmocnieniu gwarancji praw obywatelskich z 1970 r., czego następstwem było również wprowadzenie do kodeksu cywilnego art. 9[34]. Ustawodawca we francuskim kodeksie cywilnym (*code civil*) wyraźnie wyodrębnia prawo do ochrony życia prywatnego oraz sferę intymności, przez zastosowanie odmiennych sankcji za ich naruszenie[35]. W art. 9 § 1 została sformułowana ogólna zasada, zgodnie z którą każdy ma prawo do poszanowania jego życia prywatnego, jednak bez wskazania wprost definicji pojęcia prywatności. W art. 9(2) odnoszącym się do środków ochrony natomiast użyte zostało pojęcie „intymności życia prywatnego", co wskazuje na istnienie odrębnych środków ochrony, gdy dochodzi do naruszenia intymności. Wydaje się zatem, że we francuskim prawie cywilnym sfera intymności stanowi podsferę życia prywatnego podlegającą bardziej wzmożonej ochronie[36].

W obecnie obowiązującej konstytucji francuskiej z 1958 r. brak jest regulacji odnoszących się do prawa do prywatności (ani jakichkolwiek praw podstawowych)[37]. Francuska Rada Konstytucyjna w 1995 r., łącząc pojęcie życia prywatnego i wolności osobistej, uznał, że prawo do prywatności zawarte jest w sposób dorozumiany w art. 66 francuskiej konstytucji[38]. Prawo do życia prywatnego we Francji zostało także wzmocnione poprzez ratyfikację postanowień Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności[39].

---

[34] Zob. K. Sójka-Zielińska, *Kodeks Napoleona. Historia i współczesność*, Warszawa 2008, s. 123-157; K. Sójka-Zielińska, *Wielkie kodyfikacje cywilne. Historia i współczesność*, Warszawa 2009, s. 150 i n.

[35] Tekst *Code Civil* w wersji angielskiej jest dostępny na stronie: http://www.napoleon-series.org/research/government/c_code.html. Kopia cyfrowa polskiego wydania dzieła z 1810 r. dostępna jest na stronie: http://www.bibliotekacyfrowa.pl/dlibra/docmetadata?id=6697&from=publication

[36] J. Sieńczyło-Chlabicz, *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Kraków 2006, s. 110.

[37] Konstytucja V Republiki Francuskiej z 1958 r. praktycznie milczy na temat praw podstawowych i swobód publicznych. Zob. M. Verpeaux, *Rada Konstytucyjna a ochrona praw podstawowych*, „Przegląd Sejmowy" 2010, nr 1, s. 104; Z. Jarosz, *Konstytucja V Republiki Francuskiej*, Warszawa 1997, s. 46 i n.

[38] Orzeczenie *Conseil Constitutionnel* z dnia 18 stycznia 1995, No. 94-352.

[39] Dz. U. z 1998 r. Nr 147, poz. 962; tekst Konwencji dostępny na stronie: http://www.giodo.gov.pl/564/id_art/617/j/pl/.

2. Pojęcie prawa do prywatności

Sprawą bardziej skomplikowaną niż przedstawienie genezy prawa do prywatności jest podanie jej definicji. „Etymologicznie słowo prywatność wywodzi się od łacińskiego słowa *privus* tłumaczonego jako własny, wolny od, pojedynczy. To z niego wykształcił się przymiotnik *privatu*s, służący do określenia prywatnej własności czy też osób niepełniących funkcji publicznych”[40]. Jak pisał W. Szyszkowski, „pisanie o prywatności w prawie nie jest rzeczą łatwą, przede wszystkim z powodu niesprecyzowania tego pojęcia i z powodu używania go w wielu znaczeniach. Pojęcie to, tak długo nieznane słownikom języka, jest nowe w świecie, a jednocześnie odpowiada starej idei”[41].

Ze wszystkich praw jednostki zamieszczanych w konstytucjach państw, a także międzynarodowych katalogach praw człowieka, prawo do prywatności jest jednym z najtrudniejszych do wyjaśnienia i opisania. Prawo do prywatności jest niejednoznacznym zjawiskiem, gdyż z jednej strony wielokrotnie podejmowane są dyskusje w zakresie poszerzenia ochrony prawa do prywatności, co jest spowodowane zwiększeniem ilości zagrożeń w stosunku do prywatności jednostki, zaś z drugiej strony postuluje się jak najszersze zagwarantowanie prawa do prywatności człowiekowi z możliwością nieograniczonej wręcz niezależności i wolności, a z ograniczeniem do minimum niezbędnej ingerencji ze strony władzy czy wyspecjalizowanych podmiotów.

Trudno jest znaleźć jednoznaczną definicję prywatności w systemach prawnych poszczególnych państw, ponieważ ustalenie pojęć prawnych jest w większej mierze domeną doktryny prawa i orzecznictwa niż ustawodawcy[42]. Polski Sąd Najwyższy w jednym ze swoich orzeczeń stwierdził, że pojęcie „prywatna sfera życia” nie może być absolutyzowane, czy też ujmowane w ramy sztywnej definicji, ponieważ z uwagi na stopień swojej ogólności wymaga dokonywania wykładni przy uwzględnieniu konkretnych okoliczności, charakteryzujących określoną sytuację[43].

Prawo do prywatności jest pojęciem złożonym i szerokim, a do tego zmiennym w czasie. Autorzy próbując skonstruować najbardziej precyzyjną definicję prywatności wielokrotnie skupiali się na określeniu sfer kształtujących owe prawo, które także należy

---

[40] M. Puwalski, *Prawo do prywatności osób publicznych*, Toruń 2003, s. 14.
[41] W. Szyszkowski, *Rozważania o prywatności,* [w:] *Wybrane problemy prawa konstytucyjnego*, red. W. Skrzydło, Lublin 1985, s. 189.
[42] J. Hołda, Z. Hołda, J.A. Rybczyńska, *Prawa człowieka. Zarys wykładu*, Warszawa 2008, s. 114.
[43] Wyrok SN z dnia 24 maja 1999 r., II CKN 349/98, OSNC 1999, nr 12, poz. 212.

chronić w ramach mechanizmów wykształconych do ochrony prywatności[44]. W doktrynie amerykańskiej wielokrotnie wskazywano, iż nie istnieje żadna spójna i powszechnie akceptowalna definicja prywatności, o czym świadczy m. in. trwający w doktrynie amerykańskiej spór o zakres prywatności[45]. Wszelkie pojęcia konstruowane w zakresie prawa do prywatności zwykle są ogólne i mają charakter kierunkowy, a jeszcze częściej są to definicje negatywne, tzn. określające czynniki czy zjawiska powodujące naruszenie prawa do prywatności. Pojawiają się także głosy krytyczne, które odwołując się do szerokiego, nieokreślonego zakresu prawa do prywatności stwierdzają, że prawo do prywatności „znaczy już tak wiele, że nie znaczy nic"[46]. Brak jednej, powszechnej definicji prawa do prywatności nie oznacza jednak braku znaczenia tego terminu, ponieważ „w pewnym sensie wszystkie prawa człowieka są przejawami jego prawa do prywatności"[47].

Nie ulega wątpliwości, że jako pierwsi definicję prywatności podali prawnicy systemu *common law,* S. D. Warren i L. D. Brandeis, określając prywatność jako prawo do bycia i pozostawania w spokoju, tj. taki stan rzeczy, w którym jednostka pozostawiona byłaby samej sobie we wszystkich istotnych sprawach życia fizycznego i duchowego (nie związanych z prowadzeniem działalności publicznej) wtedy, gdy ona sama tego sobie życzy i gdy nie stoi to w konflikcie z doniosłymi interesami ogólnymi oraz prawami i wolnościami osób trzecich.

Inni autorzy przyjmujący wąskie rozumienie prywatności, zajmując się tylko tym zagadnieniem zakładają, iż prywatność stanowi pewnego rodzaju stan niezależności, w ramach którego jednostka może decydować o zakresie i zasięgu udostępniania innym informacji o sobie i swoim życiu[48]. Tak np. L. Nizer definiuje prywatność jako prowadzenie egzystencji samotnej i anonimowej[49]. A. Westin nawiązuje do wąskiego pojmowania prywatności jako stanu, w ramach którego jednostka decyduje o zakresie i zasięgu informacji udostępnianych i komunikowanych innym osobom[50]. H. Gross uważa, że prywatność jest takim stanem życia ludzkiego, w którym zapoznanie się z osobą czy sprawami jej życia o charakterze osobistym jest ograniczone[51]. Także A. Miller podkreśla, że podstawowym

---

[44] Zob. R. Gavison, *Privacy and the Limits of Law*, „The Yale Law Journal Company", Vol. 98, No. 3, January 1980, s. 424 i n.
[45] Zob. J. Sieńczyło-Chlabicz, *op. cit.*, s. 96.
[46] Por. K. Motyka, *Prawo do prywatności i dylematy współczesnej ochrony praw człowieka*, Lublin 2006, s. 138.
[47] Zob. J. Braciak, *Prawo do prywatności*. *Praktyczne…*, s. 76; A. Mednis, *Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?*, [w:] *Prywatność a jawność - bilans 25-lecia i perspektywy na przyszłość,* Warszawa 2016, s. 8 i n.
[48] Por. Ł. Kołodziejczyk, *Prywatność w Internecie*, Warszawa 2014, s. 15.
[49] Zob. A. H. Robertson, *Privacy and Human Rights*, Manchester University 1973, s. 20.
[50] H. Gross, The Concept of Privacy, „New York University Law Review" 1967, vol. 42, s. 35-36; A. Westin, *Privacy and Freedom*, New York 1967, s. 7.
[51] H. Gross, *op. cit.*, s. 35-36.

atrybutem efektywnego prawa do prywatności jest zdolność jednostki do kontrolowania obiegu informacji odnoszącej się do jej osoby[52].

Wśród przedstawicieli polskiej doktryny i orzecznictwa także istnieje duża rozbieżność poglądów, co do wskazania znaczenia i zakresu pojęcia prawa do prywatności. Obecnie w doktrynie spotyka się różne ujęcia tego prawa, zaś terminologia, za pomocą której próbuje się zakreślić materię, składającą się na pojęcie prawa do prywatności, nie jest jednolita. Szczegółową analizę koncepcji dotyczących prywatności dokonała J. Sieńczyło-Chlabicz, która w polskiej doktrynie wyodrębnia następujące sposoby ujęcia prawa do prywatności:

1) prywatność rozumiana jako prawo do pozostawienia w spokoju, prawo do wolności od ingerencji innych;
2) prywatność jako prawo do samookreślenia i rozwoju osobowości;
3) prywatność jako autonomia jednostki, w szczególności jako autonomia informacyjna;
4) prywatność jednostki ludzkiej ujmowana jako katalog określonych okoliczności objętych sferą prywatności[53].

Najpełniejsze określenie prawa do prywatności w polskiej doktrynie zaproponował A. Kopff, który jako pierwszy polski autor postulował, by prawo do prywatności uznane zostało za dobro osobiste podlegające ochronie prawnej. Przyjętym przez niego założeniem było wyodrębnienie prawa do prywatności w sposób formalny. A. Kopff zainspirowany rozwojem doktryny i orzecznictwa w USA i w Europie Zachodniej, przytoczył argumenty za objęciem ochroną sfery życia prywatnego jednostki zawartej w treści art. 23 i art. 24 k.c. Wskazywał, iż „dobrem osobistym w postaci życia prywatnego jest to wszystko, co ze względu na uzasadnione odosobnienie się jednostki od ogółu służy jej do rozwoju fizycznej lub psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej" oraz że „każda jednostka winna mieć możność samodzielnego kształtowania swojej osobowości oraz swego losu według własnej woli oraz żądania, by życie to nie było przedmiotem budzącego sensację zainteresowania innych ludzi"[54].

Zaproponowana teoria A. Kopffa nawiązywała także do poglądów niemieckiej teorii sfer, w której prawo do prywatności objęte jest koncepcją jednolitego prawa osobowości,

---

[52] A. R. Miller, *The Assault on Privacy,* Ann Arbor 1971, s. 24-25.
[53] J. Sieńczyło-Chlabicz, *op. cit*., s. 97.
[54] A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1971, t. XX, s. 38.

obejmującego m. in. prawo do ochrony życia prywatnego. Autor podjął próbę utożsamienia tego prawa z pojęciem: „sfery życia osobistego", w ramach którego wyróżnił: sferę intymności i prywatności oraz powszechnej dostępności, rozciągającej się poza dwiema wskazanymi sferami. Sferę tę tworzą wewnętrzne, intymne, osobiste przeżycia człowieka, o których informacje przekazywane są tylko najbliższym osobom. Sfera życia prywatnego ma już szerszy zakres, gdyż obejmuje okoliczności i zdarzenia z życia osobistego i rodzinnego, które są dostępne z reguły rodzinie, przyjaciołom, znajomym. Sfera ta nie podlega również tak ścisłej ochronie jak sfera intymna i istnieją przesłanki uzasadniające ingerencję w tę sferę osób trzecich. Sfera powszechnej dostępności jest z kolei poza ochroną[55]. Jakkolwiek propagowana przez A. Kopffa koncepcja ogólnego prawa osobistości nie spotkała poparcia w polskiej doktrynie[56] i nadal jest poglądem wyrażanym przez mniejszość, stanowisko dotyczące uznania sfery życia prywatnego za dobro osobiste objęte ochroną prawa cywilnego bez wątpienia można uznać za *communis opinio doctorum*[57].

Nowatorskie ujęcie prawa do prywatności zakłada, że prywatność to dobro autonomiczne, którego najistotniejszym składnikiem jest prawo do odosobnienia. Prawo do odosobnienia w sensie normatywnym oznacza uprawnienie jednostki do samoistnego kształtowania życia, gdy jej sfera prywatności jest niedostępna dla innych i wolna od jakichkolwiek ingerencji. Sfera ta ma podlegać ochronie dlatego, że przyznaje się każdej osobie prawo do wyłącznej kontroli tych dziedzin życia, które nie dotyczą innych, a w których wolność od ciekawości innych jest warunkiem rozwoju jednostki[58]. Co więcej, wartości z nią związane nie muszą być powiązane z jakimkolwiek innym prawem czy interesem jednostki, gdyż jednostka nie jest zobligowana, aby udowadniać cele czy powody zakazu ingerencji w swoją prywatność, powołując się na tradycyjnie uznawane przez prawo dobra jak: dobre imię, tajemnicę korespondencji czy poszanowanie własnej integralności[59].

M. Safjan podkreśla, że najistotniejszym składnikiem prawa do prywatności jest właśnie prawo do odosobnienia, natomiast w sensie normatywnym zakłada „uprawnienie

---

[55] K. Degórska, *Prawo do ochrony życia prywatnego i rodzinnego*, [w:] *Prawa i wolności I i II generacji*, red. A. Florczak, B. Olechów, Toruń 2006, s. 147.

[56] Analogiczna do zaproponowanej przez A. Kopffa koncepcja prywatności została stworzona przez Nordycką Konferencję Prawników w Sztokholmie w 1967 r. W konferencji tej uczestniczyli przedstawiciele doktryny prawniczej z różnych krajów i opracowali najbardziej znaną definicję prawa do prywatności. Opracowali deklarację, w której wskazali na dziesięć praw podmiotowych objętych prawem do prywatności. Według definicji Nordyckiej Konferencji Prawników prywatność to „prawo do bycia pozostawionym w spokoju, do prowadzenia własnego życia z minimalnym stopniem ingerencji ze strony osób trzecich".

[57] B. Kordasiewicz, *Cywilnoprawna…*, s. 24.

[58] J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie…,* s. 293.

[59] M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6, s. 127.

jednostki do takiego kształtowania sfery życia, aby była ona niedostępna dla innych i wolna od ingerencji”[60]. Autor ten twierdzi, że prywatność to „obszar niedostępności, chroniony przed ciekawością i wścibstwem innych, sfera wolna od zewnętrznych ingerencji, w której każdy ma prawo schronić się przed innymi”[61]. Prywatność podlegać ma ochronie „dlatego i „tylko” dlatego, że przyznaje każdej osobie prawo do wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a której wolność od ciekawości innych jest swoistą *conditio sine qua non* swobodnego rozwoju jednostki”[62].

Koncentrując się na koncepcji prywatności określanej jako prawo do samookreślenia i rozwoju osobowości warto odwołać się do stanowiska przedstawionego przez M. Wilda, które zakłada, że jednym z komponentów tak właśnie rozumianego prawa do prywatności jest samookreślenie informacyjne, w którego ramach jednostka może decydować czy, kiedy i w jakich granicach publikowane będą informacje na jej temat[63]. S. Grzybowski wskazuje, iż prywatność oznacza nie tylko prawo do życia w sposób zgodny z własnym życzeniem i bez kontroli innych, lecz w pewnym stopniu także prawo rozwoju i realizacji własnej osobowości[64]. Również Z. Mielnik twierdzi, że prywatność to „stan, w którym jednostka podejmuje decyzje dotyczące jej osoby bez ingerencji ze strony osób trzecich” oraz „stan, w ramach którego jednostka decyduje o zakresie i zasięgu informacji udostępnianych i komunikowanych innym osobom”[65].

Prywatność bywa określana także jako autonomia jednostki. Grecka etymologia tego pojęcia, złożonego z dwóch członów *auto-* samodzielnie, dla siebie i *nomos-* prawo, odpowiada w języku polskim wyrażeniu „samostanowienie”[66]. Autonomia jednostki to przede wszystkim jej prawo do decydowania o swoim życiu osobistym, to jej swoboda decyzyjna i kształtowanie swojego życia w drodze samodzielnie podejmowanych decyzji, zgodnych z własnym systemem wartości. Zwolennikiem tak określanej prywatności jest przede wszystkim M. Safjan. Autor ten słusznie zauważa, że prawo do prywatności to prawo do wyznaczenia przez jednostkę obszaru odosobnienia, wolnego od ingerencji ze strony władzy

---

[60] Zob. M. Safjan, *Prawo do ochrony…*, s. 71.
[61] M. Safjan, *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych*, „Kwartalnik Prawa Prywatnego” 2000, z. 1, s. 232.
[62] M. Safjan, *Prawo do prywatności…*, s. 128.
[63] Zob. M. Wild, *Ochrona prywatności w prawie cywilnym (koncepcja sfer a prawo podmiotowe)*, „Państwo i Prawo” 2001, nr 4, s. 58.
[64] S. M. Grzybowski, *Ochrona…*, s. 78.
[65] Z. Mielnik, *Prawo do prywatności (wybrane zagadnienia)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 1996, nr 2, s. 30.
[66] M. Safjan, *Granice autonomii człowieka w prawie współczesnym*, „Rocznik Polskiej Akademii Umiejętności”, 2002/2003, s. 134.

publicznej i innych podmiotów, a także jest ono „manifestacją wolności jednostki od ingerencji państwa, tarczą ochronną wobec omnipotencji władzy publicznej”[67].

L. Kański ujmując prywatność jako autonomię jednostki wskazuje, że jest to stan pewnego rodzaju niezależności, w ramach którego jednostka może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu[68]. Według tego autora podstawą całej konstrukcji prywatności jest dysponowanie przez jednostkę informacją, ale również swoboda podejmowania decyzji przez jednostkę w ważnych dla niej życiowych sprawach, bez ingerencji innych.

Również J. Wawrzyniak określa prywatność jako autonomię jednostki, jako swobodę podejmowania decyzji w ważnych życiowych sprawach jednostki, bez nacisku ze strony osób trzecich. Autor ten definiuje prywatność jako przestrzeń wolnego poruszania się, bądź jako domenę autonomicznej aktywności jednostki, wolnej od kontroli osób trzecich. Co więcej, uważa on, że prywatność obejmuje sferę aspiracji, dążności oraz tych rodzajów aktywności, które nie podlegają zewnętrznej kontroli[69].

Na prywatność człowieka składa się wiele okoliczności. Prywatność jest pojęciem bardzo szerokim i złożonym, a swoim zasięgiem obejmuje zespół wartości, wśród których znajdują się: dobre imię, wizerunek, życie osobiste, wolność, tajemnica danych osobowych, przeszłość danej osoby[70]. Według B. Michalskiego prywatność to „dobro intelektualne lub materialne jednostki, rodziny lub grupy towarzyskiej wykorzystywane w granicach dozwolonej i chronionej przez prawo sfery pozapublicznej”[71].

W zakresie autonomii jednostki ważną rolę w dzisiejszych czasach odgrywa autonomia informacyjna. Jest ona rozumiana jako decydowanie o ujawnianiu czy dzieleniu się informacjami o sobie z rożnych płaszczyzn życia człowieka, a także wszelkiego rodzaju aktywność jednostki, jej obecność czy wypowiedzi, dzielenie się informacjami na swój temat czy kształtowanie swoją postawą i zachowaniem wizerunku publicznego. W połączeniu jednak z nowoczesnymi technologiami umożliwiającymi ingerencję w prywatność człowieka oraz nierzadko dobrowolnym ujawnianiem informacji na swój temat szerokim kręgom informacyjnym przez dysponentów dóbr (Facebook, Instagram, Linkedin, Snapchat),

---

[67] Por. M. Safjan, *Refleksje…*, s. 232.
[68] L. Kański, *Prawo…*, s. 328.
[69] J. Wawrzyniak, *Prawo do prywatności. Zarys problematyki*, Warszawa 1994, s. 5-8.
[70] K. W. Kubiński, *Ochrona życia prywatnego człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny”1993, nr 1, s. 61.
[71] B. Michalski, *Podstawowe problemy prawa prasowego*, Warszawa 1998, s. 51.

dochodzi do zagrożenia autonomii informacyjnej[72]. W naczelnej zasadzie stworzonej przez S. D. Warrena i L. D. Brandeisa, że dobrowolne ujawnianie informacji ogranicza prawo (ang. *„The right to privacy ceases upon the publication of the facts by the individual, or with his consent”*, tj. „Prawo do prywatności upada w razie publikacji faktów na temat jednostki lub w razie jej zgody na to”) istotą jest zatem element woli. To wola człowieka odgrywa decydującą rolę w zakreślaniu granic prawa do prywatności każdej jednostki. Granice autonomii informacyjnej kształtuje indywidualnie każdy człowiek, który sam decyduje ile i jakie kategorie informacji udostępnia poza zakres swojej osoby. Prawo pozytywne co prawda niekiedy obiektywizuje zakres prywatności i określa jej granice, ale zazwyczaj po to, aby ograniczyć czysto wolicjonalne rozszerzenie tej kategorii na informacje niezbędne z punktu widzenia społeczności i państwa[73].

Według powszechnie akceptowanej definicji prawo do ochrony życia prywatnego jest prawem do ochrony sfery, która nie jest bezpośrednio związana z wykonywaniem przez osobę uprawnioną zadań i kompetencji organów władzy publicznej oraz dokonywaniem innych czynności i prowadzeniem działalności o publicznym zasięgu i znaczeniu[74]. Tak pojmowana prywatność odnosi się do sfery życia osobistego, rodzinnego, towarzyskiego, nienaruszalności mieszkania czy tajemnicy korespondencji, ale i niekiedy do sfery życia zawodowego.

Termin „życie prywatne” obejmuje integralność fizyczną i psychiczną osoby ludzkiej[75]. Prywatność jako prawo decydowania o sobie w znaczeniu własnej cielesności, (prywatność fizyczna) rozumiana jest jako prawo decydowania o własnym ciele i przemianach, jakim podlega[76]. Takie ujęcie prywatności jest przede wszystkim następstwem postrzegania ciała, a „ciało przestało być pomijanym w świadomości społecznej obiektem, przeciwnie – współcześnie stanowi centralny punkt zainteresowania społecznych relacji, jest istotnym elementem poczucia tożsamości i sposobem interakcji”[77]. Wiąże się z tym szereg

---

[72] Ang. *overshare* oznaczające nadmierne dzielenie się, a nawet obarczanie audytorium szczegółami i informacjami ze swojego życia ponad miarę i ponad potrzebę, zdobyło w przyznawanym przez Webster Dictionary w 2008 r. tytuł „Słowa Roku”. Zob. A. Młynarska-Sobaczewska, *Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej*, „Przegląd Prawa Konstytucyjnego” 2013, nr 1, s. 42.

[73] *Ibidem*, s. 43.

[74] P. Winczorek, *Komentarz do Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r*., Warszawa 2000, s. 66.

[75] Z. Radwański, *Zarys części ogólnej prawa cywilnego*, Warszawa 1979, s. 133.

[76] Zob. w orzeczeniu w sprawie *Roe vs. Wade* w 1973 r. Sąd Najwyższy w USA stwierdził, że prawo do prywatności chronione XIV poprawka do Konstytucji zawiera także prawo kobiety do przerwania ciąży; 410 U.S. 113.

[77] A. Młynarska-Sobaczewska, *op. cit.*, s. 40.

elementów tworzących prywatność fizyczną, do których można zaliczyć dietę, higienę, gimnastykę czy zabiegi upiększające.

Prywatność obejmuje też indywidualne cechy zawierające informacje o jednostce jak głos, wizerunek, ale i wszelkie fakty i dane o najbardziej osobistych przymiotach osoby, a więc o życiu seksualnym, stanie zdrowia czy przeszłości[78]. Także sprawy dotyczące stanu zdrowia, sprawności fizycznej, braków lub różnych kalectw, a także kult bliskich osób zmarłych odnoszą się do prywatności człowieka[79].

Według P. Suta prywatność dotyczy wszystkich stosunków jednostki z najbliższym otoczeniem i temu otoczeniu dostępnych[80]. Zdaniem J. Serdy przez sferę życia prywatnego rozumieć należy zdarzenia z życia rodzinnego jednostki, takie jak urodzenie, małżeństwo, rozwód i śmierć[81]. Sfera życia rodzinnego będąca składnikiem życia prywatnego jednostki wyznacza zakaz ingerencji w sprawy rodzinne i prawo do ochrony przed taką ingerencją, obejmując naruszenia z zakresu stanu cywilnego, nazwiska jako wyrazu przynależności do danej rodziny, naruszenia lub rozpowszechniania informacji dotyczących relacji wewnątrzrodzinnych lub statusu materialnego jej członków czy prawo do ujawniania ojcostwa[82]. Naruszeniem prywatności jest także zachowanie godzące w spokój psychiczny *sensu stricte* jednostki, przejawiające się w podsłuchiwaniu, śledzeniu, zbieraniu informacji czy też nagrywaniu wypowiedzi[83].

A. Zielonacki opowiada się za wyodrębnieniem osobnej kategorii „rodzinnych dóbr osobistych" i wprowadzeniem wyraźnego unormowania ustawowego wartości życia rodzinnego[84]. Autor ten uznawał, że w ramach intymności życia rodzinnego chronione są takie dobra jak: stan cywilny, nazwisko i imię, osobista styczność rodziców z dzieckiem czy mir domowy. Podobny postulat zgłosił także Z. Radwański, twierdząc, że rodzina ma takie same uprawnienia do uznania jej przez społeczeństwo, jak każda osoba, a w związku z tym należy jej przyznać takie same środki ochrony, jakie służą dla ochrony własnej osobowości człowieka[85].

---

[78] K. W. Kubiński, *Ochrona*…, s. 65.
[79] B. Michalski, *op. cit.*, s. 51.
[80] P. Sut, *Czy sfera intymności jest dobrem osobistym chronionym w prawie polskim?*, „Palestra" 1995, nr 7/8, s. 54.
[81] J. Serda, Glosa do wyroku SN z dnia 6 grudnia 1990 r., I CR 575/90, OSP 1992, nr 10, poz. 214.
[82] M. Pryciak, *op. cit.*, s. 217.
[83] K. W. Kubiński, *Ochrona*…, s. 65.
[84] A. Zielonacki, *Wartości życia rodzinnego w świetle ochrony dóbr osobistych*, [w:] *Dobra osobiste i ich ochrona w polskim prawie cywilnym*, red. J. S. Piątkowski, Wrocław 1986, s. 231.
[85] Zob. Z. Radwański, *Kodeks cywilny a prawo regulujące zagadnienia rodziny*, [w:] *Problemy współczesnego prawa cywilnego (konferencja naukowa)*, Warszawa 1982, s. 333 i n.

W moim przekonaniu nie jest konieczne wyodrębnienie osobnej kategorii wartości, co postulują powyżej autorzy. Jak zostało przeze mnie wskazane wcześniej w pracy, na pojęcie prawa do prywatności składa się wiele dóbr, także tych bezpośrednio związanych z życiem rodzinnym, domowym i relacjami człowieka w rodzinie. Zbędne jest tworzenie oddzielnego prawa pod nazwą rodzinnych dóbr osobistych, ponieważ prowadzić to może do niepotrzebnego i nieuzasadnionego rozdrabniania pojęcia prywatności.

Dokonując analizy prawa do prywatności, napotkać można także najrzadziej dostrzeganą sferę prywatności, tj. prawo do schronienia we własnym, intymnym domu, w rodzinie, społeczności oraz do kształtowania swoich zachowań zgodnie z własną wolą i przyjętym systemem światopoglądowym oraz kulturę. Taki element prywatności został dostrzeżony m. in. przez Europejski Trybunał Praw Człowieka w sprawie *Chapman vs. United Kingdom*[86]. Trybunał po zbadaniu specyficznych uwarunkowań wspólnot romskich, uznał, że prawo do ochrony i poszanowania życia prywatnego i rodzinnego w tym przypadku oznaczać musi także prawo do utrzymania kulturowej tożsamości mniejszości poprzez aprobatę prowadzenia życia prywatnego w zgodzie z tradycją nomadycznego trybu życia[87]. Takie rozumienie prawa do prywatności jest jak najbardziej adekwatne w dzisiejszej wielokulturowości państw i społeczeństw. Zapewnienie prawnej ochrony jednostki dla jej odmienności kulturowej, tradycji czy systemu przekonań jest niezbędne w demokratycznym państwie prawnym.

Na ogół uważa się także, iż prywatność jest związana z pojęciem interesu własnego jednostki, z aktywnością tej jednostki podejmowaną przez nią na rzecz ochrony tego dobra, w przeciwieństwie do aktywności podejmowanej dla dobra wszystkich. Według teorii przedstawionej przez J. Braciak, prywatność obejmuje sferę aspiracji, dążności oraz tych rodzajów aktywności, które nie podlegają zewnętrznej kontroli; stąd bywa definiowana jako przestrzeń wolnego poruszania się, bądź jako domena autonomicznej aktywności, wolnej od kontroli szerszych grup[88]. Autorka ta wskazuje, że w ujęciu wąskim prywatność to stan, w ramach którego jednostka decyduje o zakresie i zasięgu informacji udostępnianym innym osobom, zaś w ujęciu szerokim prywatność oznacza możliwość podejmowania decyzji dotyczących jej osoby bez ingerencji osób trzecich[89]. Wskazuje ponadto, że granice prywatności określić można przestrzennie, jako „sferę prywatną", która obejmuje dom,

---

[86] Skarga 27238/95, ECHR 2001-I.
[87] Zob. także: sprawę *Muñoz Díaz vs. Spain*, skarga 49151/07, wyrok z dnia 8 grudnia 2009 r.
[88] J. Braciak, *Prawo do prywatności*, [w:] red. B. Banaszak, A. Preisner, *op. cit.*, s. 278.
[89] J. Braciak, *Prawo do prywatności*…, s. 130-131, 134 i n.

mieszkanie, ale i własność oraz społecznie, co obejmuje rodzinę, kręgi przyjacielskie i wszystkie inne grupy nieformalne oparte na stosunkach pokrewieństwa, sąsiedztwa i przyjaźni, a które można nazwać grupami „intymnymi” [90].

K. Motyka wyróżnia cztery definicje prywatności: jako prawo do bycia pozostawionym w spokoju, jako prawo do kontroli informacji na swój temat, jako kontrolę dostępu do osoby oraz jako autonomię jednostki[91]. Autor ten prezentuje redukcjonistyczne podejście do prywatności, które sprowadza się do wyeliminowania *stricte* pojęcia prywatności i zastąpienia go takimi określeniami jak: tajemnica korespondencji, nietykalność mieszkania, ochrona własności czy nietykalność osobista. W moim przekonaniu brak sprecyzowania i określenia sfery życia prywatnego jednostki nie jest właściwe z uwagi na niemożliwość objęcia jej ochroną czy wprowadzenia prawnych mechanizmów dających gwarancje istnienia dla tej sfery życia człowieka. Zgodzić się warto jednak z K. Motyką w kwestii istnienia różnorodnych zjawisk kreujących prywatność jednostki. Ten aspekt życia człowieka niewątpliwie składa się z wielu wartości budujących sferę prywatności człowieka i niejednokrotnie przenikających się wzajemnie, stąd wskazanie wielu zjawisk w ramach pojęcia prywatności uważam za słuszne.

W doktrynie panuje powszechny pogląd, że nie jest możliwe określenie wszystkich form prywatności, gdyż stale pojawiają się sprawy ukazujące nowe pola konfliktów[92]. Sformułowanie uniwersalnej definicji prywatności jest trudne, a to z uwagi na szczególnie pojemny zakres przedmiotowy pojęcia prywatności. Obok zatem niejasnych terminów określających prywatność jako „sferę osobistą człowieka”, „prawno-osobistą sferę własną”, „sferę osobowości”, pojawiają się też bardzo obrazowe wyrażenia, które są albo zbyt wąskie (jak np. „sfera samego siebie”, „sfera intymności”, „obszar tajności”), albo zbyt szerokie (jak „sfera indywidualności”)[93].

Przegląd podstawowych typów definiowania pojęcia prywatności ukazuje, że niemożliwym zadaniem jest sprecyzowanie kompletnej definicji tego pojęcia. Wśród przedstawicieli doktryny znajdują się także tacy, którzy twierdzą, że takie pojęcie jest w ogóle niepotrzebne. Ich zdaniem pod pojęciem prywatności i prawa do prywatności rozumie się tak różne zjawiska, że poza nazwą nie mają one ze sobą nic wspólnego i w istocie wszystkie mają charakter samodzielny i podlegają ochronie bez potrzeby korzystania z kategorii

---

[90] J. Braciak, *Prawo do prywatności*, [w:] red. B. Banaszak, A. Preisner, *op. cit.*, s. 279.
[91] Zob. K. Motyka, *Prawo..*, s. 11.
[92] B. Michalski, *op. cit.*, s. 52.
[93] J. Braciak, *Prawo do prywatności*, [w:] red. B. Banaszak, A. Preisner, *op. cit.*, s. 279.

prywatności[94]. Na pewno jest racjonalnym podejściem, aby eliminować z języka prawnego i prawniczego wielość konstrukcji czy pojęć prawnych, jednak w moim przekonaniu pozbywanie się pojęcia, które od dawna istnieje w świadomości ludzkiej oraz w prawie mija się z celem. Taka jest istota obecnych czasów, że z uwagi na wielość zjawisk, zmienność świata w wielu dziedzinach i poszerzenie świadomości ludzkiej wprost nazwanie pewnych instytucji czy zagadnień może być wręcz niemożliwe. Uściślenie pojęcia prawa do prywatności na pewno byłoby znacznie wygodniejsze z punktu widzenia teorii i praktyki i ułatwiałoby postawienie tez, jakie konkretnie zagadnienia mieszczą się w zakresie prywatności człowieka, ale jak na razie jest to chyba niewykonalne.

3. Prawo do ochrony danych osobowych jako element prawa do prywatności

Pomimo niezbyt długiego rodowodu prawa do życia prywatnego, odgrywa ono coraz ważniejszą rolę i wywiera coraz silniejszy wpływ na pozycję jednostki we współczesnym świecie. Wypracowana koncepcja prawa do prywatności zakłada możliwość życia jednostki swoim własnym, nieskrępowanym życiem („prawo do pozostawienia w spokoju" czy „prawo jednostki do bycia pozostawionej samej sobie") i zakłada jej niezależności w sferze życia osobistego, rodzinnego czy towarzyskiego. Niektóre z aspektów prywatności, jak już zostało wspomniane, są chronione jako dobra samoistne, a ich ochrona stanowi gwarancję nienaruszalności życia prywatnego (nieingerencja z zewnątrz, czy to ze strony państwa czy innych podmiotów), zapewniając jednocześnie poszanowanie godności człowieka. Wiązać się z tym także może zapewnienie jednostce prawa ochrony danych dotyczących szeroko rozumianej tożsamości, jeśli takimi danymi rozporządzałby podmiot inny niż dysponent tych danych, gdyż wówczas przestajemy mieć do czynienia z prywatnością człowieka. W takim ujęciu prawo do prywatności uwzględnia więc ochronę informacji dotyczących danej osoby i gwarancje pewnego stanu niezależności, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu[95]. W ten instrument niezależności ochrony jednostki wpisuje się instytucja zwana autonomią informacyjną lub prawem do ochrony danych osobowych[96]. Prawo do prywatności jest podstawą ochrony danych osobowych, a także jest pojęciem szerszym niż sama ochrona

---

[94] Zob. M. Jagielski, *Konstytucjonalizacja*…, s. 267.
[95] Por. wyrok TK z dnia 19 maja 1998 r., U5/97, OTK 1998, nr 4, poz. 46.
[96] Prawo to bywa także nazywane prawem do autonomii informacyjnej. Zob.: D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 127.

danych osobowych. Pomiędzy prawem do prywatności a prawem do ochrony danych osobowych istnieje jeszcze jeden znaczący związek; źródłem obu tych praw jest godność ludzka (co wprost wynika z treści Konstytucji), a ich ochrona ma zapewnić nienaruszalność tej godności[97]. Bezpośrednią zaś funkcją, jaką niewątpliwie spełnia ochrona danych osobowych, jest zabezpieczenie samego prawa do prywatności[98].

Prawo do ochrony danych osobowych i wypracowane przez wiele lat różnorodne regulacje prawne w tym zakresie w epoce globalizacji procesu przetwarzania danych osobowych nabierają kluczowego znaczenia dla jednostki i społeczeństwa pragnącego rozwijać się w sposób wolny od krępującej ingerencji państwa. Ochrona danych osobowych realizuje właśnie ten cel i zajmuje się szerokimi aspektami ochrony wolności osobistej zagrożonej zwłaszcza w epoce rozwoju różnych form i narzędzi komunikowania się i przetwarzania danych.

Ochrona danych osobowych jest trudnym zadaniem, głównie dlatego, że wymaga pogodzenia sprzecznych interesów zwiększenia dostępu do informacji i nieograniczania sfery prywatności[99]. Dotychczasowa cywilnoprawna ochrona prywatności jako dobra osobistego była możliwa dopiero po stwierdzeniu jej zagrożenia, zaś sądowa ochrona okazywała się zbyt późna dla przeciwdziałania naruszeniom[100]. W tak naturalny sposób powstała konieczność wykształcenia się metod, które zapobiegałyby i nie dopuszczały tym samym do naruszeń prywatności zarówno w życiu jak i w obrocie prawnym. Problematyka ochrony danych osobowych jest skomplikowana także dlatego, że występuje na styku trzech sfer zagadnień: prywatności i prawa do prywatności, bezpieczeństwa narodowego (państwowego), a także potrzeb obrotu prawnego (w tym i prywatnoprawnego), który wymaga m. in. swobodnego przepływu informacji[101].

Podstawowym celem przyświecającym ochronie danych osobowych jest ochrona prywatności jednostki, a zagadnienia dotyczące ochrony danych osobowych związane są niewątpliwie z pojęciem prawa do prywatności[102]. W doktrynie jednak nie ma zgodności co do wzajemnej relacji prawa do prywatności i prawa do ochrony danych osobowych. Spowodowane to jest równoczesnym rozwojem prawa do informacji, do transparencji życia

---

[97] D. Fleszer, *Zakres przetwarzania danych osobowych w działalności gospodarczej*, Warszawa 2008, s. 37.
[98] G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2002, s. 11
[99] G. Szpor, *Publicznoprawna ochrona danych osobowych*, „Przegląd Ustawodawstwa Gospodarczego" 1999, nr 12, s. 2.
[100] G. Szpor, *Publicznoprawna…*, s. 2.
[101] A. G. Harla, *Termin „dane osobowe" - uwagi de lege lata i de lege ferenda na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, „Palestra" 2001, nr 1-2, s. 32.
[102] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 21.

publicznego, do swobody i wolności wyrażania poglądów czy do świadomego uczestnictwa w życiu publicznym i korzystania z dobrodziejstw demokracji na tle dynamicznie rozwijającej się koncepcji ochrony jednostki[103].

Reprezentowane bywają stanowiska, według których między ochroną prawa do prywatności (zakotwiczoną w ramach konstytucyjnych) a ochroną danych osobowych zachodzi stosunek krzyżowania, przy tym są to systemy wzajemnie niezależne.

Podzielam tezę, według której prawo do ochrony danych osobowych wiąże się z ochroną prywatnością jednostki. Każda osoba ma prawo dbania o proces przetwarzania informacji o sobie czy to poprzez zachowanie ich w tajemnicy, czy poprzez rozporządzanie informacjami o sobie wedle jej potrzeb i uznania, indywidualnie decydując komu i w jakim celu mają zostać przekazane, udostępnione i kto ma prawo ich przetwarzania. Jednocześnie przychylam się też do stanowiska, które zajął w jednym z orzeczeń Trybunał Konstytucyjny, stwierdzając, iż art. 47 (prawo do ochrony prywatności) i art. 51 (prawo do ochrony danych osobowych) obowiązującej Konstytucji RP z 2 kwietnia 1997 r.[104] pozostają ze sobą w następującej relacji: „prawo do prywatności statuowane w art. 47 Konstytucji zagwarantowane jest m in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51 Konstytucji. Ten ostatni, rozbudowany przepis, odwołując się aż pięciokrotnie do warunku legalności *expressis verbis* w art. 51 ust. 1, 3, 4 i 5 Konstytucji oraz pośrednio przez powoływanie się na zasady demokratycznego państwa prawnego w art. 51 ust. 2 Konstytucji - stanowi też konkretyzację prawa do prywatności w aspektach proceduralnych”[105].

Ochrona danych osobowych na przestrzeni lat ewaluowała w kierunku ochrony prywatności w doktrynie formalno-prawnej. Ulegając stopniowej jurydyzacji, jako dobro jednostki, uzyskała też ochronę za pomocą różnych instrumentów prawnych, głównie z zakresu prawa cywilnego[106]. Żądania ochrony danych osobowych można dochodzić przed sądem, skoro jako indywidualne prawo podmiotowe jest prawnie chronione. Na skutek włączenia prawa do prywatności do kategorii konstytucyjnych praw człowieka ochrona danych osobowych zyskała ochronę za pomocą instrumentów konstytucyjnoprawnych.

Na skutek wzrostu znaczenia praw jednostki i wyrazu ochrony godności ludzkiej ukształtowała się nowa kategoria jej praw, tj. prawo do ochrony danych osobowych i z prawa do prywatności wydzieliła się zindywidualizowana kategoria prawa do ochrony danych

---

[103] M. Safjan, *Prawo do prywatności…*, s. 4.
[104] Dz. U. Nr 78, poz. 483.
[105] Wyrok TK z dnia 19 maja 1998 r., U5/97, OTK 1998, nr 4, poz. 46.
[106] M. Jagielski, *Prawo…*, s. 9.

osobowych. Podwaliny, które niewątpliwie stworzył rozwój prawa do prywatności i rozwój autonomii informacyjnej, a także globalizacja informacji i dostępu do niej sprawiły, iż problem ochrony danych jednostki został zauważony.

Ochrona danych osobowych koresponduje zatem z wolnością osobistą i chroni prawne jej aspekty w warunkach zagrożeń stwarzanych przez nowoczesne technologie[107]. Na przełomie lat 60. i 70. XX wieku istotną już rolę odgrywało istnienie zintegrowanych systemów służących do przesyłu, gromadzenia i dokonywania różnorodnych procesów przetwarzania danych w szerokim zakresie, dlatego też zaczęto upatrywać coraz to nowych zagrożeń interesów jednostki, której to dane dotyczyły. Okazało się, że ochrona sfery prywatności jednostki jest ściśle uzależniona od stopnia skuteczności mechanizmów ochrony informacji o charakterze osobowym, a zagrożenie prywatności pojawia się głównie w obszarze nowoczesnych systemów informatycznych i z wykorzystaniem nowoczesnych technik elektronicznego przetwarzania danych[108].

Socjolog G. Simmel stwierdzając, iż „podstawą wszelkich stosunków międzyludzkich jest to, że ludzie wiedzą coś o sobie", podkreślił znaczenie autonomii ludzi w procesie wymiany informacji[109]. Impulsami do stworzenia prawa człowieka do decydowania o losie danych go dotyczących, są właśnie przesłanki, o których pisał G. Simmel, a także rezultaty, które przyniósł żywiołowy rozwój technologii informatycznych i technologii służących komunikowaniu się ludzi (np. Internet, telefony komórkowe itp.) oraz hegemonia informacji we współczesnym społeczeństwie połączona z rosnącą ingerencję w sferę prywatności. Postęp technologiczny spowodował wzrost znaczenia kapitału informacji, a dane ze sfery publicznej i prywatnej gromadzone w sieciach informatycznych, w różnorodnych olbrzymich zbiorach, „bankach danych" instytucji, firm prywatnych, prywatnych administratorów, obejmowały zakresem cały świat. Dane osobowe wykorzystywano więc w różnorodny sposób, by np. zarządzać przedsiębiorstwem, prowadzić badania medyczne, czy wykorzystywać informacje osobowych w życiu społecznym czy w polityce.

Celem ochrony danych osobowych jest gwarantowanie decydowania w sferze informacji przez jednostkę, a zarazem zapewnienie realizacji jej prawnie chronionego interesu do zachowania prywatności i intymności[110]. Jednostka na podstawie konstytucyjnego prawa do ochrony osobowości ma prawo do informacji, przez co rozumie się prawo do

---

[107] M-T. Tinnefeld, *Ochrona danych - kamień węgielny budowy Europy*, [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 35.
[108] M. Safjan, *Prawo do ochrony…,* , s. 133.
[109] Za: M-T. Tinnefeld, *op. cit*, s. 35.
[110] Zob. M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 43 i n.

otrzymywania wiadomości o tym, gdzie, kiedy i w jakim celu są przekazywane dane dotyczące jej osoby, a także prawo do uzyskania informacji, w jaki sposób będą przetwarzane te dane i jakie będzie miało to dla niej konsekwencje. Prawo do informacji obejmuje również istnienie prawa do niewiedzy. Jest to związane głównie z rozwijającą się np. tendencją do prowadzenia badań genetycznych warunkujących życie jednostki, które niewłaściwie wykorzystane dają możliwość dysponowania cudzymi danymi i kontrolowania cudzego postępowania[111]. Jest to sprzeczne z koncepcją prawa do ochrony osobowości, gdyż w tych warunkach osoba zostaje zupełnie pozbawiona przysługującego jej prawa do wolności decydowania o swoim postępowaniu i rozporządzania informacjami o sobie.

Prawo do informacji o charakterze osobowym należy do fundamentalnych praw człowieka. Na rolę „prywatności informacyjnej" wskazywał m. in. Trybunał Konstytucyjny RFN w orzeczeniu z 1983 r., że jeśli ktoś nie może z wystarczającą pewnością przewidzieć, jak informacja o nim jest znana jego otoczeniu, ani nie może ocenić, jaką wiedzą na jego temat dysponują inne osoby, to jest on znacznie ograniczony w swej wolności planowania i decydowania bez presji lub wpływu innych osób. Ograniczenie tak rozumianego prawa do samookreślenia się jest podstawowym warunkiem funkcjonowania wolnej społeczności demokratycznej, opartej na zdolności działania i współdziałania obywateli"[112].

Już od dawna przedmiotem rozważań doktryny prawa jest kształtowanie się skutecznych metod ochrony informacji osobowych w kontekście prawa do prywatności każdej jednostki[113]. Ustalenia doktryny i orzecznictwo przyczyniły się do rozstrzygnięcia istotnych wątpliwości i pokonania różnych trudności wykładni, stosowania oraz przestrzegania prawa ochrony danych osobowych[114]. W związku z tym został sformułowany postulat zwiększania skuteczności prawnych regulacji w zakresie ochrony danych osobowych. To z kolei daje impuls do zgłębienia obszarów badawczych istniejących na pograniczu prawa administracyjnego, konstytucyjnego wraz z wpływem prawa europejskiego i regulacji międzynarodowych na rozwój krajowych norm w zakresie bezpieczeństwa przetwarzania danych osobowych.

---

[111] Np. idea analizy genetycznej (*Theres Lüthi*) tzw. „genetycznej kuli kryształowej", dzięki której istnieje możliwość poznania swojego losu, kontrolowania swojego postępowania.

[112] Wyrok Federalnego Trybunały Konstytucyjnego (BrerfGE) 65, 1, 42.; zob. N. Brieskorn, *Ochrona danych osobowych a zagrożenia* prywatności, [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 206.

[113] Metody prawnej ochrony danych osobowych analizowali w 1993 r. J. Barta i R. Markiewicz [w:] *Główne problemy prawa komputerowego*, Warszawa 1993, s. 229-251.

[114] G. Szpor, *Uwarunkowania skuteczności regulacji ochrony danych osobowych*, [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009, s. 22.

Istnieją dwa główne powody tworzenia prawnych mechanizmów ochrony danych osobowych. Po pierwsze, nieskutecznymi okazały się dotychczas istniejące możliwości wykorzystywane na gruncie prawa cywilnego i prawa karnego, które nie sprawdziły się z punktu widzenia funkcji prewencyjnej. Po drugie, koniecznym stało się wprowadzenie publicznoprawnych środków ochrony, a więc ochrony instytucjonalnej, a nie ochrony mającej jedynie źródło i umocowanie w autonomicznych dyspozycjach jednostki[115].

W przypadku ochrony danych chodzi o wzmocnienie autonomii jednostki w realizacji przysługujących jej praw za pomocą procedur i środków o charakterze prawnym, organizacyjnym i technicznym. Konieczność stworzenia nowych i adekwatnych do rozwijającej się zinformatyzowanej i nowoczesnej rzeczywistości mechanizmów ochrony jednostki i przysługującej jej praw jest warunkiem dalszego rozwoju tego prawa. W demokratycznym państwie prawnym podstawą zabezpieczenia praw jednostki jest istnienie funkcjonalnych, prawnych oraz środowiskowych regulacji. Przed istniejącymi zagrożeniami chronić mają nie tylko rozbudowane, ale i interpretowane zgodnie z krajowymi oraz międzynarodowymi standardami warunki ochrony odnoszące się do przetwarzania danych osobowych. Tworzące się nowe mechanizmy ochrony, bez względu na to, czy są tworzone na płaszczyźnie krajowej czy międzynarodowej, muszą być ze sobą zgodne, a u ich podstaw powinny się znaleźć tożsame założenia.

Kształtowanie ochrony praw jednostki w związku z przetwarzaniem informacji osobowych na jej temat jest procesem nieco różniącym się od kształtujących się wcześniej mechanizmów ochrony praw i wolności człowieka. Prawa człowieka, zwłaszcza te o charakterze osobistym i politycznym, kształtowały się na gruncie prawa wewnętrznego poszczególnych państw. W prawie krajowym wypracowywano wszystkie istotne koncepcyjnie elementy konstrukcji praw człowieka oraz następowało doktrynalne uznanie ich społecznej doniosłości, i tam też dokonywał się proces jurydyzacji i konstytucjonalizacji[116]. Dopiero gdy prawo czy wolność zdobyły odpowiednią rangę na gruncie prawa konstytucyjnego określonego państwa, rozpoczynał się proces internacjonalizacji[117]. Na poziom międzynarodowy trafiła zatem ukształtowana w prawie krajowym danego państwa koncepcja z wypracowanymi teoretycznymi i praktycznymi mechanizmami granic i ochrony.

Z ochroną danych osobowych było inaczej, gdyż prawo to pojawiło się w momencie, gdy wpływ uwarunkowań międzynarodowych na rozwój praw człowieka był już znaczący.

---

[115] M. Safjan, *Prawo do prywatności…,* s. 7.
[116] M. Jagielski, *op. cit.*, s. 13.
[117] *Ibidem*, s. 13.

Koncepcja rozwoju ochrony praw jednostki w zakresie danych osobowych kształtowała się równolegle na płaszczyźnie międzynarodowej jak i krajowej. Znacznym ułatwieniem, zwłaszcza w aspekcie ponadnarodowym, była rozwijająca się stale, aktywna i wzajemna współpraca w większości dziedzin współpracujących państw, przede wszystkim na płaszczyźnie przesyłu informacji o charakterze osobowym. Rozwijające się uregulowanie międzynarodowe odgrywały istotną rolę, tak samo silnie jak i prowadzone stale procesy instytucjonalizacji w ramach integracji Europy. Włączenia ochrony danych osobowych do konstytucyjnego katalogu ochrony praw człowieka i nadanie konkretnych treści postanowieniom konstytucji, wiąże się niewątpliwie z rozwojem tego procesu w skali międzynarodowej.

Kształtowanie systemu ochrony danych osobowych niewątpliwie związane jest zatem z wypracowanym ponadnarodowym dorobkiem zarówno na płaszczyźnie doktrynalnej, jak i normatywnej. Rozwój cywilizacji, stale ewoluujące aspekty ochrony danych osobowych i prężny rozwój tych zagadnień w konsekwencji stały się także przedmiotem zainteresowania różnych dziedzin prawa począwszy od materii konstytucyjnoprawnych poprzez regulacje w zakresie prawa administracyjnego czy prawa europejskiego. Dało to możliwość wypracowania standardów z zakresu ochrony danych osobowych znajdujących zastosowania w przypadku nieokreślonego adresata i do nieokreślonych materii. Dzięki temu ochrona danych osobowych wypracowała i ugruntowała sobie miejsce pośród innych istniejących już gałęzi prawa.

Znaczenie ochrony danych osobowych dla prawa do prywatności jest bardzo istotne. Wszelkie operacje dokonywane na danych osobowych czy to na płaszczyźnie zawodowej, czy podczas czynności prywatnych, hobbystycznych i naukowych odnoszą się do ochrony prywatności jednostki[118]. Do zapewnienia więc najpewniejszej ochrony prywatności jednostki niezbędne jest równoczesne wypracowanie jednorodnych i skutecznych mechanizmów ochrony danych osobowych, które są niezbędnym gwarancjami ochrony praw i wolności człowieka w dzisiejszych czasach.

---

[118] Np. codzienne z pozoru błahe zachowania, jak zbieranie danych geolokalizacyjnych, tworzenie profilów użytkowników Internetu czy tworzenie rejestru połączeń posiadacza telefonu komórkowego oznaczają, niezależnie od pierwotnego i głównego celu administratora danych kontrolę miejsca pobytu czy przemieszczania się użytkownika, identyfikację tożsamości rozmówców, a także identyfikację jednostek w oparciu o wskazywane informacje w sieci na temat zachowania, preferencji, zainteresowań, sposobów spędzania wolnego czasu (np. zakupy wszelkich towarów i usług *on line*, dokonywanie transakcji bankowych *on line*).

ROZDZIAŁ II
OCHRONA PRYWATNOŚCI I DANYCH OSOBOWYCH W PRAWIE MIĘDZYNARODOWYM I W WYBRANYCH PAŃSTWACH

1. Ochrona prywatności i danych osobowych w uniwersalnym systemie ochrony praw człowieka

Wprowadzenie ochrony prywatności do katalogu praw fundamentalnych ma przede wszystkim znaczenie na gruncie relacji między jednostką a państwem, wymuszając w tym zakresie istnienie pewnych standardów normatywnych, które powinny znaleźć swój wyraz także w ustawodawstwach innych państw. Zadaniem państwa jest stworzenie takiego systemu prawnej ochrony praw jednostki, aby nie dotykała jej ingerencja ani ze strony państwa, ani ze strony innej jednostki.

Podstawowym celem ochrony danych osobowych jest zapewnienie ochrony prywatności człowieka. Cel ten wskazują zarówno akty międzynarodowe i europejskie, wyznaczając standardy ochrony danych osobowych na świecie.

Kontekst międzynarodowy ochrony prywatności i ochrony danych osobowych niewątpliwie odnosi się do konieczności analizy aktów prawnych niejednokrotnie cechujących się specyficzną konstrukcją. Wszystkie akty prawne o zasięgu ponadnarodowym odnoszące się do ochrony prywatności i ochrony danych osobowych stanowią nie tylko porozumienie co do prawa, ale też co do programu, a zatem określają intencje umawiających się stron oraz ich sposób podejścia do przyjmowanych zobowiązań[119]. Takie międzynarodowe porozumienie w sprawie ochrony danych osobowych z jednej strony pozwala na wyznaczenie minimum koniecznej ochrony, a z drugiej strony ma zapewnić zgodne i jak najbardziej jednorodne stworzenie mechanizmów swobodnego przepływu informacji pomiędzy państwami członkowskimi. Jak to ujmują wytyczne OECD z 23 września 1980 r., obowiązujące na poziomie krajowym regulacje ochronne mogą „utrudniać" transgraniczny przepływ informacji; chodzi zatem o to, by „wesprzeć swobodny przepływ informacji pomiędzy Państwami Członkowskimi oraz by uniknąć tworzenia „nieusprawiedliwionych przeszkód" w procesie gospodarczego i społecznego rozwoju relacji pomiędzy Państwami

[119] M. Jagielski, *Prawo…*, s. 36.

Członkowskimi”[120]. Wprowadzenie ochrony praw jednostkowych w zakresie przetwarzania informacji ma zatem stworzyć na obszarze obowiązywania danego aktu jednolitą przestrzeń przepływu informacji[121]. Jeśli chodzi zaś o zapewnienie minimalnego poziomu ochrony i stworzenie standardów gwarancji ochrony, to akty prawne o zasięgu ponadkrajowym mają być podstawą do wprowadzenia w ustawodawstwach krajowych równie skutecznych rozwiązań prawnych opartych właśnie na funkcjonujących rozwiązaniach międzynarodowych[122].

Większość aktów prawnych o zasięgu międzynarodowym dotyczących praw człowieka traktuje sferę prywatności jednostki jako prawo fundamentalne i umieszcza ją w katalogu praw chronionych. Uniwersalny system ochrony praw człowieka wyznaczają niewątpliwie postanowienia zawarte w Karcie Narodów Zjednoczonych (dalej: Karta)[123]. Chociaż w Karcie brak jest definicji praw człowieka lub ich katalogu, to w pełni odzwierciedla ona przekonanie, że skuteczna międzynarodowa ochrona praw człowieka jest jednym z naczelnych warunków utrzymania pokoju i postępu[124]. Już w preambule Karty Narodów Zjednoczonych mowa jest o „wierze w podstawowe prawa człowieka, godność i wartość jednostki”, stąd Karta stała się niewątpliwie punktem wyjścia do rozwoju fundamentalnych instytucji prawa międzynarodowego w dziedzinie ochrony praw człowieka[125]. Karta Narodów Zjednoczonych zobowiązuje wszystkich członków ONZ do „współpracy z organizacją indywidualnie i zbiorowo nad osiągnięciem celów, do których należy ochrona praw człowieka”[126].

Poszukując podstaw prawa do prywatności w prawie międzynarodowym, w pierwszej kolejności (i chronologicznie) należałoby sięgnąć do Powszechnej Deklaracji Praw Człowieka (dalej: PDPCz lub Deklaracja), uchwalonej 10 grudnia 1948 r. przez Zgromadzenie Ogólne Narodów Zjednoczonych. Zdeklarowane już w Karcie Narodów Zjednoczonych poparcie powszechnego poszanowania i przestrzegania praw człowieka i podstawowych wolności dla wszystkich bez względu na rasę, płeć, język lub wyznanie, zostało skonkretyzowane właśnie

---

[120] Rekomendacja Organizacji Współpracy gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami, dostępna na stronie: http://www.oecd.org/internet/interneteconomy/15590241.pdf.
[121] M. Jagielski, *Prawo…*, s. 38.
[122] Wprost deklarują to wytyczne OECD z 1980 r., gdzie czytamy że „maja być traktowane jako określające minimalne standardy, które mogą być uzupełniane przez dodatkowe środki ochrony prywatności i indywidualnych wolności” a także wytyczne ONZ z 190 r., gdzie w części dotyczącej zasad ochrony wskazane jest, iż „zasady dotyczące minimalnych gwarancji mają być wprowadzone do ustawodawstw krajowych”.
[123] Dz. U. Nr 23, poz. 90 z późn. zm.
[124] J. Braciak, *Prawo do prywatności*…,s. 61.
[125] R. Kuźniar, *O prawach człowieka. Idee, instytucje, praktyka*, Warszawa 1992, s. 35-37.
[126] J. Braciak, *Prawo do prywatności*…, s. 61

w Powszechnej Deklaracji Praw Człowieka. Uznaje się, że Deklaracja po raz pierwszy określiła uniwersalny katalog praw osobistych, politycznych, ekonomicznych i społecznych[127].

Powszechna Deklaracja Praw Człowieka jest aktem międzynarodowym, w którym po raz pierwszy pojawiła się formuła prawa do prywatności. Prawo do prywatności zostało określone w art. 12 Deklaracji, który stanowi, iż „nikt nie będzie poddany arbitralnemu wkraczaniu w jego życie prywatne, rodzinę, mieszkanie lub korespondencję, ani też zamachom na jego honor i reputację". Ponadto każdemu człowiekowi zagwarantowano prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaszczaniu"[128]. Deklaracja ma formę rezolucji, stąd nie ma formy w pełni wiążącego aktu prawnego, niemniej wyraża idee ochrony tej sfery życia człowieka[129]. Można więc uznać, iż art. 12 PDPCz był wstępem do przekształcenia tej idei w formułę prawną[130].

Chociaż z Deklaracji nie płyną zobowiązania prawnomiędzynarodowe (gdyż nie jest ona traktatem międzynarodowym), a także nie przewiduje ona środków kontroli nad realizacją płynących z niej postanowień i pozostawia państwom pełną swobodę w doborze metod oraz zakresu jej wypełniania, to stanowiła ona niewątpliwie inspirację dla rozwoju uniwersalnego systemu ochrony praw człowieka dla wszystkich systemów regionalnych[131]. Odegrała znacząca rolę jako impuls do wzmocnienia ochrony praw człowieka w ustawodawstwach krajowych wielu państw. Praktyka wielu państw polegająca na wdrażaniu zasad PDPCz do prawa krajowego i odwoływaniu się do nich w umowach międzynarodowych sprawiła, że przynajmniej niektóre z jej postanowień są uznawane za reguły prawa zwyczajowego lub zasady ogólne prawa[132].

Sformułowane w Deklaracji pierwsze gwarancje odnoszące się do prawa do prywatności stały się podstawą do kolejnych międzynarodowych uregulowań w tym zakresie. 19 grudnia 1966 r. stworzony został Międzynarodowy Pakt Praw Obywatelskich i

---

[127] Por. B. Banaszak, *Prawa jednostki i systemy ich ochrony*, Wrocław 1995, s. 83. Autor zauważa, że katalog praw zawartych w PDPCz nie jest jednoznacznie zdefiniowany.
[128] Powszechna Deklaracja Praw Człowieka i Obywatela, art. 17, strona internetowa Polskiego Komitetu ds. UNESCO; http://www.unesco.pl/fileadmin/user_upload/pdf/Powszechna_Deklaracja_Praw_Czlowieka.pdf
[129] J. Braciak, *Prawo do prywatności…,* s. 63.
[130] M. Modzelewska, *Państwo wobec ochrony prywatności informacyjnej*, [w:] *Silne państwo*, red. M. Szyszkowska, Warszawa 1997, s. 118.
[131] Zob. P. Hofmański, *Europejska Konwencja Praw Człowieka i jej znaczenie dla prawa karnego materialnego, procesowego i wykonawczego*, Białystok 1993, s. 20.
[132] C. Mik, *Zbiorowe prawa człowieka. Analiza krytyczna koncepcji*, Toruń 1992, s. 12.

Politycznych (dalej: MMPPOiP albo Pakt)[133], który wraz z przyjętymi procedurami i Protokołem Fakultatywnym stanowi niejako podsystem systemu uniwersalnego[134].

W zakresie ochrony prywatności postanowienia Paktu chronią dwa rodzaje dóbr osobistych: po pierwsze, życie prywatne, rodzinne, domowe i korespondencję, a po drugie, honor i dobre imię jednostki[135]. Art. 17 ust. 1 Paktu stanowi, że „nikt nie będzie poddany arbitralnej lub bezprawnej ingerencji w jego życie prywatne, rodzinne, mir domowy czy korespondencję, ani tez bezprawnym zamachom na jego cześć i dobre imię". Prawo do prywatności zostało tu ujęte w niemal identycznej formule jak w przypadku Deklaracji, wskazując, iż nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne czy rodzinne. Pakt nie precyzuje jednak, o działania jakich podmiotów tu chodzi, ani nie formułuje warunków, w których na podstawie przepisów prawnych ingerencja może być podjęta przez władzę publiczną. Stanowi jednak, że każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami.

W doktrynie przyjmowano, że Pakt wraz Powszechną Deklaracją stanowią akty o charakterze fundamentalnym, niemal konstytucyjnym, a wszystkie później podpisane traktaty rozwijały i uszczegóławiały gwarancje zawarte w Pakcie[136]. W piśmiennictwie utrzymuje się również, że Pakt stanowi minimalny standard ochrony praw o charakterze uniwersalnym, który nie może być obniżany, ani relatywizowany w procesie jego stosowania[137].

2. Ochrona prywatności i ochrona danych osobowych w systemie Rady Europy

Po zakończeniu II wojny światowej głównym celem w Europie Zachodniej było wzmocnienie ochrony praw człowieka. Konieczne stało się tworzenie prawa, które zagwarantowałoby podstawowe prawa i wolności jednostce, a także wprowadzenie mechanizmów kontrolnych w tym zakresie. Z doświadczeń II wojny światowej powstała Organizacja Narodów Zjednoczonych (ONZ), a także idee wspólnych demokracji europejskich[138].

---

[133] Dz. U. Nr 38, poz. 167 z późn. zm.
[134] R. Kuźniar, *Międzynarodowe systemy ochrony praw człowieka*, „Sprawy Międzynarodowe"1981, s. 516.
[135] Szerzej na ten temat: A. Gliszczyńska- Grabias, K. Sękowska- Kozłowska, *Komentarz do art. 17 MPPOiP,* [w:] *Międzynarodowy Pakt Praw Obywatelskich (osobistych) i Politycznych*, red. R. Wieruszewski, Warszawa 2012, s. 371 i n.
[136] Z. Resich, *Nowy etap w rozwoju międzynarodowej ochrony praw człowieka*, „Państwo i Prawo" 1973, nr 8-9, s. 76.
[137] Tak A. Michalska, *Prawa człowieka w systemie norm międzynarodowych*, Warszawa 1982, s. 117.
[138] J. Braciak, *Prawo do prywatności…,* s. 69.

Wraz powstaniem w 1949 r. Rady Europy[139] został zapoczątkowany proces tworzenia europejskiego systemu ochrony praw człowieka[140]. Jednym z pierwszych i najważniejszych osiągnięć Rady Europy było przygotowanie Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (dalej: Europejska Konwencja lub EKPCz)[141], przyjętej 4 listopada 1950 r. w Rzymie jako międzynarodowej umowy z zakresu ochrony praw człowieka[142].

Waga Europejskiej Konwencji polegała nie tylko na tym, że była pierwszą konwencją regionalną, regulującą ogólnie prawa człowieka oraz formułującą prawa, stanowiące przedmiot ochrony, lecz także na tym, że stworzyła mechanizmy dochodzenia przez jednostkę poszanowania postanowień EKPCz przez którekolwiek państwo - stronę[143]. Konwencja powołała do życia Europejską Komisję Praw Człowieka i Europejski Trybunał Praw Człowieka. Ustanowienie Trybunału i możliwość wnoszenia doń spraw przez państwa i Europejską Komisję Praw Człowieka stanowiło precedens w skali światowej[144]. Przyjęte w Europejskiej Konwencji standardy zabezpieczenia praw jednostki są fenomenem w obrębie międzynarodowej ochrony praw człowieka i należy się im pierwszeństwo ze względu na moc ich oddziaływania zarówno w sferze prawnomaterialnej, jak i proceduralnej[145]. Także dorobek organów kontrolujących wykonywanie postanowień Europejskiej Konwencji jest bogaty, a zatem obie te przesłanki pozwalają wyodrębnić system ochrony praw jednostki stworzony przez EKPCz i uznać go za zasługujący na wnikliwe omówienie.

---

[139] Rada Europy powstała jako organizacja międzynarodowa, utworzona po II wojnie światowej, nadzieja powojennej integracji, konsolidacji sił i wspólnej wizji zjednoczonej politycznie i gospodarczo Europy na wzór Zjednoczonych Stanów Ameryki. Według projektodawców Rada Europy miała być pierwszym instytucjonalnym krokiem do utworzenia ponadnarodowego rządu Europy. Była pierwszą organizacją ucieleśniającą ducha współpracy panadeuropejskiej. Zob. J. Jaskiernia, *Rada Europy jako organizacja międzynarodowa*, [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009*, red. J. Jaskiernia, Toruń 2001, s. 33.

[140] J. Simonides, *Ewolucja systemu ochrony praw człowieka w Europie*, [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009*, red. J. Jaskiernia, Toruń 2001, s. 141.

[141] Dz. U. z 1998 r., Nr 147, poz. 962.

[142] Jedna z form prowadzenia wspólnych działań w ramach Rady Europy jest przygotowywanie projektów umów międzynarodowych. Prowadzi to, często nawet bezpośrednio, do harmonizacji wewnętrznych systemów prawnych państw członkowskich. Ta działalność rady Europy jest na tyle istotna, że w literaturze Rada europy bywa określana jako „znany i ważny ośrodek traktatotwórczy". Zob. R. Szafarz, *Dorobek traktatowy Rady Europy*, [w:] *Valeat aequitas. Księga pamiątkowa ofiarowana Księdzu Profesorowi Remigiuszowi Sobańskiemu,* red. M. Pazdan, s. 429.

Tekst Europejskiej Konwencji dostępny na str. : http://www.giodo.gov.pl/564/id_art/617/j/pl/. Europejska Konwencja była zmieniona Protokołami 3,5 i 8 oraz uzupełniona Protokołem nr 2.

[143] J. Braciak, *Prawo do prywatności…,*s. 70.

[144]J. Simonides, *op. cit.,* s. 141-164 oraz L. Garlicki, *Nowe demokracje przed Europejskim Trybunałem Praw Człowieka,* [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009*, red. J. Jaskiernia, Toruń 2001, s. 165- 180

[145] B. Gronowska, *Wolność i bezpieczeństwo osobiste w sprawach karnych w świetle standardów Rady Europy*, Toruń 1996, s. 8.

Wśród praw uwzględnionych w Europejskiej Konwencji Praw Człowieka na szczególną uwagę z punktu widzenia niniejszego opracowania zasługuje treść art. 8, który jednoznacznie stanowi o prawie do prywatności. Art. 8 EKPC jest gwarantem prawa do poszanowania życia prywatnego i rodzinnego, mieszkania oraz tajemnicy korespondencji[146]. Twórcy EKPCz posłużyli się uznanym schematem, zawierając w jednej jednostce redakcyjnej cztery strefy życia prywatnego jednostki. Zakres przedmiotowy prawa do prywatności składa się więc z czterech sfer i choć różnią się one od siebie zakresowo, to poszczególne elementy wzajemnie się przenikają, a ich tematem przewodnim jest prawo do prywatności. Ochrona prawa do prywatności w EKPCz nie jest wyrażona ani w formie zakazu (jaka art. 2-4), ani w formie wyraźnie sformułowanych uprawnień (np. postanowienia art. 6 oraz art. 9-11), lecz w formie „niezbyt jasno wytyczonego i przedstawionego w nieco bardziej ceremonialny sposób wymogu poszanowania" tych sfer [147].

Regulacja art. 8 Europejskiej Konwencji tworzy duży obszar szczegółowych wolności praw jednostki oraz negatywnych i pozytywnych obowiązków władzy publicznej[148]. Postanowienia tego artykułu mają przede wszystkim chronić jednostkę przed arbitralnym działaniem władz publicznych i nakierowane są bardziej na ochronę interesów indywidualnych niż zbiorowych[149].

W Europejskiej Konwencji (inaczej niż jest to zapisane w art. 12 Powszechnej Deklaracji Praw Człowieka) dopuszcza się pod pewnymi warunkami ograniczenie tych praw w przepisach wewnętrznych. W sytuacjach określonych przez art. 15 EKPCz można wyłączyć stosowanie norm prawnych wskazanych w art. 8. Na mocy art. 8 ust. 2 EKPCz zastrzega się, że jakiekolwiek ingerowanie przez władze publiczne w wykonywanie praw wskazanych w art. 8 ust. 1 dopuszczalne jest tylko wówczas, gdy następuje na podstawie ustawowego upoważnienia oraz gdy stanowi środek niezbędny do zapewnienia w demokratycznym społeczeństwie: bezpieczeństwa narodowego, porządku i spokoju publicznego, gospodarczego dobra kraju, obrony ładu i przeciwdziałania czynom karalnym oraz ochrony zdrowia i moralności lub ochrony praw i wolności innych osób.

System ochrony Europejskiej Konwencji Praw Człowieka obwarowany jest gwarancjami jej wykonywania, wśród których doniosłą rolę odgrywa orzecznictwo

---

[146] Art. 8 ust. 1 stanowi, że „każda osoba ma prawo do poszanowania (*has the right to respekt for*) swojego życia prywatnego i rodzinnego, swojego domu oraz korespondencji (*has private and family life, his home and his correspondence*)".

[147] J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie…,* s. 305.

[148] L. Garlicki, *Komentarz do art. 8 EKPCz,* [w:] *Konwencja i Ochronie Praw Człowieka i Podstawowych Wolności*, Tom I, *Komentarz do artykułów 1-18*, red. L. Garlicki, Warszawa 2010, s. 481.

[149] J. Braciak, *Prawo do prywatności…,* s. 72.

Europejskiego Trybunału Praw Człowieka w Strasburgu (dalej: Trybunał Europejski lub ETPCz). Orzecznictwo ETPCz dotyczące prawa do prywatności jest dość bogate, a to z dwóch względów. Po pierwsze, aktywność Europejskiego Trybunału na polu orzeczniczym rozpoczęła się już w latach 70. i 80. XX w.[150]. Po drugie, art. 8 EKPCz w sposób bardzo ogólny zakreślił prawo do prywatności - jak to zostało wspomniane wyodrębnił cztery elementy wchodzące w zakres tego prawa. Takie ujęcie prawa do prywatności było też najczęściej stosowane przez Europejski Trybunał Praw Człowieka w jego orzeczeniach. Różnorodne współzależności zakresowe pojęcia prawa do prywatności spowodowały zatem, że w praktyce Trybunału Europejskiego nie wytworzyło się dokładne rozgraniczenie tych czterech terminów wchodzących w zakres pojęcia prawa do prywatności[151].

Znalezienie jednoznacznej definicji określającej życie prywatne na gruncie art. 8 EKPC jest praktycznie niemożliwe. Komisja Praw Człowieka np. w sprawie *Van Osterwijck v. Belgia* określiła prawo do prywatności jako „prawo do życia w sposób zgodny z wolą jednostki i bez rozgłosu […]. Zawiera ono także, do pewnego stopnia, prawo do nawiązywania i rozwijania stosunków z innymi osobami, szczególnie w sferze emocjonalnej, dla rozwoju i zaspakajania indywidualnych potrzeb"[152]. Europejski Trybunał Praw Człowieka w sprawie *Niemietz v. Niemcom* orzekł jednak, że nie ma podstaw do zawężenia pojęcia życia prywatnego do „wewnętrznego kręgu", w którym jednostka może prowadzić życie osobiste według własnego wyboru, z wyłączeniem z niego całkowicie świata zewnętrznego nie mieszczącego się w tym kręgu.

Poszanowanie życia prywatnego oznacza również prawo do nawiązywania i rozwijania kontaktów z innymi ludźmi. W sprawie *Wakefield v. Wielka Brytania* Trybunał stwierdził, że stosunki między więźniem a jego narzeczoną, nawet jeśli nie mogą być uznane za życie rodzinne w rozumieniu art. 8, mieszczą się w pojęciu życia prywatnego. Nie ma tym samym powodów, aby z pojęcia „życie prywatne" wyłączać działalność zawodową i prowadzenie interesów, jeśli większość ludzi może rozwijać takie kontakty głównie w życiu zawodowym[153].

Co więcej, Trybunał stwierdził, iż pojęcie życia prywatnego w rozumieniu art. 8 ust. 1 jest szerokie i nie daje się wyczerpująco zdefiniować[154]. Można wskazać jedynie pewne

---

[150] L. Garlicki, *Komentarz do art. 8 EKPCz…,* s. 481.
[151] J. Braciak, *Prawo do prywatności…,* s. 72.
[152] Decyzja Komisji z 1979 , A. 40.
[153] Orzeczenie ETPCw sprawie *Wakefield v. Wielka Brytania* z dnia 16 grudnia1992, A.251-B, pkt 29.
[154] Orzeczenie ETPC w sprawie *Costello- Roberts v. Zjednoczone Królestwo* z dnia 25 marca 1993. A.247-C, pkt 36.

aspekty, uznane w orzecznictwie strasburskim, które składają się na sferę życia prywatnego. Są to m. in: życie seksualne, które jest najbardziej intymnym elementem[155] (z wyłączeniem stosunków seksualnych uprawianych zawodowo za wynagrodzeniem[156]), integralność fizyczna lub psychiczna (przy czym chodzi tu nie tylko o stosowanie przez władzę środków bezpośrednio wobec konkretnej osoby, ale i o ingerencje pośrednie w integralność fizyczną i psychiczną, jak np. duży hałas, który może naruszyć dobre samopoczucie jednostki, a tym samym i stanowić zamach na jej życie prywatne[157] czy nakaz poddania się testowi powodującemu potrzebę pobrania krwi w toku postępowania o ustalenie ojcostwa[158]. Do sfery życia prywatnego można także zaliczyć, według Trybunału, wybór imienia dla dziecka przez rodziców, który jest sprawą osobistą, należącą do sfery emocjonalnej, a więc prywatnej i chronionej w art. 8[159], czy wybór nazwiska i prawo do jego zmiany[160].

Dalsza analiza treści art. 8 EKPCz pozwala stwierdzić, iż do zakresu przedmiotowego omawianego artykułu zakwalifikować można także prawo do ochrony danych osobowych. W pewnym stopniu Europejska Konwencja bezpośrednio dotyczy ochrony danych osobowych, gdyż przetwarzanie danych osobowych nierzadko związane jest właśnie ze sferą prywatności człowieka.

Naruszeniem prywatności, jak uznał ETPC w orzeczeniu w sprawie *Murray v. Zjednoczone Królestwo*[161], jest rejestrowanie danych osobowych lub fotografowanie danej osoby lub jej rodziny bez jej wiedzy i zgody[162] czy gromadzenie danych osobowych przez służby ochrony państwa[163]. Przyglądając się dalej orzecznictwu Trybunału można stwierdzić również, że prawo do ochrony danych osobowych obejmuje konieczność uzyskania zgody osoby, której dane dotyczą, w związku z przetwarzaniem danych, a zgoda ta nie może być dorozumiana ani domniemana[164]. Dla udowodnienia braku arbitralnej ingerencji ze strony państwa należy również stwierdzić, czy krajowa regulacja dotycząca ochrony danych osobowych jest zgodna ze standardami wypracowanymi przez Europejska Konwencję i czy

---

[155] Orzeczenie ETPC w sprawie *Dudgeon v. Zjednoczone Królestwo* z dnia 22 października 1981, A. 45, pkt 52.
[156] Decyzja Komisji w sprawie *F. v. Szwajcaria* z dnia 10 marca 1988, skarga nr 11680/85, DR 55/178.
[157] Decyzja Komisji w sprawie *Powell i Rayaner v. Zjednoczone Królestwo* z dnia 16 lipca 1986, skarga nr 9310/81, DR 47/22.
[158] Orzeczenie w sprawie *Y.F. v. Turcja* z dnia 2 lipca 2003.
[159] Orzeczenie w Sprewie *Guillot v. Francja* z dnia 24 października 1996, RJD 1996. pkt 22.
[160] Orzeczenie w sprawie *Stjerna v. Finlandia* z dnia 25 listopada 1994, A.299-B.
[161] Orzeczenie z dnia 28 października 1994, A.300-A, pkt 86.
[162] Sfotografowanie osoby biorącej udział w wydarzeniu publicznym nie stanowi jednak ingerencji w jej prawo do prywatności.
[163] Orzeczenie *Rotaru v. Rumunia* z dnia a4 maja 2000.
[164] A. Redelbach, *Natura praw człowieka. Strasburskie standardy ich ochrony*, Toruń 2001, s. 226.

ewentualne ograniczenie prawa do prywatności spełnia przesłanki zawarte w art. 8 ust. 2 EKPCz[165].

Każdy, kto wykaże uzasadnione prawdopodobieństwo gromadzenia przez władze publiczne i przechowywania danych o jego życiu prywatnym, może domagać się uznania za pokrzywdzonego[166]. W sprawie *H. Amann v. Szwajcaria*[167] Trybunał stwierdził, że gromadzenie przez władze publiczne danych o jednostce jest ingerencją w prawo do poszanowania życia prywatnego, nawet gdy nie chodzi o tzw. dane wrażliwe[168].

W orzeczeniu *Rotaru v. Rumunia*[169] Trybunał potwierdził, że informacje o życiu jednostki, jej nauce, działalności politycznej, karalności, jeśli są systematycznie zbierane i przechowywane w kartach przez funkcjonariuszy państwa, mieszczą się w zakresie pojęcia „życie prywatne". Jeżeli władze publiczne nie wykażą odpowiednich podstaw prawnych przechowywania i udostępniania informacji z życia prywatnego jednostki, stanowi to ingerencję w prawo do poszanowania życia prywatnego. Przechowywanie w niejawnych rejestrach oraz udostępnianie informacji związanych z życiem prywatnym jednostki jest tym samym ingerencją w prawo do prywatności, wskazane w art. 8 EKPCz[170].

Podobne konkluzje można także wywieść z orzeczenia ETPC w sprawie *Leander v. Szwecja*, gdy skarżący zarzucał, że szwedzki rząd otrzymuje o nim poufne informacje, a ich wykorzystywanie przez państwo uniemożliwia mu uzyskanie pracy w sektorze publicznym. W orzeczeniu tym uznano legalność działań szwedzkiego rządu na tle art. 8 EKPCz i stwierdzono, że rejestracja danych osobowych może naruszać prawo do życia prywatnego określone właśnie w art. 8 EKPC. Trybunał stwierdził, że przechowywanie w tajnym rejestrze policyjnym i udostępnianie informacji dotyczących życia prywatnego jednostki, połączone z odmową zgody na jakiekolwiek poprawki, może być ingerencją w prawo do poszanowania życia prywatnego[171]. Nie ma potrzeby przy tym udowodnienia, że taka informacja została użyta na jej szkodę[172].

---

[165] A. Posiadła, S. Winiecka, *Ochrona danych osobowych w świetle wybranych orzeczeń Europejskiego Trybunału Praw Człowieka*, [w:] G. Goździewicz, M. Szabłowska red., *Prawna ochrona danych osobowych na tle europejskich standardów*, Toruń 2008, s. 199-200.
[166] I CR 234/77, LEX nr 7963.
[167] Sprawa nr 27798/5, LEX nr 76904; I CR 252/68, OSNC 1970, NR 1, POZ. 18.
[168] Zob. A.M. Nowacki, *Radziecki łącznik*, „Rzeczpospolita" z 2 marca 2000 r.
[169] Orzeczenie z dnia 4 maja 2000, skarga nr 28341/95.
[170] Zob. B. Gronowska, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii - problem poszanowania życia prywatnego człowieka na tle gromadzenia danych osobowych przez służby ochrony państwa*, „Prokuratura i Prawo" 2000, nr 9, s. 131-136.
[171] Orzeczenie z dnia 26 marca 1987, skarga nr 9248/81.
[172] J. Braciak, *Prawo do prywatności…,* s. 76.

W kontekście ochrony danych osobowych na uwagę zasługuje także wyrok z 25 września 2001 r. w sprawie *P.G i J. H. v. Wielka Brytania*[173], w którym stwierdzono, że znaczna liczba elementów relewantnych dla stwierdzenia, czy życie prywatne jednostki zostało naruszone, może wynikać także z działań poza domem lub nieruchomością danej osoby. Jest bowiem wiele takich sytuacji, że ludzie umyślnie (lub jedynie zgadzając się na to) podejmują działania, które mogą być rejestrowane lub relacjonowane publicznie; nawet jednak wtedy mogą oczekiwać poszanowania swej prywatności. Trybunał zauważył słusznie, że naruszenie prywatności ma miejsce wówczas, jeżeli w grę wchodzi stały i systematyczny zapis materiału z monitoringu sceny publicznej (np. utrwalanie sytuacji, gdy ma miejsce monitorowanie za pomocą środków technicznych sceny publicznej i chodzących tam ludzi)[174]. Z tej przyczyny gromadzenie przez służby ochrony lub inne instytucje o podobnym zakresie działania materiałów odnoszących się do konkretnego przypadku wchodzi w zakres ochrony, jaki przewiduje art. 8, nawet gdy informacje te nie zostały zebrane przy użyciu jakichkolwiek dokuczliwych metod lub w sposób niejawny[175].

Aspekt zapewnienia ochrony danym osobowym, tym razem w procesie lustracji, został przedstawiony w sprawie *Turek v. Słowacja*[176], która dotyczyła zarzutu naruszenia prawa do poszanowania życia prywatnego przez Ministerstwo Spraw Wewnętrznych w wyniku bezpodstawnej odmowy wglądu do dokumentów, na podstawie których powód został uznany za agenta komunistycznej służby bezpieczeństwa. Trybunał orzekł, iż władze Słowacji błędnie powoływały się na interes publiczny, odmawiając tym samym dostępu do dokumentacji, bo fakt z przeszłości dotyczy komunistycznych służb bezpieczeństwa i na tej podstawie nie ma mowy obecnie o jakimkolwiek istnieniu interesu publicznego. Co więcej, Trybunał stwierdził, że nie doszło do naruszenia art. 8 EKPCz ze względu na brak procedury, która umożliwiałaby ochronę prawa do poszanowania życia prywatnego.

Także ochrona danych osobowych, w tym danych medycznych, ma istotne znaczenie, jeśli chodzi o gwarancje ochrony prywatności. Zagwarantowanie tajemnicy danych lekarskich jest zasadą istotną nie tylko dla poszanowania prywatności pacjenta, ale również dla zachowania zaufania lekarzy i do służby zdrowia[177]. W skardze *M. S. v Szwecja (1997)*[178] powódka podniosła zarzut naruszenia prawa do poszanowania życia prywatnego i rodzinnego

---

[173] Wyrok z dnia 26 listopada 2013 r., sygn.. akt P 33/12.
[174] *Ibidem*, s. 75.
[175] Tak: L. Kański, *Prawo do prywatności (Miejsce w prawie polskim)*, Biuletyn RPO, Materiały 1989, nr 4, s. 75-76.
[176] Orzeczenie z dnia 16 lutego 2006, skarga nr 57986/00.
[177] J. Braciak, *Prawo do prywatności…,* s. 76.
[178] Orzeczenie z dnia 27 sierpnia 1997, Reports 1997, skarga nr 20837/92.

przez klinikę, która bez jej zgody przekazała do Biura Ubezpieczeń Społecznych dokumentację medyczną zawierającą według niej informacje wrażliwe, tj. o przerwanej w przeszłości ciąży, co stanowiło dużo szerszy zakres niż to było konieczne (chodziło konkretnie o stwierdzenie zakresu uszkodzenia kręgosłupa). Trybunał nie stwierdził naruszenia art. 8 ust. 2 Konwencji podnosząc, że informacje zostały udostępnione prawidłowo, tj. zaistniały odpowiednie i wystarczające przesłanki dla przekazania dokumentacji przez klinikę bez naruszenia prywatności powódki. Wymóg formalny zgodności z prawem też został spełniony, gdyż był zgodny z *Insurance Act*, który regulował ową kwestię. Ewentualnym zarzutem, nad którym zastanawiał się Trybunał, był brak zgody M. S. na ujawnienie dokumentów medycznych, jednak został on ostatecznie odrzucony, gdyż skarżąca składając wniosek o odszkodowanie w sposób dorozumiany zgodziła się na ujawnienie swoich danych. Orzeczenie to jest charakterystyczne, gdyż Trybunał potwierdził w nim wyraźnie, że ochrona danych osobowych, zwłaszcza o charakterze medycznym, ma znaczenie fundamentalne dla korzystania przez obywatela ze służącego mu prawa do poszanowania życia prywatnego i rodzinnego, o którym mówi art. 8 Europejskiej Konwencji. Podkreślono tym samym, że prawo krajowe powinno zapewnić właściwe gwarancje zapobiegające ujawnianiu lub przekazywaniu danych tak wrażliwych jak dane medyczne, które mogłoby być niezgodne z wytycznymi zawartymi w art. 8 EKPC[179].

W kontekście prawa do poszanowania życia prywatnego, istotna jest sprawa *Gaskin v. Wielka Brytania*[180], która odnosi się do zagwarantowania prawa do znajomości swojego pochodzenia. W przedmiotowej sprawie powód podniósł zarzut naruszenia prawa do poszanowania życia prywatnego i rodzinnego w wyniku odmowy dostępu do całości akt prowadzonych przez lokalne władze na jego temat w okresie sprawowania nad nim opieki publicznej do uzyskania pełnoletności. Trybunał orzekł o naruszeniu art. 8 EKPCz i stwierdził, iż osoby znajdujące się w sytuacji podobnej do przedstawionej (gdy informacje zawarte w aktach stanowiły jedyne źródło poznawcze o dzieciństwie, pośrednio zastępując pamięć rodziców w tym zakresie) mają żywy interes, chroniony przez Konwencję w uzyskaniu informacji koniecznej dla posiadania wiedzy na temat swojego dzieciństwa i swojego rozwoju, a państwo ma obowiązek udostępniania osobie zbioru danych na jej temat. Podobnie orzekł Trybunał w sprawie *Odievre v. Francja*[181], stwierdzając, że każdy człowieka ma prawo do uzyskania informacji o swoim pochodzeniu czy dzieciństwie.

---

[179] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 41.
[180] Orzeczenie z dnia 7 lipca 1989, skarga nr 10454/83.
[181] Orzeczenie z dnia 13 lutego 2003, Wielka Izba, skarga nr 42326/98.

Pojawiające się na przełomie lat. 70. i początku lat 80. orzecznictwo strasburskie ukazywało w praktyce problem zapewnienia gwarancji poszanowania życia prywatnego, a stosowanie art. 8 Konwencji uwidoczniło coraz większe znaczenie ochrony prywatności jednostki. W tych okolicznościach Rada Europy zauważyła, że istnieje konieczność doprecyzowania oraz uaktualnienia regulacji prawnych z tego zakresu, doszukując się istotnych ograniczeń i wad w treści art. 8 EKPCz, zwłaszcza w odniesieniu do rozwoju technologii informacyjnej. Zwrócono uwagę, iż nie do końca określony został zakres terminu „życie prywatne", a nacisk na ochronę przed ingerencją „organów publicznych" nie odpowiadał w wystarczającym stopniu rosnącej potrzebie stworzenia pozytywnego i proaktywnego podejścia, odnosząc się także do innych właściwych organizacji i interesów[182].

Nierozerwalnym powodem, dla którego pojawiały się wizje dopracowania zagadnień z zakresu ochrony prywatności na poziomie międzynarodowym, była także coraz silniejsza budowa wspólnoty wśród państw Europy Zachodniej. Proces ten zainicjowany został stworzeniem wspólnego rynku gospodarczego, a co za tym idzie stworzeniem swobodnego przepływu towarów, usług, osób i kapitału. Ta rozwijająca się wspólnota ekonomiczno-społeczna niosła ze sobą także globalizację informacji, konieczność wymiany i przepływu danych, co nie odbywa się bez ingerencji w sferę praw i wolności jednostki. Konieczne stało się stworzenie na tyle silnych procedur, które pogodziłyby prawo do prywatności jednostki ze stale rozwijającym się rynkiem wewnętrznym Unii Europejskiej i które byłyby na tyle stabilne, by zniwelować wszelkie rozbieżności prawne w tym zakresie w państwach członkowskich.

Te wszystkie przesłanki przemawiały także za koniecznością stworzenia nowej regulacji, która w specjalistyczny sposób dotyczyłaby ochrony danych osobowych i autonomii informacyjnej jako aspektów prawa do prywatności. Dotychczasowa wieloelementowa konstrukcja prawa do prywatności wypracowana na gruncie art. 8 EKPCz, a także brak jednoznacznego określenia definicji prywatności chociażby w orzecznictwie strasburskim, wskazały, iż bez wątpienia przepisy o ochronie danych osobowych są związane z realizacją prawa do prywatności i wchodzą w zakres tego pojęcia.

W ramach działalności Rady Europy indywidualna kwestia ochrony danych osobowych pojawiła się w 1968 r., kiedy Zgromadzenie Parlamentarne skierowało do Komitetu Ministrów zalecenie nr 509, w którym wskazano na potrzebę określenia, czy

---

[182] Peter J. Hustinx, *Rola Europejskiego Inspektora Ochrony Danych Osobowych w strukturach Unii Europejskiej zajmujących się ochroną danych*, Wykład Europejskiego Inspektora Ochrony Danych Osobowych, Warszawa 2004, s. 4. dostępne na str: http://www.giodo.gov.pl/1520090/id_art/1013/j/pl/.

Europejska Konwencja Praw Człowieka oraz prawa wewnętrzne państw członkowskich wystarczająco zapewniają ochronę wobec zagrożeń płynących z ówczesnego stanu rozwoju nauki i technologii[183]. Powołana przez Komitet Ministrów grupa ekspertów doszła do wniosku, że istniejący stan prawny jednak w niedostatecznym stopniu chroni prawa i interesy osób fizycznych w obliczu zagrożeń płynących z istnienia „zautomatyzowanych banków danych"[184]. Na tej podstawie Komitet Ministrów przyjął dwie rezolucje dotyczące zasad ochrony danych w sektorze publicznym i prywatnym: Rezolucję (73) 22 z 1973 r. zawierającą zasady ochrony danych w sektorze prywatnym oraz Rezolucję (74) 29 dotyczącą sektora publicznego[185]. Jednocześnie grupa ekspertów wskazała na konieczność stworzenia jednolitego międzynarodowego aktu prawnego o charakterze wiążącym, który wzmocniłby proces ochrony danych osobowych.

Konsekwencją prac organów europejskich w zakresie kompleksowej ochrony danych osobowych było opracowanie w 1981 r. odrębnej Konwencji o Ochronie Danych, tj. Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (dalej: Konwencja lub Konwencja nr 108)[186]. W takich okolicznościach powstał jeden z najważniejszych instrumentów prawnych ochrony danych osobowych.

Normy Konwencji nr 108 nie mają charakteru samowykonalnego, tzw. *self- executing*, ponieważ są sformułowane w postaci obowiązków dla ustawodawcy wewnętrznego

---

[183] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i dyrektywie Unii Europejskiej*, „Państwo i Prawo" 1997, nr 6, s. 32.

[184] Sz. Szmak, *Europejskie standardy w zakresie ochrony danych osobowych- zarys problemu*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008, s. 167.

[185] Zalecane standardy europejskie w zakresie ochrony danych osobowych, sformułowane w trybie rezolucji i rekomendacji Komitetu Ministrów RE lub Zgromadzenia Parlamentarnego RE, odnoszą się do różnych dziedzin życia. Akty te rozwijają ogólne zapisy Konwencji 108, precyzują jej wymagania oraz wprowadzają dodatkowe warunki przetwarzania danych osobowych w określonych dziedzinach (marketing bezpośredni, policja, zatrudnienie, terminy płatności, telekomunikacja ze szczególnym uwzględnieniem usług telefonicznych itd.). A. Mednis, *Ochrona…,* s. 32.

[186] Dz. U. z 2003 r., Nr 3, poz. 25 z późn. zm.; Tekst Konwencji opracowywano w latach 1976- 1980, zaś 28 stycznia 1981 r. w Strasburgu Komitet przyjął gotowy tekst i zainicjował procedurę podpisania. Zgodnie z art. 22 ust. 2 Konwencja miała wejść w życie pierwszego dnia miesiąca następującego po upływie trzech miesięcy od momentu, kiedy przynajmniej pięć państw członkowskich wyrazi zgodę na związanie się jej przepisami. Nastąpiło to więc dopiero 1 października 1985 r. po ratyfikowaniu postanowień Konwencji kolejno przez Szwecję, Francję, Hiszpanię, Norwegię i RFN. Polska podpisała Konwencję dopiero 21 kwietnia 1999 r., a ratyfikowała 23 maja 2002 r. Zasadniczą przyczyną tej sytuacji stały się przepisy art. 4 ust. 1 i 2 Konwencji, gdyż obligują one stronę do podjęcia niezbędnych kroków dla osiągnięcia zgodności przepisów prawa wewnętrznego z normami konwencyjnymi, przy czym harmonia ta powinna zostać osiągnięta nie później niż w dniu wejścia w życie Konwencji nr 108 dla strony; K. Czarnecki, *Ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008, s. 190.

określonego państwa[187]. Konwencja wyznacza jedynie minimalny standard ochrony, gdyż na mocy art. 11 państwo- strona może zagwarantować daleko bardziej idącą ochronę niż ta, którą jako minimalną zapewniają przepisy Konwencji[188]. Konwencja wskazując jedynie w ogólnym zarysie standardy ochrony danych, zobowiązuje państwa członkowskie, by w swoim prawie krajowym wprowadziły stosowne środki służące do realizacji owych standardów. Środki te mają być powzięte najpóźniej w dniu wejścia w życie Konwencji w danym państwie.

Jak zostało wskazane w preambule do Konwencji nr 108, jej motywem przewodnim jest wypracowanie kompromisu pomiędzy ochroną praw i podstawowych wolności każdej jednostki (zaś w szczególności jej prawa do prywatności) a wolnością przepływu informacji bez względu na dzielące ludzi granice państwowe[189]. W art. 1 wyraźnie został skonkretyzowany przedmiot i cel powstania tego aktu prawnego, zgodnie z którym „niniejsza Konwencja ma na celu zagwarantowanie, na terytorium każdej ze Stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowanie jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych („ochrona danych")".

W Konwencji nr 108 pojawiły się sformułowania z zakresu ochrony danych, które po raz pierwszy starano się wyczerpująco zdefiniować i ujednolicić. Wprawdzie na tle późniejszych aktów prawnych z zakresu ochrony danych w Konwencji zauważyć można wiele nieścisłości czy mało precyzyjnych definicji kluczowych pojęć, jednak biorąc pod uwagę ówczesne zaawansowanie technologii i wypracowane dotąd standardy ochrony danych osobowych wydawać się to mogło na tamten czas wystarczającą i adekwatną regulacją w tym zakresie.

Konwencja przyjmuje, że „dana osobowa" to informacja o charakterze osobowym, którą może być każda informacja dotycząca konkretnej osoby lub takiej osoby, którą można zidentyfikować (art. 2 Konwencji nr 108). Cechą wyróżniającą dane osobowe od innych informacji dotyczących osób jest brak anonimowości, tak więc informacja będzie miała charakter osobowy, dopóki jest możliwe ustalenie tożsamości osoby, której ona dotyczy[190]. Informacją o charakterze osobowym jest według Konwencji nie tylko informacja, która

---

[187] A. Mednis, *Ochrona…,* s. 41.
[188] A. Mednis, *Prawna ochrona danych osobowych*, Warszawa 1995, s. 22.
[189] W Preambule do Konwencji nr 108 czytamy: „Zważywszy, że celem Rady Europy jest osiągnięcie większej jedności jej członków, w poszanowaniu zwłaszcza zasady rządów prawa oraz praw człowieka i podstawowych wolności. Zważywszy, że pożądane jest rozszerzenie zakresu ochrony praw i podstawowych wolności każdego człowieka, w szczególności prawa do poszanowania prywatności, biorąc pod uwagę zwiększający się przepływ przez granice danych osobowych przetwarzanych automatycznie".
[190] A. Mednis, *Ochrona…,* s. 34.

dotyczy konkretnej osoby, ale również takiej, której tożsamości nie znamy, ale z łatwością możemy ją zidentyfikować. Zgodnie z raportem wyjaśniającym do Konwencji nr 108 i rekomendacją R (91) 10 na temat udostępniania danych o charakterze osobowym posiadanych przez instytucje publiczne, przyjęte zostało, że osoba fizyczna nie jest „identyfikowalna", jeśli ustalenie jej tożsamości wymaga nieproporcjonalnie dużo czasu, kosztów i działań[191].

Po raz pierwszy w odniesieniu do aspektów ochrony danych pojawiło się także w Konwencji nr 108 przedstawienie różnych form, które mogą przybierać dane osobowe. Wskazano, iż danymi osobowymi mogą być także zdjęcia, filmy czy zarejestrowane głosy, o ile spełniają wymagane prawem kryteria dotyczące pojęcia danych osobowych. Utrwalony na fotografii czy rysunku wizerunek osoby do tej pory korzystał z ograniczonej ochrony danych osobowych, gdyż stan techniki zwyczajnie nie dawał możliwości zastosowania automatycznych form przetwarzania obrazu czy głosu.

Konwencja nr 108 w art. 3 ust. 1 nakłada na państwa- strony obowiązek stosowania jej postanowień w stosunku do kartotek[192], a także i procesów przetwarzania automatycznego[193]. W Konwencji użyto pojęcia „przetwarzanie automatyczne", które pojawiło się jako wyraz informatycznych i nowoczesnych procesów przetwarzania danych, stwarzających możliwość ewaluacji w zakresie wyodrębniania się różnych form informacji o charakterze osobowym, których dotąd nie określano jeszcze mianem danych osobowych. Zgodnie z definicją „przetwarzania automatycznego" zawartą w Konwencji są to „następujące operacje wykonywane w całości lub częściowo przy pomocy procedur zautomatyzowanych: rejestracja danych, zastosowanie do tych danych operacji logicznych i/lub arytmetycznych, ich modyfikacja, usuwanie, wyprowadzania lub rozpowszechnianie" (art. 2 lit. c Konwencji nr 108).

Wraz ze wskazaną definicją przetwarzania automatycznego w Konwencji pojawiło się także określenie „zbioru zautomatyzowanego", jako „każdego zestawu danych podlegających automatycznemu przetwarzaniu" (art. 2 lit. b Konwencji nr 108) [194]. Z uwagi na mało

---

[191] Raport wyjaśniający do Konwencji nr 108, s. 8 , w którym czytamy: *„Identifiable persons" means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods;* Raport dostępny pod adresem: http://www.giodo.gov.pl/230/id_art/1685/j/pl/.

[192] Zastosowanie postanowień Konwencji w stosunku do kartotek, tj. zbiorów ręcznych, zostało także wprowadzone w ustawodawstwie m. in w Austrii, Belgii, Finlandii, Islandii, Lichtensteinie, Holandii, Norwegii,, Słowacji i Słowenii i na Węgrzech, a pośrednio we Francji i w Niemczech. Ustawa polska także obejmuje swoim zakresem przetwarzanie danych w kartotekach.

[193] Art. 3 ust. 2 lit. c dopuszcza stosowanie Konwencji do zbiorów danych osobowych, które nie są przetwarzane automatycznie.

[194] Zgodnie z art. 3 ust. 1 Konwencji nr 108, określającym zakres zastosowania konwencji, ma być ona zastosowana do „zautomatyzowanych zbiorów danych", a art. 3 ust. 2 odnosi się do przetwarzania innego niż automatyczne.

wyczerpujące określenie zbioru zautomatyzowanego w raporcie wyjaśniającym sprecyzowano jednak, że chodzi nie tylko o zbiory jednolite, ale i o zespoły danych znajdujące się w różnych miejscach, jednak połączonych dzięki „zautomatyzowanemu systemowi" w jeden zbiór[195].

Normatywna ochrona danych wynikająca z Konwencji nie dotyczy tylko danych osób fizycznych, gdyż Konwencja swoim zasięgiem objęła także gwarancję ochrony w stosunku do danych dotyczących ugrupowań, stowarzyszeń, fundacji, spółek, korporacji i innych organizacji skupiających bezpośrednio lub pośrednio osoby fizyczne, przy czym fakt posiadania osobowości prawnej przez te podmioty nie miał znaczenia (art. 3 ust. 2 lit. b Konwencji nr 108.).

Ustawodawstwo europejskie o ochronie danych osobowych powstało jako reakcja na zinformatyzowanie procesów przetwarzania, przechowywania i transmisji danych[196]. We wstępie do raportu wyjaśniającego stwierdza się, iż celem Konwencji jest wzmocnienie prawnej ochrony jednostek wobec zautomatyzowanego przetwarzania danych osobowych, a wzmocnienie ochrony było, zdaniem autorów, niezbędne ze względu na stale rosnące wykorzystanie informatyki dla celów administracyjnych i zarządzania[197]. Jak czytamy w raporcie, „kartoteki automatyzowane mają dużo większe możliwości rejestracyjne niż kartoteki ręczne i pozwalają na szybsze dokonywanie bardziej różnorodnych operacji"[198].

Zawarcie w Konwencji procedur w odniesieniu do informatycznych metod przetwarzania danych było pierwszym tego typu rozwiązaniem prawnym i adekwatną reakcją ustawodawcy europejskiego w stosunku do zmieniającej się wówczas rzeczywistości. Konwencja zawarła definicje „przetwarzania automatycznego" i uregulowała ochronę danych w zakresie stosowania procesów przetwarzania, przechowywania i transmisji danych z wykorzystaniem automatycznych środków[199].

Można podsumować więc, że Konwencja nr 108 może mieć zastosowanie w przypadku każdej informacji osobowej przetwarzanej automatycznie niezależnie od tego, czy występuje ona pojedynczo, czy w zbiorze oraz do danych osobowych przetwarzanych ręcznie, jeśli występują w zbiorze, o ile dane państwo rozciągnęło ochronę na zbiory ręczne[200]. Takie ujęcie wskazuje, iż pomimo zawarcia w Konwencji definicji nowego rodzaju przetwarzania,

---

[195] A. Mednis, *Ochrona…,* s. 36.
[196] Ibidem, s. 36.
[197] *Ibidem,* s. 32.
[198] Zob. *Rapport explicatif concernant la Convention pour la protection des personnes à l'ègard du traitement automatisè des donnèes à caractère personnel*, Strasburg 1981, s. 5
[199] A. Mednis*, Ochrona…,* s. 36.
[200] *Ibidem*, s. 34.

tj, przetwarzania zautomatyzowanego, zbyt wiele regulacji odnosi się do tego rodzaju przetwarzania. Pominięte zostały procedury związane z przetwarzaniem manualnym (ręcznym), które w dalszym ciągu istniały mimo daleko już posuniętego rozwoju technologicznego i nadal były źródłem wielu zagrożeń dla prywatności człowieka[201].

W początkowej fazie rozwoju ochrony danych osobowych uwidaczniała się także istotna różnica w sposobie i zakresie ochrony danych w sektorze publicznym i prywatnym. Konwencja nr 108 była pierwszym aktem, który nie wprowadzał takiego podziału, co skutkowało brakiem konieczności uchwalania odrębnego ustawodawstwa w stosunku do przetwarzania danych odpowiednio w sektorze publicznym i prywatnym[202]. Gwarantuje to wprost art. 3 ust. 1, zgodnie z którym strony Konwencji zobowiązują się do stosowania jej postanowień zarówno do zautomatyzowanych zbiorów danych osobowych, jak również automatycznego przetwarzania danych osobowych tak w sektorze publicznym jak i prywatnym.

W Konwencji pojawiło się jeszcze jedno istotne zobowiązanie z punktu widzenia zapewnienia właściwych procedur ochrony danych osobowych. Dotyczyło ono zastosowania w państwach-stronach Konwencji niezbędnych środków dla wprowadzenia w swoim prawie wewnętrznym podstawowych zasad ochrony danych. Z treści art. 4 ust. 1 można pośrednio wyprowadzić m. in. obowiązek stworzenia organu nadzoru jako formalnego środka ochrony danych osobowych. Wprost obowiązek ten został zawarty w protokole dodatkowym do Konwencji z 2001 r., który ustanawiał dodatkowe materialne oraz formalne warunki dla przetwarzania danych osobowych i dotyczył zasad transgranicznego przepływu danych oraz obligował strony do utworzenia niezależnych w działaniu organów nadzoru, zapewniających ochronę danych osobowych osób fizycznych[203].

---

[201] Art. 3 ust. 1 Konwencji stanowi, iż „strony zobowiązują się stosować niniejszą Konwencję do zautomatyzowanych zbiorów danych osobowych i do automatycznego ich przetwarzania", a przetwarzanie manualne wskazane jest tylko opcjonalnie w art. 3 ust. 2 lit. c, gdzie czytamy, że państwo będące stroną może zadeklarować, iż „będzie stosować niniejszą Konwencję również do zbiorów danych osobowych nieobjętych automatycznym przetwarzaniem".

[202] W niektórych krajowych ustawach poświęconych ochronie danych osobowych pochodzących z tego okresu utrzymany został ten podział. Przykładem jest Dania, gdzie odrębne ustawy obowiązywały do 2000 r. czy Niemcy, gdzie odrębność ochrony danych w obu systemach funkcjonuje do dziś. Poza Europą odrębne ustawy odnoszące się do regulacji w sektorze publicznym i prywatnym istnieją w Australii, Japonii, kanadzie, Korei Południowej czy w USA, gdzie w 1947 r. uchwalono *Privacy Act*, który dotyczył przetwarzania danych jedynie w sektorze publicznym. Zob. M. Jagielski, *Prawo…*, s. 60-61.

[203] Zob. Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych sporządzony w Strasburgu 8 listopada 2001 r. (Dz. U. z 2006 r. Nr 3, poz.15), dostępny na: http://www.giodo.gov.pl/564/id_art/778/j/pl/.

Istotną część protokołu stanowią przepisy odnoszące się do utworzenia organu nadzorującego w zakresie ochrony prywatności i ochrony danych osobowych. W swoim pierwotnym kształcie Konwencja nie zawierała wprost wyrażonej dyspozycji, co do utworzenia organów nadzorczych i kontrolnych w tym zakresie. Jedynie dyspozycja zawarta w art. 8 Konwencji przewiduje, że osobie przysługiwać musi środek prawny, z którego mogłaby skorzystać, gdyby jej prawa dotyczące sprawdzenia, weryfikacji czy usunięcia danych nie były respektowane. W protokole zawarty został obowiązek ustanowienia przez każdą ze stron jednego lub większej liczby organów odpowiedzialnych za zapewnienie zgodnej ze środkami swego prawa krajowego realizacji zasad ochrony danych osobowych. W treści art. 1 protokołu wskazano też minimalny zakres uprawnień, w jakie wyposażony powinien być taki organ, by rzetelnie i skutecznie nadzorować procesy przetwarzania danych i ich ochrony wynikające zarówno z norm prawa krajowego jak i pozakrajowego. Do kompetencji takiego organu należeć powinno m.in. interweniowanie w interesie poszczególnych osób w przypadku naruszenia prawa oraz wszczynanie postępowań kontrolnych, a także postępowań sądowych[204].

W skali międzynarodowej Konwencja nr 108 stała się pierwszym i jednym z głównych aktów prawnych indywidualnie odnoszącym się do ochrony danych osobowych[205]. Choć w dzisiejszej rzeczywistości odbiega znacznie od wizji idealnie kompletnego aktu regulującego tą materię, to niemniej stworzyła ona podwaliny i wprowadziła minimalny poziom wymaganej ochrony, który w swoich prawach wewnętrznych zobowiązane były zapewnić państwa członkowskie. Celem stworzenia Konwencji było zachęcenie państw nieposiadających regulacji na tym polu do wydania odpowiednich przepisów, ukierunkowując prace legislacyjne w tym zakresie i pozostawiając pewien margines swobody w kształtowaniu rozstrzygnięć odpowiadających danemu systemowi prawa[206]. Konwencja bierze pod uwagę istniejące już w niektórych państwach rozstrzygnięcia prawne i stara się wprowadzać pewien wspólny poziom ochrony oraz nie tworzyć bariery dla wykorzystywania nowoczesnej techniki informacyjnej i komunikacyjnej; okoliczności te są szczególnie istotne, jeśli zważy się, iż Konwencja zajmuje się także kwestią przekazywana danych osobowych pomiędzy krajami[207]. Można zatem powtórzyć za J. Bartą, P. Fajgielskim i R. Markiewiczem, że „głównym zadaniem, jakie sobie stawia Konwencja, jest wprowadzenie ujednoliconej

---

[204] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 52.
[205] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, cz. I, ODO 2000, nr 1, s. 31.
[206] D. Fleszer, *Zakres przetwarzania danych osobowych w działalności gospodarczej*, Warszawa 2008, s. 14.
[207] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 46.

ochrony danych osobowych w krajach europejskich i zharmonizowanie jej z ideą swobodnego przepływu danych w obrębie państw członkowskich”[208].

Analiza przedstawionych aktów prawnych Rady Europy Unii Europejskiej wskazuje, iż pierwsze próby regulacji prywatności informacyjnej były podobne względem siebie, powtarzając często te same unormowania. Przełom nastąpił wraz z rozwojem technologii, co jest zrozumiałe, ale nikt chyba jednak nie zdawał sobie sprawy z tak szybkiego postępu technologicznego, kiedy np. w 1950 r. powstawała Europejska Konwencja Praw Człowieka. Istnienie ponadpaństwowych standardów, wypracowanych latami i wciąż ulepszanych rozwiązań prawnych stało się podstawą na następne lata do tworzenia różnorodnych uregulowań ochrony danych osobowych i ochrony prywatności człowieka. Powstawanie zaś coraz to nowszych i sprawniejszych systemów ochrony jest wyzwaniem nie tylko dla Unii Europejskiej ale i każdego państwa dbającego o należyty poziom ochrony prywatności swoich obywateli.

3. Ochrona prywatności i ochrona danych osobowych w systemie Unii Europejskiej

Akty prawne z lat 70. i początku lat 80. XX wieku poświęcone zagadnieniom ochrony prywatności i ochrony danych osobowych nakierunkowanie były na ochronę zasobów zautomatyzowanych baz danych, gdyż ochrona poza bazami była wystarczająco gwarantowana w stosunku do potrzeb przez inne gałęzie prawa[209]. Ustawodawstwo europejskie z tego okresu i zawarte w nim regulacje dotyczące bezpieczeństwa informacji były także odzwierciedleniem poziomu zaawansowania informatyzacji[210], ale i ówczesnych założeń programowych, które wskazywały, iż głównym zagrożeniem dla prywatności były „banki danych”, umożliwiające gromadzenie w sposób systematyczny informacji o jednostce i posiadających możliwość ich automatycznego porządkowania[211]. Jak wskazuje M. Jagielski panowało „statyczne podejście do kwestii ochrony danych, wyrażające się w nastawieniu przede wszystkim na ochronę zgromadzonych zasobów danych (zbiorów), dopiero potem na regulację działań podejmowanych z użyciem danych”[212].

---

[208] *Ibidem*, s. 46.
[209] M. Jagielski, *Prawo…*, s. 56.
[210] Nie było sieci informatycznych, komputerów osobistych ani żadnych innych możliwości przekazywania czy gromadzenia rożnych danych na dużą skalę.
[211] M. Jagielski, *Prawo…*, s. 56.
[212] *Ibidem*, s. 56.

Całkowita zmiana podejścia do zagadnień ochrony danych pojawiła się w drugiej połowie lat 80 i w latach 90. XX wieku. Wypracowane dotąd standardy i założenia w zakresie ochrony danych uległy znaczącej transformacji. Istotnym *novum*, które wpłynęło bez wątpienia na prawną regulację w tym zakresie, było pojawienie się sieci Internet, spopularyzowanie systemów informatycznych i wprowadzenie wszelkich nowinek informatycznych do życia codziennego. Wszystkie te „zdobycze techniki" niosły potencjalne zagrożenia dla prywatności jednostki. Dotychczasowe regulacje prawne w tym względzie nie zapewniały skutecznej ochrony, co zrodziło konieczność dokonania kolejnych zmian.

Aktem prawnym o zasięgu UE, który jako pierwszy zawarł czytelne regulacje w zakresie ochrony prywatności jednostki i jej danych osobowych, był Traktat o Unii Europejskiej (Traktat z Maastricht, podpisany 7 lutego 1992 r., wszedł w życie 1 listopada 1993 r.). Treść art. 286 stanowiła samodzielny standard ochrony danych osobowych, na mocy którego rozszerzono krąg zobowiązanych do ochrony danych podmiotów, obok państw, do organów i instytucji. Zgodnie z art. 286 przewidziano także utworzenie niezależnego organu kontrolnego powołanego do ochrony danych osobowych, odpowiedzialnego za nadzorowanie stosowania aktów prawa wspólnotowego w zakresie ochrony danych osobowych zarówno w instytucjach, jak i w organach Unii Europejskiej.

Ochrona prywatności informacyjnej, a dokładnie ochrona danych osobowych została precyzyjnie uregulowana dopiero wraz z wydaniem 24 października 1995 r. Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (w skrócie: dyrektywa lub dyrektywa 95/46/WE)[213]. Do czasu przyjęcia dyrektywy, to Konwencja nr 108 Rady Europy była jedynym aktem prawnym indywidualnie poświęconym ochronie prywatności w zakresie ochrony danych osobowych[214]. Unia Europejska nie zajmowała się problemami odrębnej regulacji ochrony danych, a tylko Komisja Europejska postulowała, by kraje członkowskie ratyfikowały Konwencję do końca 1982 r. Z uwagi jednak na liczne rozbieżności w ustawodawstwach państw członkowskich w zakresie ochrony

[213] Dz. Urz. L Nr 281 z 23 listopada 1995 r., s. 31 i n.
[214] Wydano także odrębną dyrektywę w odniesieniu do ochrony danych osobowych w zakresie telekomunikacji tj. Dyrektywę 97/66/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym (Dz. Urz. L Nr 24 z 30 stycznia 1998 r. s. 1), która została znacząco znowelizowana w 2002 r.

danych osobowych i realną konieczność wprowadzenia jednolitego aktu w tym zakresie wydano wspomnianą dyrektywę[215].

Dyrektywa 95/46/WE stanowi podstawowy akt prawa wtórnego UE *acquis communautaire* w dziedzinie danych osobowych[216]. Wydana została w ramach delegacji z art. 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej, który pozostawił w kompetencjach Parlamentu Europejskiego i Rady określenie zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasad dotyczących swobodnego przepływu takich danych.

Dyrektywa wyznaczyła zasady ochrony podstawowych praw i wolności osób fizycznych, a w szczególności ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych. Powstała w celu wyeliminowania przeszkód dla swobodnego przepływu danych pomiędzy krajami członkowskimi bez równoczesnego zmniejszania ich ochrony, a także zabezpieczenia jednolitego i minimalnego poziomu ochrony prywatności osób fizycznych w związku z przetwarzaniem danych osobowych zawartych w zbiorach danych[217].

Z uwagi na miejsce w hierarchii aktów prawnych dyrektywa jest kierowana wyłącznie do państw członkowskich i nie wynikają z niej żadne prawa ani obowiązki dla osób fizycznych[218]. To państwo jest zobowiązane w swoim prawie wewnętrznym do spełnienia wymagań zawartych w dyrektywie, bez względu na formę ich realizacji. Dyrektywa nie należy zatem do *self- executing* law i może być stosowana bezpośrednio jedynie w wypadku, gdy upłynął termin jej realizacji, a państwo nie dokonało jej implementacji lub dokonana implementacja okazała się wadliwa[219].

Z punktu widzenia istoty regulacji prawnych odnoszących się do danych osobowych, przedstawienie i wskazanie znaczenia podstawowych pojęć zawartych w dyrektywie 95/46/WE jest konieczne. Dyrektywa nie tylko zawiera wiele nowoczesnych, nareszcie

---

[215] Problemem było stworzenie wspólnego rynku wewnętrznego, w którym miałby szanse dobywać się swobodny przepływ towarów, osób, usług czy kapitału, a także i danych osobowych przy zapewnionej jak najlepszej ochronie prywatności.

[216] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych, w obecnym i nadchodzącym stanie prawnym,* Warszawa 2014, s. 35.

[217] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 64.

[218] Dyrektywy to akty prawne, które nie mają odpowiednika w prawie polskim. Skierowane są tylko do państw członkowskich i wskazują cel, który muszą osiągnąć za pomocą dostępnych sobie środków. Organy państw członkowskich nie mogą wymagać od swoich obywateli postępowania zgodnego z dyrektywą, dopiero przepisy krajowe wydane na podstawie dyrektywy stanowią źródło praw i obowiązków dla osób fizycznych i prawnych. Zob. D. Bogucka, *Co nas będzie obowiązywało*, „Gazeta Prawna" z dnia 29 stycznia 2003 r.

[219] http://www.giodo.gov.pl/1234/j/pl/.

spójnych i wyczerpujących definicji i postanowień, które dotąd w tak kompleksowy i uporządkowany sposób nie zostały zawarte w żadnym akcie prawnym o międzynarodowym zasięgu, ale i znacząco wpłynęła na kształt ustawodawstwa i wprowadzonych mechanizmów z zakresu ochrony prywatności i ochrony danych osobowych w innych państwach, w tym także i w Polsce.

Zawarte w dyrektywie podstawowe definicje danych osobowych oraz przetwarzania danych zostały ujęte w sposób szeroki. Dane osobowe (*personal data*), na mocy art. 2 lit. a, oznaczają wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"), zaś osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie poprzez powołanie się na numer identyfikacyjny bądź jeden lub kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Na gruncie dyrektywy informacją o charakterze osobowym może być każda informacja dotycząca konkretnej osoby, którą to można zidentyfikować, a informacja ma charakter osobowy, dopóki możliwe jest ustalenie tożsamości osoby[220]. W dyrektywie w stosunku do osoby fizycznej pojawia się określenie „identyfikowalna", co pozwala dodatkowo na sprecyzowanie jednostki poprzez powołanie się na numer identyfikacyjny czy jeden lub wiele specyficznych elementów właściwych dla tożsamości określonej osoby.

Co więcej, zakres zastosowania postanowień dyrektywy dotyczy tylko zapewnienia właściwej ochrony w stosunku do danych osobowych osób fizycznych i nie przewiduje żadnej możliwości rozszerzenia zakresu obowiązywania przedmiotowej dyrektywy na dane osób prawnych czy innych jednostek organizacyjnych posiadających lub nie osobowość prawną.

Pojęcie „przetwarzania danych" (ang. *processing)* zostało zdefiniowane jako każda operacja lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie, układanie, kompilowanie, blokowanie, usuwanie czy niszczenie (Art. 2 lit. b dyrektywy 95/46/WE).

---

[220] A. Mednis, *U nas i gdzie indziej*, „Rzeczpospolita" z dnia 21 stycznia 1995 r.

Przedstawiony katalog czynności składających się na proces przetwarzania jest bogaty. Przetwarzanie ma miejsce począwszy od etapu gromadzenia danych, a skończywszy na ich niszczeniu. Objęcie ochroną danych osobowych następuje już zatem na etapie zbierania tych danych, o ile dane te mają figurować w zbiorze lub o ile mają być przetwarzane automatycznie. Definicja ta jest efektem doświadczenia w wieloletnim stosowaniu postanowień Konwencji nr 108, która skupiła się w głównej mierze na zautomatyzowanych procesach przetwarzania danych, spychając na dalszy plan manualne formy przetwarzania danych. Pojęcie przetwarzania zawarte w dyrektywie z kolei jest szersze, bardziej wyczerpujące, a ponadto na równi odnoszące się do automatycznych, jak i tradycyjnych form przetwarzania.

Zbiór zdefiniowany w dyrektywie znacząco odbiega chociażby od definicji zawartej w Konwencji nr 108, która okazała się niekompletna i niezbyt precyzyjna, szczególnie w odniesieniu do zbiorów ręcznych (brakowało tam np. informacji o uporządkowanym charakterze zbioru). Według dyrektywy zbiór danych osobowych (ang. *filing system*) to każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, scentralizowanych lub rozproszonych funkcjonalnie lub geograficznie (Art. 2 lit. c dyrektywy 95/46/WE.). Na mocy tej definicji można stwierdzić, iż dyrektywa nie obejmuje ochroną danych osobowych figurujących w zespołach danych, niemających żadnej struktury ani żadnego elementu porządkującego[221].

Podmiotem obowiązków przewidzianych w dyrektywie jest administrator danych (ang. *controller*), którym stosownie do art. 2 lit. d jest osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powołany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe[222].

Jeśli chodzi o zakres podmiotowy dyrektywy 95/46/WE, to obejmuje on podmioty, które przetwarzają dane w ramach działalności gospodarczej prowadzonej na terytorium

---

[221] W pkt 27 preambuły dyrektywy wyraźnie stwierdzono, że w zakresie ręcznego przetwarzania" w polu widzenia dyrektywy 95/46/WE znajdują się tylko zbiory danych (systemy ewidencyjne), natomiast poza nim pozostają „niezorganizowane akta", których zawartość nie jest ułożona (zorganizowana) według określonych kryteriów osobowych. Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 135; A. Mednis, *Ochrona…,* s. 36.

[222] Rozwiązanie zawarte w dyrektywie 95/46/WE, że w przypadkach, gdy cele i środki przetwarzania danych nie zostają wyznaczone przez oznaczoną osobą fizyczną lub prawną, lecz wynikają z przepisów prawa (lub postanowień administracyjnych), wówczas przepisy mogą wskazać administratora bądź określić specjalne kryteria, według których ma być on wyznaczony, nie zostało jednak przeniesione chociażby na grunt polskiej ustawy o ochronie danych osobowych.

państwa członkowskiego oraz podmioty, które nie prowadzą działalności gospodarczej na terytorium Unii Europejskiej, ale przetwarzają dane przy wykorzystaniu środków technicznych znajdujących się na terytorium Wspólnoty[223].

Wprowadzenie ujednoliconych standardów w zakresie ochrony danych, jak wskazuje pkt 3 i pkt 7 dyrektywy, jest warunkiem koniecznym do funkcjonowania swobodnego przepływu towarów, usług i osób, a to niewątpliwie związane jest także z przekazywaniem danych osobowych. By zapewnić właściwe warunki transferu danych i swobodnego acz legalnego korzystania z informacji o charakterze osobowym, w art. 6 dyrektywy 95/46/WE zostało sformułowanych pięć podstawowych zasad odnoszących się do właściwego przetwarzania danych osobowych.

Dyrektywa stawia warunek państwom członkowskim, by zobowiązały się do rzetelnego (sprawiedliwego, uczciwego), „w dobrej wierze" przetwarzania danych osobowych (art. 6 ust. 1 lit. a dyrektywy 95/46/WE). Akt ten nie poprzestaje tylko na zgodnym z prawem i celowym przetwarzaniu danych, ale wskazuje również na konieczność zapewnienia prawidłowego, stosownego i nienadmiernie ilościowego w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone dane (art. 6 ust. 1 lit. c dyrektywy 95/46/WE). Dane osobowe powinny być na mocy dyrektywy prawidłowe oraz, w razie konieczności, aktualizowane oraz korygowane („należy podjąć wszelkie uzasadnione działania, aby zapewnić usuniecie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane"- art. 6 ust. 1 lit. d dyrektywy 95/46/WE). W tym przypadku dyrektywa wprowadza bardzo rozbudowany obowiązek dbania o rzetelność przetwarzanych danych, wskazując, by były merytorycznie prawdziwe, ścisłe i w miarę możliwości aktualne, uwzględniając najnowszy ich stan. Zasady dotyczące jakości danych odnoszą się również do konieczności przechowywania danych w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne dla celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane (art. 6 ust. 1 lit. e dyrektywy 95/46/WE). Odnosząc się zaś do legalnych warunków gromadzenia danych, to dyrektywa wskazuje, iż gromadzenie danych powinno być dokonywane zgodnie z określonym, jednoznacznym i

[223] Istotne znaczenie w tym kontekście ma definicja siedziby zawarta w pkt 16 preambuły dyrektywy 95/46/WE. Głównym kryterium pozwalającym na oznaczenie siedziby jest miejsce, gdzie występuje efektywne i rzeczywiste (realne) wykonywanie określonej działalności w sposób stały, a nie ma znaczenia status prawny prowadzonej działalności gospodarczej, tj. czy jest ona prowadzona przez jednostkę podporządkowaną, przez oddział, czy filie posiadająca osobowość prawną. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 136.

legalnym celem, zaś dalsze przetwarzanie danych w sposób niezgodny z tym celem jest zakazane[224].

Szczegółowe przesłanki odnoszące się z kolei do legalnego przetwarzania danych zostały zawarte w art. 7 dyrektywy 95/46/WE, który wskazuje jednoznacznie sześć aspektów dopuszczalności przetwarzania danych osobowych[225].

Po pierwsze, osoba której dane dotyczą musi wyrazić zgodę na ich przetwarzanie, i to w sposób jednoznaczny i niewątpliwy (art. 7 lit. a).

Po drugie, przetwarzanie danych jest dopuszczalne, gdy jest to konieczne dla realizacji umowy, której strona jest osobą, której dane dotyczą lub w celu podjęcia działań na życzenie osoby, której dane dotyczą przed zawarciem umowy (art. 7 lit. b)[226].

Po wtóre, przetwarzanie danych osobowych jest także dopuszczalne na mocy Dyrektywy, w przypadku gdy jest to konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega, tj. do wykonania przez podmiot, odpowiedzialny za zbiór, spoczywającego na nim obowiązku ustawowego[227] (art. 7 lit. c), lub przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą[228] (art. 7 lit. d).

Kolejnym kryterium legalności przetwarzania danych jest konieczność realizacji zadania wykonywanego w interesie publicznym lub dla sprawowania władzy publicznej, przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia dane (art. 7 lit. e).

Ostatnim warunkiem przetwarzania danych jest ich przetwarzanie z uwagi na konieczność wynikającą z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, a które gwarantują ochronę na mocy art. 1 ust.1 dyrektywy (art. 7 lit. f).

Rygorem prawnym obostrzone zostało także przetwarzanie szczególnej kategorii danych, tj. danych wrażliwych (*sensitive data*), z uwagi na fakt, iż tego rodzaju informacje już same w sobie stanowią pewne zagrożenie dla prywatności jednostki. Katalog danych

---

[224] „Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie jest uważane za niezgodne z przepisami pod warunkiem ustanowienia przez państwa członkowskie odpowiednich środków zabezpieczających”- Art. 6 ust. 1 lit. b dyrektywy 95/46/WE.

[225] O ile Konwencja nr 108 nie wskazywała ani nie narzucała żadnych warunków dopuszczalności gromadzenia i przetwarzania danych, to dyrektywa czyni to w sposób wyczerpujący.

[226] Jak wskazuje A. Mednis, przykładem może być konieczność zebrania i przetworzenia informacji przez firmę ubezpieczeniową w związku z wystawieniem polisy. A. Mednis*, Ochrona…,* s. 38.

[227] Np. policja, służby celne, administracja podatkowa.

[228] Np. dla potrzeb ochrony zdrowia.

wrażliwych, który pojawia się w art. 8 ust. 1, obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, informacje odnośnie przynależności do związków zawodowych, jak również informacje dotyczące zdrowia i życia seksualnego; pomija jednak dane odnoszących się do przynależności partyjnej, przynależności wyznaniowej, kodu genetycznego czy nałogów.

W art. 8 ust. 2 dyrektywy 95/46/WE zostały wskazane sytuacje, kiedy to przetwarzanie danych sensytywnych jest prawnie dopuszczalne, a zatem ogólny zakaz przetwarzania danych wrażliwych nie obowiązuje.

Przetwarzanie danych wrażliwych jest dopuszczalne, gdy osoba, której dane dotyczą, udzieliła wyraźniej zgody na przetwarzanie tych danych, chyba że ustawodawstwo wewnętrzne państwa członkowskiego może przewidywać, iż zakaz przetwarzania danych wrażliwych nie może zostać uchylony na podstawie samej zgody zainteresowanego (art. 8 ust. 2 lit. a).

Dopuszczalne jest przetwarzanie danych z dziedziny prawa pracy, a dotyczy to przetwarzania przez pracodawcę informacji o pracownikach, o ile jednak jest do dozwolone przez prawo wewnętrzne przewidujące określone środki zabezpieczające (art. 8 ust. 2 lit. b).

Przetwarzanie danych niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą lub osoby trzeciej, w przypadku, gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody, jest także legalnie dopuszczalne na mocy dyrektywy (art. 8 ust. 2 lit. c).

Zakaz przetwarzania danych z art. 8 dyrektywy 95/46/WE nie obowiązuje także w przypadku legalnej działalności fundacji, stowarzyszeń lub innych instytucji o charakterze politycznym, filozoficznym, religijnym lub związkowym, które przetwarzają informacje o swoich członkach lub osobach utrzymujących z tymi instytucjami regularne kontakty związane z celem danej instytucji, a instytucja może tylko ujawniać dane na zewnątrz za zgodą osoby zainteresowanej (art. 8 ust. 2 lit. d).

Jeśli chodzi o dane dotyczące przestępstw, wyroków skazujących czy środków bezpieczeństwa, to mogą one być gromadzone jedynie w zbiorach o charakterze publicznym, pod kontrolą władz publicznych (art. 8 ust. 5 dyrektywy 95/46/WE.). Specjalne postanowienia dotyczą ponadto danych wrażliwych o charakterze medycznym. Warunki dopuszczalności przetwarzania tej kategorii informacji reguluje art. 8 ust. 3 dyrektywy, na mocy którego dopuszczalne jest przetwarzanie danych do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia czy zarządzania opieką zdrowotną, jak też, gdy

dane są przetwarzane przez pracownika służby zdrowia, zgodnie z przepisami prawa krajowego i z zachowaniem wszelkich warunków dotyczących tajemnicy zawodowej.

Dyrektywa, tak jak i opisywana wcześniej Konwencja nr 108, pozbawiona jest niemal całkowicie odniesień do zróżnicowania stopnia i zakresu ochrony danych w sektorze publicznym i prywatnym. O ile jednak ten podział został zniesiony, to w zamian istnieją wyraźnie wskazane wyłączenia z ochrony danych osobowych (w całości lub w części) odnoszące się do pewnych materii. Choć ich ujęcie bywa różnie określane, to można wskazać pewne ogólne dziedziny objęte zakresem takich wyłączeń. Jest to bezpieczeństwo państwa, porządek publiczny oraz ochrona praw i wolności jednostek.

Dyrektywa 95/46/WE stwierdza, w art. 3 ust. 2 myślnik pierwszy, iż nie ma zastosowania „w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa)". W art. 13 ust. 1 jednocześnie czyni jednak możliwość ograniczenia pewnych praw dla zabezpieczenia „bezpieczeństwa narodowego", „obronności", „bezpieczeństwa publicznego" i „ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi". Pojawiające się rozbieżności interpretacyjne w owej materii nie są jedynie widoczne na gruncie dyrektywy, gdyż na gruncie międzynarodowym brak jest jednolitego stanowiska co do czynienia zwolnień lub ograniczeń w zakresie sprawowania ochrony danych osobowych w pewnych materiach. Wytyczne OECD z 1980 r. wskazują, że wyjątki takie powinny być „możliwie nieliczne"[229], a wytyczne ONZ z 1990 r. wskazują, iż są one dopuszczalne, jeżeli są „konieczne"[230]. Europejska Konwencja Praw Człowieka[231] wskazuje natomiast, by stosować przewidziane w art. 8 kryteria, takie jak: wymóg regulacji ustawowej, konieczność respektowania „demokratycznego społeczeństwa", czy zasada proporcjonalności oraz koncepcja istoty prawa (wolności). Uwzględnienie wszystkich powyższych przesłanek będzie wymuszało na ustawodawcy, a także organach stosujących prawo, poszukiwanie kompromisu pomiędzy interesem publicznym i jednostkowym oraz konkurencyjnymi interesami indywidualnymi[232].

Drugie wyłączenie stanowią sprawy związane z zakresem porządku publicznego. I tak, zgodnie z art. 3 ust. 2 myślnik pierwszy, sprawy związane z zakresem porządku

---

[229] Wytyczne OECD z 1980 r., pkt 4, lit. a.
[230] Wytyczne ONZ z 1990 r., pkt 6.
[231] Europejska Konwencja Praw Człowieka zawiera generalne wyłączenie stosowania jej przepisów w zakresie „bezpieczeństwa państwowego" (art. 8 ust. 2; Por. art. 9 ust. 2, art. 10 ust. 2, art. 11 ust. 2).
[232] M. Jagielski, *Prawo…*, s. 63.

publicznego są określane jako związane z „bezpieczeństwem publicznym" czy z „działalnością państwa w obszarach prawa karnego". W art. 13 ust. 1 natomiast pojawia się ograniczenie stosowania pewnych praw dla zapewnienia „bezpieczeństwa publicznego, „działań prewencyjnych, prowadzonych czynności dochodzeniowo - śledczych i prokuratorskich w sprawach karnych lub w sprawach o naruszenie zasad etyki w zawodach podlegających regulacji", czy też „funkcji kontrolnych, inspekcyjnych i regulacyjnych" z tym związanych[233].

Ostatnią dziedziną objętą wyłączeniami z zakresu stosowania przedmiotowej dyrektywy jest ochrona praw i wolności jednostki. Akt ten wyraźnie w art. 3 ust. 2 wyłącza z zakresu własnej regulacji przetwarzanie danych „o charakterze czysto osobistym i domowym", a także w art. 13 ust. 1 pozwala ograniczyć pewne zawarte w nim prawa z uwagi na „ochronę osoby, której dane dotyczą oraz praw i wolności innych osób"[234].

W celu pełnej realizacji i zapewnienia najwłaściwszej ochrony danych jednostki dyrektywa 95/46/WE wprowadziła katalog minimalnych praw służących osobom, których dane dotyczą i których dane są przetwarzane, wykorzystane czy zbierane.

Punkt 38 preambuły dyrektywy 95/46/WE wskazuje, że „jeżeli przetwarzanie danych ma być rzetelne, osoba, której dane dotyczą, musi mieć możliwość dotarcia do informacji o wystąpieniu czynności przetwarzania danych, oraz jeżeli dane są uzyskiwane od niej, musi otrzymać dokładne i pełne informacje, uwzględniające okoliczności pozyskiwania danych"

Na tej podstawie, stosownie do treści art. 10, został nałożony na administratora danych obowiązek informacyjny. Polega on na wskazaniu osobie, której dane są gromadzone,

---

[233] Obecnie w zakresie szeroko pojętego bezpieczeństwa publicznego wprowadzono już szczegółowe regulacje na poziomie europejskim odnoszące się do ochrony przetwarzania danych osobowych i zapewniające kooperację m. in. w takich sektorach jak: przyznawanie azylu- Rozporządzenie Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiające kryteria i mechanizmy określania Państwa Członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z Państw Członkowskich przez obywatela państwa trzeciego (Dz. Urz. UE L 50, z 25.02.2003, s. 1-10)- ustanawia on tzw. system EURODAC; współpracy celnej - Konwencja w sprawie wzajemnej pomocy i współpracy miedzy administracjami celnymi (OJ C 316, 27.11.1995)- ustanawia tzw. celny system informacyjny (CIS);swobody przemieszczania się- tzw. Układy z Schengen: umowa między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach - Schengen I, Konwencja Wykonawcza do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach-Schengen II - ustanowiły one tzw. system informacyjny Schengen (SIS); współpracy policyjnej i sądowej w sprawach karnych, które regulują przepisy szczególne o ochronie danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych (były trzeci filar), w tym decyzję ramową 2008/977/WSiSW Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. U. L 350 z 30.12.2008, s. 60).

[234] Przedstawione regulacje są analogiczne względem postanowień Konwencji Rady nr 108, które umożliwiają ograniczenie pewnych praw w niej przewidzianych ze względu na ochronę „podmiotu danych oraz praw i wolności innych osób"- art. 9 ust. 2 lit. b Konwencji Rady Europy nr 108.

niezbędnych wiadomości odnośnie administratora, informacji o zborze danych, jego charakterze oraz celu, w jakim są gromadzone dane osobowe, a także informacji w sprawie dobrowolności udostępniania danych. Obowiązek informacyjny nie istnieje jednak w przypadku, gdy osoba, której dane są gromadzone, posiada wiedzę na temat tożsamości administratora danych ewentualnie jego przedstawiciela, dokładnie zna cel przetwarzania danych, a także jest w posiadaniu wszelkich dalszych informacji takich jak: odbiorcy lub kategorie odbiorców danych, tego czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz jakie są ewentualnie konsekwencje nieudzielanie odpowiedzi, a także że istnieje prawo do wglądu do swoich danych oraz prawo ich sprostowania (art. 10 dyrektywy 95/46/WE).

W przypadku pozyskiwania informacji z innych źródeł niż osoba, której dane dotyczą, konieczny jest do spełnienia obowiązek informacyjny wynikający z treści art. 11 dyrektywy. Administrator danych lub jego przedstawiciel zobowiązani są wtedy, by od początku gromadzenia danych osobowych lub w przypadku ujawnienia danych osobie trzeciej, nie później niż do momentu, gdy dane są ujawnione po raz pierwszy, dostarczyć osobie, której dane dotyczą, co najmniej następujące informacje: tożsamość administratora danych i ewentualnie jego przedstawiciela, cele przetwarzania danych a także wszelkie inne informacje, jak np. : kategorie potrzebnych danych, odbiorcy lub kategorie odbierających dane czy istnienie prawa wglądu do swoich danych oraz ich sprostowania, o ile jednak takie dalsze informacje są konieczne, biorąc pod uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą. (art. 111 ust. 1 dyrektywy 95/46/WE).Wyjątkiem względem obowiązku wynikającego z art. 111 dyrektywy 95/46/WE są sytuacje, gdy osoba posiada już przedstawione powyżej informacje.

Obowiązek wskazania powyższych informacji nie obowiązuje, na mocy art. 11 ust. 2 dyrektywy, gdy, szczególnie w przypadku przetwarzania danych dla celów statystycznych, historycznych lub naukowych, dostarczanie takich informacji wymagałoby niewspółmiernie dużego wysiłku lub jeżeli gromadzenie lub ujawnienie informacji jest wyraźnie przewidziane przez prawo. W takich przypadkach państwa członkowskie zapewniają odpowiednie środki zabezpieczające.

Minimum ochrony interesów osoby fizycznej zagwarantowane jest także poprzez wskazanie wprost legalnych przesłanek dopuszczalności przetwarzania danych w przypadku braku zgody dysponenta tych danych. Te ściśle określone sytuacje wymienione zostały w art.

7 dyrektywy, co zostało już wcześniej przedstawione przy okazji opisu prawnych warunków przetwarzania danych osobowych na mocy dyrektywy 95/46/WE.

Art. 12 dyrektywy gwarantuje z kolei każdej osobie prawo dostępu do swoich danych. Prawo to polega na uzyskaniu od administratora danych bez ograniczeń, w odpowiednich odstępach czasu oraz bez nadmiernego opóźnienia lub kosztów wiadomości takich jak: potwierdzenie, czy dotyczące jej dane są przetwarzane oraz co najmniej informacji o celach przetwarzania danych, kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane. Co więcej, w przypadku odpowiedzi pozytywnej, osobie fizycznej przysługuje prawo do uzyskania w zrozumiałej formie informacji o danych przechodzących przetwarzanie oraz posiadanych informacji o ich źródłach, a także wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego.

Uprawniony może także odpowiednio do przypadku domagać się sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z przepisami dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych oraz prawo do zawiadomienia osób trzecich, którym dane zostały ujawnione, o ewentualnym sprostowaniu, usunięciu lub zablokowaniu danych (art. 12 lit. c dyrektywy 95/46/WE).

Prawo dostępu do swoich danych nie jest jednak prawem bezwzględnym, gdyż uprawnienia osoby, której dane dotyczą, do dostępu lub korekty albo wycofania danych, mogą zostać ustawowo wyłączone lub ograniczone z uwagi na bezpieczeństwo narodowe, obronność, bezpieczeństwo publiczne, działania prewencyjne, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub w sprawach o naruszenie zasad etyki w zawodach podlegających regulacji, ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi czy podatkowymi oraz funkcji kontrolnych, inspekcyjnych oraz regulacyjnych (art. 13 ust. 1 dyrektywy 95/46/WE).

Przepisy dyrektywy zawierają również wyraźne postanowienia co do zakazu zbierania w celu automatycznego przetwarzania szczególnej kategorii danych osobowych (art. 8 ust. 1 dyrektywy), chyba że sam zainteresowany wyrazi na to zgodę w formie pisemnej. Warunki legalnego przetwarzania danych sensytywnych, a także wszelkie ograniczenia tego zakazu zostały już wcześniej omówione przy okazji przedstawiania zagadnienia związanego z wrażliwymi danymi osobowymi na mocy dyrektywy 95/46/WE.

Ostatnim uprawnieniem przysługującym dysponentowi danych jest możliwość wniesienia sprzeciwu (art. 14 dyrektywy 96/46/WE). Sprzeciw może zostać wniesiony wobec

przetwarzania dotyczących danych, zebranych w warunkach, gdy było to niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego, lub gdy było to niezbędne dla wypełnienia usprawiedliwionych celów administratorów danych, jeśli administrator danych zamierza je przetwarzać w celach marketingowych. Prawo sprzeciwu przysługuje osobie, której dane dotyczą także wobec przekazania jego danych osobowych innemu administratorowi danych. Stosownie do art. 14 lit. b dyrektywy, istnieje także możliwość osobie, której dane dotyczą, wniesienia sprzeciwu wobec przetwarzania danych, które administrator danych zamierza przetwarzać dla potrzeb bezpośredniego obrotu. Zgodnie z dyspozycją art. 14 lit. b dyrektywy dysponent danych osobowych ma ponadto prawo bycia poinformowanym przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub wykorzystaniem w ich imieniu dla potrzeb bezpośredniego obrotu, jak również ma prawo wyraźnego powoływania się na prawo sprzeciwu, bez opłat, wobec ujawniania lub wykorzystywania danych.

Prawo do złożenia sprzeciwu przysługuje w dowolnym czasie z ważnych i uzasadnionych przyczyn wynikających z konkretnej sytuacji osoby, której dane dotyczą. Jeśli sprzeciw jest uzasadniony, to wówczas administrator danych nie może przetwarzać kategorii danych objętej sprzeciwem.

Opisywana dyrektywa nakłada obowiązek uwzględnienia w przepisach krajowych prawa każdej osoby do nieobjęcia jej decyzją, która wywołuje skutki prawne, jej dotyczące lub mające na nią istotny wpływ, jeśli decyzja ta została oparta wyłącznie na zautomatyzowanym przetwarzaniu danych, w wyniku którego dokonywana jest ocena niektórych dotyczących jej aspektów o charakterze osobistym, jak np. wyników osiąganych w pracy, zdolności kredytowej, wiarygodności, sposobów zachowania itp. (art. 15 ust. 1 dyrektywy 95/46/WE). Państwa członkowskie zapewniają, że każda osoba będzie mogła być wyłączona z zakresu objętego wspomnianą decyzją, jeśli decyzja taka zostanie podjęta w trakcie zawierania lub realizacji umowy, pod warunkiem, że wniosek w sprawie zawarcia lub realizacji umowy wniesiony przez osobę, której dane dotyczą, zostanie przyjęty lub że istnieją odpowiednie sposoby zabezpieczenia jej uzasadnionych interesów (jak np. uregulowania umożliwiające jej przedstawienie swojego punktu widzenia) lub gdy decyzja taka zostanie dozwolona przez prawo, które określa również sposoby zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą (art. 15 ust. 2 dyrektywy 95/46/WE).

Także obowiązek administratora do zabezpieczenia będących w jego władaniu danych przed przypadkowym lub nielegalnym zniszczeniem, przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem jest jednym z istotnych postanowień dyrektywy

95/46/WE, które niewątpliwie stały się wytycznymi do tworzenia tożsamych uregulowań w krajowych porządkach państw członkowskich, w tym Polski. Stworzenie organizacyjnych, technicznych i prawnych środków służących bezpieczeństwu przetwarzania danych jest istotnym wymogiem z punktu widzenia praktycznej realizacji prawa do ochrony danych osobowych. Zawarta w art. 17 ust. 1 zasada proporcjonalności wskazuje, by środki służące zabezpieczeniu danych osobowych były odpowiednie do zagrożeń wynikających z przetwarzania danych oraz charakteru tych danych[235].

Właściwa realizacja wszystkich przedstawionych wytycznych, które zawiera przedmiotowa dyrektywa jest niezbędna do prawidłowego i bezpiecznego przetwarzania danych osobowych. By jeszcze bardziej wzmocnić ochronę danych osobowych i zapewnić skuteczne wykonywanie zawartych w niej obowiązków, dyrektywa wymaga stworzenia instytucji kontroli i nadzoru. Instytucja taka musi być niezależna w zakresie wykonywania swoich obowiązków, zwłaszcza w odniesieniu do agencji publicznych podlegających jej kontroli. W tej kwestii w art. 28 formułuje względem każdego państwa członkowskiego obowiązek powołania całkowicie niezależnych przy wykonywaniu powierzonych funkcji, jednego lub więcej organów władzy publicznej odpowiedzialnych za kontrolę stosowania na jego terytorium przepisów niniejszej dyrektywy. Organ taki wyposażony powinien być w kompetencje kontrolne lub nawet nadzorcze wobec podmiotów korzystających z informacji osobowych, co jednak nie powinno wyłączać możliwości dochodzenia przez osoby zainteresowane swoich roszczeń przed sądem, jeśli prawo wewnętrzne kraju takie roszczenia przewiduje.

Każde państwo członkowskie ma obowiązek konsultowania się z organami nadzorczymi przy opracowywaniu środków administracyjnych lub przepisów dotyczących ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych (art. 28 ust. 2 dyrektywy 95/46/WE). Dyrektywa wyraźnie wskazuje także, jakie kompetencje powinien posiadać organ właściwy do sprawowania kontroli procesów przetwarzania danych osobowych.

Organ nadzoru ma być w pierwszej kolejności odpowiedzialny za monitorowanie, czy na jego terytorium właściwie są wykonywane postanowienia dyrektywy 95/46/WE (art. 28 ust. 1 dyrektywy 95/46/WE) oraz godnie z art. 21 dyrektywy za prowadzenie publicznego rejestru zbiorów danych osobowych. Każdy organ wyposażony ma zostać w uprawnienia

---

[235] Zob. A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej,* cz. II, ODO 2000, nr 2, s. 6.

dochodzeniowe, jak np. prawo dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych (art. 28 ust. 1 myślnik 2 dyrektywy 95/46/WE). Organ, o którym mowa, powinien posiadać także skuteczne uprawnienia interwencyjne, jak np. prawo do wyrażania opinii przed przystąpieniem do operacji przetwarzania danych, zapewnienie odpowiedniej publikacji swoich opinii, a także zarządzania blokady, usunięcia czy zniszczenia danych, nakładania czasowego czy ostatecznego zakazu przetwarzania danych, ostrzegania lub upominania administratora danych, lub tez prawo kierowania sprawy do parlamentów narodowych lub innych instytucji publicznych (art. 28 ust. 3 myślnik 2 dyrektywy 95/46/WE). Organ nadzorczy ma także na mocy dyrektywy możliwość pozywania w przypadku naruszenia przepisów o ochronie danych osobowych lub powiadamiania organów sądowych o takim naruszeniu (art. 28 ust. 3 myślnik 3 dyrektywy 95/46/WE). Decyzje organu nadzorczego nie są ostateczne, gdyż przysługuje prawo odwołania się od nich do właściwego sądu.

Dyrektywa przewiduje także możliwość kierowania skarg do organu nadzorczego, które mogą być zgłaszane przez każdą osobę lub przez stowarzyszenie ją reprezentujące, w przypadku naruszenia jej praw i wolności poprzez fakt przetwarzania jej danych osobowych (art. 28 ust. 4 dyrektywy 95/46/WE). Organ nadzorczy rozpatruje także skargi dotyczące kontroli legalności przetwarzania danych, które także mogą być kierowane przez dowolną osobę (art. 28 ust. 4 dyrektywy 95/46/WE).

Stosownie do treści art. 20 dyrektywy organ nadzorczy w ramach swoich uprawnień dokonywać ma kontroli wstępnej (ang. *prior checking*). W oznaczonych przypadkach, gdy przetwarzanie danych może prowadzić do szczególnego narażenia praw i wolności jednostki, przed rozpoczęciem procesu przetwarzania danych powinna zostać dokonana właśnie taka kontrola uprzednia (art. 20 ust. 1 dyrektywy 95/46/WE). Ten rodzaj kontroli może zostać przeprowadzony na wniosek administratora, albo osoby odpowiedzialnej za ochronę danych (urzędnika odpowiedzialnego za ochronę danych), która w przypadku wątpliwości powinna skonsultować się z organem kontrolnym[236].

W celu właściwego wypełniania przydzielonych zadań, organy nadzorcze współpracują ze sobą w zakresie koniecznym do wykonywania swoich obowiązków,

[236] Na mocy art. 20 ust. 3 dyrektywy 95/46/WE państwa członkowskie mogą również przeprowadzać takie kontrole w kontekście opracowywania odpowiedniego środka w parlamencie narodowym lub środka opartego na takim rozwiązaniu legislacyjnym, które określa charakter przetwarzania danych oraz stwarza odpowiednie zabezpieczenia.

zwłaszcza poprzez wymianę wszelkich przydatnych informacji. Każdy organ nadzorczy sporządza regularnie ze swojej działalności sprawozdanie, które jest podawane do publicznej wiadomości (art. 28 ust. 5 dyrektywy 95/46/WE).

Organ nadzorczy odgrywa także istotną rolę w przypadku stosowania procedury zawiadamiania, dokonywanej w trybie art. 18 dyrektywy o przeprowadzaniu całościowej lub częściowej operacji automatycznego przetwarzania danych. Zawiadomienia należy dokonać przed rozpoczęciem procesu przetwarzania danych (w rozumieniu omawianej dyrektywy przetwarzaniem jest także gromadzenie danych), a treść zawiadomienia dokładnie została określona w art. 19 dyrektywy. Procedura zawiadamiania organu nadzorczego służy przede wszystkim realizacji przez niego funkcji kontrolnej, w zakresie posiadania informacji co do tożsamości administratora danych, celu przetwarzania danych, kategorii przetwarzanych danych czy tożsamości odbiorcy danych. Posiadanie takich wiadomości zapewnić ma organowi kontrolnemu sporządzenie wstępnej oceny prawidłowości i bezpieczeństwa przebiegu procesu przetwarzania danych osobowych.

Ogólna dyrektywa 95/46/WE została uchwalona w celu stworzenia generalnych ram ochrony danych osobowych we Wspólnocie Europejskiej. Dopełnieniem tej dyrektywy, niezbędnym ze względu na specyfikę zagadnienia i zagrożenia dla prywatności wynikające z nieuprawnionego dostępu do danych w Internecie, są szczegółowe dyrektywy, tj.: dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego[237]; dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej[238]; dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE[239].

Uchwalenie tych dyrektyw wynika ze specyfiki procesu przetwarzania danych osobowych także w Internecie i towarzyszących mu zagrożeń dla prywatności jednostki. Ich zasięg oddziaływania obejmuje przetwarzanie niezależnie od branży czy sektora, w którym odbywa się proces przetwarzania oraz działalności administratora danych osobowych, jeżeli

---

[237] Dz. Urz. WE L 178 z 17.07.2000, s. 1.
[238] Dz. Urz. WE L 201 z 31.07.2002, s. 37.
[239] Dz. Urz. UE L 105 z 13.04.2006, s. 54.

stosuje on określone narzędzia, kanały dystrybucji lub środki komunikacji, do których odnoszą się wskazane dyrektywy[240].

Dyrektywa 95/46/WE została również uzupełniona przez szereg instrumentów przewidujących przepisy szczególne o ochronie danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych (były trzeci filar), w tym decyzję ramową 2008/977/WSiSW Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[241].

Jednym z najważniejszych dokumentów niewiążących Unii Europejskiej traktujących o prawach człowieka jest także Karta Praw Podstawowych Unii Europejskiej (dalej: Karta lub KPP UE)[242]. Zgodnie z art. 6 ust. 1 Traktatu o Unii Europejskiej uznano, że Karta ma taką samą wartość prawną jak Traktaty[243]. Na tej podstawie zatem moc prawna postanowień Karty jest równa prawu pierwotnemu Unii Europejskiej[244]. Z postanowień Karty odnoszących się do ochrony prywatności na uwagę zasługują unormowania zawarte w art. 7 i 8 , przy czym pierwszy odnosi się do prywatności w szerszym znaczeniu, zaś drugi do prywatności informacyjnej, czyli ochrony danych osobowych[245].

Art. 7 Karty Praw Podstawowych UE gwarantuje każdemu prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się, a więc zakres tego prawa odpowiada chociażby treści prawa do prywatności zawartego w Europejskiej Konwencji Praw Człowieka. KPP UE daje możliwość dochodzenia roszczeń przez osobę, której wolność lub prawo zostały naruszone tylko na podstawie samych postanowień Karty zarówno przed sądami krajowymi, jak i unijnymi. Warunkiem jest, by dana norma spełniała kryteria bezpośredniej skuteczności, przede wszystkim zaś by była dostatecznie precyzyjna[246].

---

[240] M. Krzysztofek, *op. cit.*, s. 36.
[241] Dz. U. L 350 z 30.12.2008, s. 60.
[242] Karta Praw Podstawowych Unii Europejskiej (*Charter of Fundamental Rights of The European Union*), podpisana 7 grudnia 2000 r. podczas szczytu Rady Europejskiej w Nicei przez przedstawicieli trzech organów Unii Europejskiej: Parlamentu, Rady i Komisji, została podpisana ponownie, po poddaniu jej korektom, przez przewodniczących tych organów podczas szczytu w Lizbonie 12 grudnia 2007 r. Podstawą obowiązywania Karty jest traktat lizboński; Dz. Urz. UE C 326 z 26.10.2012, s. 391.
[243] Postanowienie to ulega jednak modyfikacji w stosunku do Polski i Wielkiej Brytanii z uwagi na przyjęcie Protokołu nr 7 w sprawie stosowania Karty Praw Podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa (inaczej: protokół brytyjski). Zob. M. Jabłoński, J. Węgrzyn, J. Rzucidło, *Znaczenie protokołu nr 7 do Traktatu z Lizbony dla procesów integracyjnych w Unii Europejskiej*, „Przegląd Prawa i Administracji" 2011, nr 86, s. 67 i n.
[244] A. Wyrozumska, *Znaczenie prawne zmiany statusu karty Praw Podstawowych Unii Europejskiej,* „Przegląd Sejmowy" 2008, nr 2 (85), s. 28.
[245] J. Braciak, *Prawo do prywatności…*,s. 109.
[246] B. Banaszak, *Prawo konstytucyjne*, Warszawa 2008, s. 102.

Art. 8 KPP UE zawiera z kolei *stricte* regulację w zakresie ochrony danych osobowych. Zgodnie z treścią art. 8 ust. 1 „każda osoba ma prawo do ochrony dotyczących jej danych osobowych", a zgodnie z treścią art. 8 ust. 2 „dane te mogą być przetwarzane zgodnie z zasadami współżycia społecznego, w określonych celach i za zgoda osoby, której dotyczą, lub na innej, ustawowej podstawie posiadającej prawna legitymację. Każda osoba ma prawo do otrzymania informacji o zgromadzonych danych, które jej dotyczą oraz do spowodowania ich skorygowania". W ust. 3 tego artykułu pojawiła się zapowiedź utworzenia niezależnego organu uprawnionego do kontroli przestrzegania niniejszych przepisów[247]. Artykuł 8 jest związany z poprzednim zapisem dokumentu, który dotyczy poszanowania życia prywatnego i rodzinnego. Dane osobowe są chronione w zakresie normy gwarantującej nienaruszalność życia prywatnego i rodzinnego, jednak prawodawca chciał podkreślić rolę ochrony danych osobowych przez stworzenie indywidualnego standardu ochrony[248]. Przyczyny tego zapisu można się doszukiwać zarówno w art. 6 Europejskiej Konwencji Praw Człowieka, jak i w art. 286 Traktatu ustanawiającego Wspólnotę Europejską.

Kolejnym ważnym dokumentem, zawierającym postanowienia z zakresu prawnej ochrony danych osobowych na gruncie prawa Unii Europejskiej, jest również Traktat o funkcjonowaniu Unii Europejskiej[249]. Akt ten przyznał w treści art. 16 ust. 1 każdej osobie prawo do ochrony dotyczących jej danych osobowych. Art. 16 stanowi, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Parlament Europejski i Rada określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów.

Ustanowienie i funkcjonowanie na gruncie Unii Europejskiej regulacji w zakresie danych osobowych było bardzo istotnym dokonaniem. Zawarte tam zasady ochrony danych

---

[247] „Przestrzeganie tych przepisów podlega kontroli niezależnego organu" (art. 8 ust. 3 Karty Praw Podstawowych Unii Europejskiej).

[248] Sz. Szmak, *op. cit.,* s. 173.

[249] Geneza Traktatu o funkcjonowaniu Unii Europejskiej jest następująca: Traktat ustanawiający Europejską Wspólnotę Gospodarczą (Traktat rzymski) w latach 1958-1992, po zmianach wprowadzonych przez traktat z Maastricht- Traktat ustanawiający Wspólnotę Europejską; obecne brzmienie i tytuł nadane są przez Traktat Lizboński. Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską , podpisany 13 grudnia 2007 r., wszedł w życie 1 grudnia 2009 r.; Dz. Urz. UE C 306z 17.12.2007. Szerzej: M. Herdegen, *Prawo europejskie*, Warszawa 2006, s. 39-51.; P. Sarnecki, [w:] *Ustrój Unii Europejskiej i ustroje państw członkowskich,* red. P. Sarnecki, Warszawa- Kraków 2007, s. 22-27; J. Sozański, *Prawo Unii Europejskiej,* Warszawa- Poznań 2010, s. 22-37.

osobowych znalazły odzwierciedlenie w obowiązku ochrony cudzych danych przez inne osoby, władze publiczne oraz różne inne organy odpowiedzialne za przetwarzanie danych. Z drugiej strony, czytelne normy w zakresie ochrony prywatności zapewniły dysponentom danych gwarancję realizacji ich praw w zakresie ich kontroli oraz ochrony. Wzmocniło się dzięki temu przekonanie, iż stworzenie kompleksowych prawnych procedur w zakresie ochrony prywatności realnie gwarantuje poszanowanie praw i wolności człowieka w Unii Europejskiej.

4. Rola i kompetencje Europejskiego Inspektora Ochrony Danych

Całokształt regulacji z zakresu ochrony danych osobowych na płaszczyźnie międzynarodowej i europejskiej to nie tylko system aktów prawnych, ale także narzędzia i procedury ochrony wdrożone i funkcjonujące w oparciu o właściwe przepisy. Upowszechnianie zagadnień z zakresu ochrony danych jest coraz bardziej potrzebne, gdyż w obliczu błyskawicznego rozwoju informatyzacji i przekazu danych nie trudno jest dziś stać się ofiarą przestępstwa kradzieży tożsamości czy bezprawnego wykorzystania informacji o innej osobie. Istniejące procedury zapewniają niewątpliwie promowanie kultury ochrony danych jednostki, ale także są wzorcem do tworzenia analogicznych systemów ochrony w innych państwach na bazie wypracowanych międzynarodowych standardów ochrony danych.

Utworzenie na szczeblu ponadpaństwowym niezależnego organu zapewniającego kontrolę nad procesami przetwarzania danych osobowych w Unii Europejskiej było niewątpliwie ważnym krokiem z punktu widzenia podstawowego prawa do ochrony danych osobowych człowieka[250]. To Europa stała się kolebką ochrony danych osobowych i to w niej powstawały pierwsze regulacje prawne gwarantujące ochronę prywatności jednostce. Funkcjonowanie niezależnego organu do spraw ochrony danych osobowych pozwala w praktyce obserwować jak istotnym procesem dla bezpieczeństwa jednostki jest ochrona jej prywatności.

W 2000 r. Parlament Europejski i Rada przyjęły rozporządzenie 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i swobodnym przepływie tych danych (w skrócie: rozporządzenie 45/2001)[251].

---

[250] Zob. E. Kuczma, *Pozycja ustrojowa i rola Europejskiego Inspektora Ochrony Danych w procesie przetwarzania danych osobowych w Unii Europejskiej*, [w:] *Polska wobec standardów Unii Europejskiej*, red. P. Kuczma, Polkowice 2015, s. 87-103.

[251] Dz. U. L 8 z dn. 12.01.2001.

Rozporządzenie 45/2001 wprowadziło w życie postanowienia art. 286 Traktatu WE i stworzyło ramy prawne dotyczące przetwarzania danych osobowych przez instytucje i organy Wspólnoty[252]. Rozporządzenie to, będąc elementem prawa wtórnego w dziedzinie ochrony danych osobowych, ustanowiło powołanie niezależnego organu nadzoru procesów przetwarzania danych osobowych przez instytucje i organy Wspólnoty, tj. Europejskiego Inspektora Ochrony Danych (ang. *European Data Protection Supervisor*; w skrócie: EIOD lub Europejski Inspektor). Przepisy regulujące zagadnienia ochrony danych osobowych zaczęły obowiązywać od 2001 r., przewidując roczny okres przejściowy, jednak nominacja Europejskiego Inspektora Ochrony Danych miała miejsce dopiero w styczniu 2004 r[253]. Od tego roku konsekwentnie z każdym rokiem umacniała się i konkretyzowała pozycja Europejskiego Inspektora w procesach kontroli i nadzoru przetwarzania danych w strukturach Unii Europejskiej, co stanowiło mocną podstawę dla prowadzenia kompleksowej ochrony danych we wszystkich dziedzinach polityki Wspólnoty.

Europejski Inspektor Ochrony Danych jest niezależnym organem nadzoru odpowiedzialnym za kontrolę i stosowanie rozporządzenia (WE) 45/2001 oraz każdego innego aktu wspólnotowego dotyczącego ochrony danych osobowych[254]. EIOD działa na podstawie wspomnianego rozporządzenia 45/2001, a regulamin i ogólne warunki wykonywania przez niego obowiązków określa decyzja nr 1247/2002/WE z 1 lipca 2002 r.

Ten niezależny organ nadzoru monitoruje stosowanie przepisów rozporządzenia 45/2001 do wszystkich operacji przetwarzania danych przeprowadzanych przez instytucje lub organy Wspólnoty (art. 2 ust. 2 rozporządzenia 45/2001) i jest odpowiedzialny za poszanowanie prywatności osób fizycznych w obrębie struktur unijnych[255].

---

[252] *Europejski Inspektor Ochrony Danych, Sprawozdanie za 2004 r., streszczenie*, s.2, dostępne na stronie: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Annualreport/2004/AR_summary_PL.pdf.

[253] Zgodnie z decyzją Parlamentu Europejskiego i Rady z 22 grudnia 2003 r. pierwszym w historii Europejskim Inspektorem Ochrony Danych został mianowany na okres pięciu lat Peter Hustinx, który pełnił funkcję inspektora od stycznia 2004 r., zaś jego zastępcą został Joaquín Bayo Delgado. Od stycznia 2009 r. na stanowisko EIOD został mianowany ponownie na kolejną pięcioletnią kadencję Peter Hustinx zaś jego zastępcą został Giovanni Buttarelli. Obecnie, od 4 grudnia 2014 r., funkcję Europejskiego Inspektora Ochrony Danych pełni Giovanni Buttarelli, zaś jego zastępcą jest Wojciech Rafał Wiewiórowski.

[254] Art. 1 ust. 2 Rozporządzenia (WE) 45/ 2001- „Niezależny organ nadzoru ustanowiony przez niniejsze rozporządzenie, zwany dalej europejskim inspektorem ochrony danych, monitoruje stosowanie przepisów niniejszego rozporządzenia do wszystkich operacji przetwarzania danych przeprowadzanych przez instytucje lub organy Wspólnoty."

[255] Art. 41 ust. 2 rozporządzenia (WE) 45/2001 stanowi iż Europejski Inspektor Ochrony Danych jest odpowiedzialny za zapewnienie, że podstawowe prawa i wolności osób fizycznych, w szczególności prawo do prywatności są respektowane przez instytucje i organy wspólnotowe w odniesieniu do przetwarzania danych osobowych.

Europejski Inspektor pełni rolę doradczą względem instytucji i organów wspólnoty oraz osób, których dane dotyczą w odniesieniu do wszystkich kwestii związanych z przetwarzaniem danych osobowych[256]. Jest to organ kompetentny jedynie w odniesieniu do danych przetwarzanych przez instytucje i organy Wspólnoty, a nie jest natomiast kompetentny w odniesieniu do spraw szczebla krajowego i w związku z tym nie posiada uprawnień nadzorczych w zakresie przetwarzania danych przez organy krajowe lub przedsiębiorstwa prywatne[257].

EIOD jest powoływany przez Parlament Europejski i Radę Unii Europejskiej na pięcioletnią kadencję, w drodze wspólnego porozumienia na podstawie listy przedstawionej przez Komisję Europejską, po ogłoszeniu publicznego naboru na to stanowisko (art. 42 ust. 1 rozporządzenia 45/2001). Taka sama procedura wyboru dotyczy także stanowiska zastępcy Europejskiego Inspektora Ochrony Danych Osobowych, który to wspomaga Inspektora w wykonywaniu jego obowiązków i zastępuje go, gdy Inspektor jest nieobecny lub nie może ich wypełniać (art. 42 ust. 1 rozporządzenia 45/2001). Wymagania stawiane kandydatom to m. in niekwestionowana niezależność oraz doświadczenie i umiejętności niezbędne do wykonywania obowiązków (art. 42 pkt 2 rozporządzenia 45/2001).

EIOD korzysta z przywilejów i immunitetów, które przysługują sędziom i sekretarzowi Trybunału Sprawiedliwości Wspólnot Europejskich[258]. Traktowany jest na równi z sędzią ETS odnośnie wynagrodzenia, dodatków czy emerytury za wysługę lat. Może być on jednak zwolniony lub pozbawiony prawa do emerytury lub innych świadczeń przez Trybunał Sprawiedliwości na wniosek Parlamentu Europejskiego, Rady lub Komisji, jeśli przestanie spełniać warunki wymagane do wykonywania przez niego obowiązków lub jeśli jest winny poważnego uchybienia (art. 42 ust. 5 rozporządzenia 45/2001).

Siedziba Europejskiego Inspektora mieści się w Brukseli, aby ułatwić realizowanie jego obowiązków i zachować niezbędna bliskość między nim a podlegającymi jego nadzorowi instytucjami i organami[259]. Zgodnie z art. 43 pkt 4 rozporządzenia 45/2001 Europejski Inspektor Ochrony Danych jest wspomagany przez sekretariat. W praktyce

---

[256] *Europejski Inspektor Ochrony Danych, Sprawozdanie za 2006 r., streszczenie*, s. 2, dostępne na stronie: www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Annualreport/2006/AR_summary_PL.pdf.

[257] Pkt 16 preambuły do rozporządzenia (WE) 45/2001 stanowi, iż „niniejsze środki nie powinny mieć zastosowania do organów ustanowionych poza ramami Wspólnoty. Europejski Inspektor Ochrony Danych nie powinien mieć uprawnień do monitorowania danych osobowych przetwarzanych przez takie organy".

[258] Art. 42 ust. 7 rozporządzenia (WE) 45/2001 stanowi, iż „Art. 12-15 i 18 Protokołu w sprawie przywilejów i immunitetów Wspólnot Europejskich stosują się także do europejskiego inspektora ochrony danych."

[259] Siedziba Europejskiego Inspektora Ochrony Danych mieści się przy Rue Montoyer 63, VI, B- 1047 Bruxelles.

oznacza to wsparcie zespołu ekspertów o wszechstronnych kompetencjach, urzędników, jak i personelu sekretariatu, których wyznacza Inspektor i względem których jest przełożonym. Sekretariat liczy około 25 pracowników (ich liczba jest częścią coroczne procedury ustalania budżetu), pochodzących z różnych krajów członkowskich Unii i reprezentujących różne dziedziny zawodowe.

W wykonywaniu swoich obowiązków Europejski Inspektor jest niezależny, przez co rozumie się, iż nie oczekuje on ani nie uzyskuje żadnych instrukcji od nikogo. Jest zobligowany do powstrzymywania się od wszelkich czynności niezgodnych z jego obowiązkami, a w czasie sprawowania urzędu nie może wykonywać żadnej innej zarobkowej lub niezarobkowej działalności zawodowej. Inspektor jest związany tajemnicą zawodową zarówno w trakcie pełnienia funkcji, jak i po jej zakończeniu, w odniesieniu do wszelkich uzyskanych poufnych informacji (art. 45 rozporządzenia 45/2001), a także po zakończeniu swojej kadencji zachowuje się z uczciwością i dyskrecją w o przyjmowaniu zleceń i korzyści (art. 44 ust. 4 rozporządzenia 45/2001).

Zasadniczym celem Europejskiego Inspektora Ochrony Danych jest zagwarantowanie, że w trakcie przetwarzania danych osobowych lub opracowywania nowych strategii politycznych instytucje i organy Wspólnoty będą respektować prawo do prywatności[260]. Szczegółowe zadania Inspektora zawarte zostały w art. 46 rozporządzenia 45/2001 i obejmują one trzy dziedziny takie jak: „nadzór", „konsultacje" i „współpracę".

Pierwszym obowiązkiem EIOD jest sprawowanie kontroli. Kontrola oznacza monitorowanie przetwarzania danych osobowych w instytucjach i organach Wspólnoty przez Inspektora, we współpracy z inspektorami ochrony danych powołanymi w każdej instytucji lub organie Wspólnoty. W związku z tym Europejski Inspektor przyjmuje i bada skargi złożone przez osoby prywatne, których dane są przetwarzane przez instytucje i organy unijne, w tym przez członków personelu i administracji UE, a także prowadzi z własne inicjatywy lub na podstawie skargi, dochodzenia i dokonuje kontrole (art. 46 lit. a, b oraz j rozporządzenia 45/2001).

Każdy kto uzna, że podczas przetwarzania dotyczących go danych osobowych przez instytucje czy organy Wspólnoty jego prawa zostały naruszone, może złożyć skargę do Europejskiego Inspektora Ochrony Danych. Co do zasady w pierwszej kolejności dochodzenie swoich praw przez jednostkę powinno mieć miejsce w instytucji lub organie

---

[260] *Europejski Inspektor Ochrony Danych a ochrona danych osobowych w instytucjach i organach Wspólnoty*, Wspólnoty Europejskie 2009, Urząd Publikacji Unii Europejskiej 2009, s. 5, dostępne na stronie: www.edps.europa.eu.

Wspólnoty odpowiedzialnym za przetwarzanie danych. Jeśli nie było odpowiedzi lub odpowiedź była niesatysfakcjonująca, skargę można wnosić do inspektorów z danej instytucji lub organu, a jeśli złożenie skargi wydaje się być niezbędne, przyjmuje ją EIOD[261].

W celu zapewnienia efektywnego rozpatrywania skarg dotyczących procesu przetwarzania danych i ustalenia „elastycznej organizacji pracy tak, aby uniknąć niepotrzebnego powielania procedur […] rozbieżnych interpretacji w takich przypadkach"[262], w listopadzie 2006 r. między Europejskim Inspektorem Ochrony Danych a Europejskim Rzecznikiem Praw Obywatelskich, zajmującym się „skargami na niewłaściwe administrowanie w organach i instytucjach Unii Europejskiej", został podpisany protokół ustaleń. Wyznacza on ramy tzw. „konstruktywnej współpracy" w przypadkach należących do właściwości rzeczowej obu tych instytucji[263].

Prowadzenie dochodzeń zarówno z własnej inicjatywy EIOD, jak i na podstawie skarg jest możliwe dzięki szerokiemu wachlarzowi uprawnień, w które - na mocy art. 47 pkt 2 - został wyposażony EIOD. Ma ona zatem prawo do uzyskania od administratora lub instytucji bądź organu Wspólnoty dostępu do wszystkich danych osobowych i do wszystkich informacji koniecznych dla prowadzonych przez niego dochodzeń, jak też uzyskania dostępu do pomieszczeń, w których administrator lub instytucja bądź organ Wspólnoty prowadzi działalność, jeżeli są wystarczające powody, aby przypuszczać, że prowadzona jest tam działalność podlegająca niniejszemu rozporządzeniu.

Europejski Inspektor przyjmuje także zawiadomienia od inspektorów ochrony z danej instytucji lub organu Wspólnoty w przypadkach związanych ze szczególnym zagrożeniem praw i wolności podmiotów danych oraz dokonuje wstępnej kontroli przetwarzania takich danych (art. 47 rozporządzenia 45/2001).

Proste operacje przetwarzania danych, które nie niosą ze sobą szczególnego niebezpieczeństwa dla podmiotów danych, są nadzorowane przez inspektorów danych osobowych z danej instytucji lub organu Unii Europejskiej[264]. Każda instytucja i każdy organ wspólnoty musi mianować na mocy art. 24 rozporządzenia 45/2001 inspektora ochrony

---

[261] *Europejski Inspektor Ochrony Danych, Sprawozdanie za 2006 r., streszczenie,* s. 1.

[262] Protokół ustaleń między Europejskim Inspektorem Ochrony danych a Europejskim Rzecznikiem Praw Obywatelskich, s. 1, dostępny na stronie: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/News/06-11-30_EO_EDPS_MoU_PL.pdf

[263] A. Szczerba, *Europejski Inspektor Ochrony Danych - niezależny organ,* [w:] *Prawna ochrona danych osobowych na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008, s. 220.

[264] Pkt 32 preambuły do rozporządzenia (WE) 45/2001 stanowi, iż „w każdej instytucji lub organie Wspólnoty jeden lub więcej inspektor ochrony danych powinien zapewnić, że stosowane są przepisy niniejszego rozporządzenia i powinien doradzić administratorom w kwestii wypełniania ich zobowiązań".

danych, który jest odpowiedzialny za zagwarantowanie, że owa instytucja czy organ unijny we właściwy sposób przestrzega zasad w zakresie bezpiecznego przetwarzania danych osobowych. Inspektor danych jest osobą o znaczącym autorytecie w procesie informowania administratorów i osób, których dane są przetwarzane, o ich prawach i obowiązkach, a także współpracuje z Europejskim Inspektorem w zakresie przestrzegania rozporządzenia (WE) 45/2001[265]. To on przekazuje EIOD powiadomienia dotyczące kontroli wstępnej i w przypadku jakichkolwiek wątpliwości konsultuje się właśnie z nim.

Kontroli wstępnej dokonywanej przez Europejskiego Inspektora podlegają z kolei procesy przetwarzania danych generujące niebezpieczeństwo dla osób, których dane są przetwarzane. Dotyczy ona nie tylko działań, które jeszcze się nie rozpoczęły (tzw. „właściwe kontrole wstępne"), ale dotyczą także operacji przetwarzania danych, które rozpoczęły się przed wejściem w życie rozporządzenia lub przed 17 stycznia 2004 r.[266]. Sprawy te są wówczas załatwiane na zasadzie *ex post*.

Co więcej, Europejski Inspektor „monitoruje i zapewnia zastosowanie przepisów niniejszego rozporządzenia i każdego innego aktu wspólnotowego odnoszącego się do ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucję lub organ Wspólnoty, z wyjątkiem Trybunału Sprawiedliwości Wspólnot Europejskich działającego z mocy prawa."(art. 46 lit. c rozporządzenia 45/2001). Prowadzi on również rejestr operacji przetwarzania, o których został powiadomiony i zapewnia metody dostępu do rejestrów prowadzonych przez inspektorów ochrony danych (art. 46 lit. i rozporządzenia 45/2001).

Drugim istotnym zadaniem Europejskiego Inspektora Ochrony Danych jest dokonywanie doradztwa i konsultacji. Jest odpowiedzialny za doradzanie wszystkim instytucjom i organom Wspólnoty we wszystkich zakresach związanych z przetwarzaniem danych osobowych, co czyni to z własnej inicjatywy (doradztwo) lub w odpowiedzi na zapytanie (konsultacje). Konsultacje i doradztwo odnoszą się zarówno do propozycji nowego prawodawstwa, jak i instrumentów *soft law*, a także zagadnień technologicznych, które mogą mieć wpływ na ochronę danych[267].

Na mocy art. 28 rozporządzenia 45/2001 instytucje i organy wspólnotowe informują Europejskiego Inspektora Ochrony Danych, gdy podejmują środki administracyjne odnoszące się do przetwarzania danych osobowych, w których bierze udział instytucja lub organ

---

[265] *Europejski Inspektor Ochrony Danych a ochrona*…, s. 9.
[266] A. Szczerba, *op. cit.*, s. 221.
[267] *Ibidem*, s. 221.

Wspólnoty, samodzielnie lub razem z innymi. Chodzi tu o przepisy wykonawcze przyjęte przez instytucje i organy w dziedzinie danych osobowych. Komisja zaś konsultuje się z Europejskim Inspektorem przyjmując projekty aktu prawnego odnoszącego się do ochrony praw i wolności osoby fizycznej w odniesieniu do przetwarzania danych osobowych[268].

Monitorowanie propozycji i projektów wspólnotowych aktów prawnych w zakresie ochrony i bezpieczeństwa informacji oraz ochrony prywatności to jedno z kluczowych zadań Europejskiego Inspektora. Sporządzane regularnie przez niego (ang. *opinion*s) przyczyniają się do wypracowania spójnej polityki w zakresie ochrony danych. Opinie skierowane są do podmiotów zaangażowanych w całokształt procesów prawotwórczych a publikowane są na stronie internetowej Europejskiego Inspektora oraz w Dzienniku Urzędowym Unii Europejskiej. Analizując owe opinie pod kątem przedmiotowym można stwierdzić, że większość z nich odnosiła się do tzw. trzeciego filaru UE oraz polityki imigracyjnej i wizowej. Inspektor zwracał także szczególną uwagę na bezpieczeństwo procesów przetwarzania danych biometrycznych oraz do zachowania szczególnej staranności w przypadku nieuprawnionego udostępniania baz danych do celów innych niż pierwotnie wskazano.

Europejski Inspektor Ochrony Danych korzysta także do realizacji wspomnianych zadań z tzw. spisu zamierzeń (ang. *inventory*). Jest to dokument publikowany corocznie w grudniu i stanowi spis najważniejszych zadań, planowanych przedsięwzięć EIOD na rok następny, obejmujący też wykaz propozycji legislacyjnych Komisji Europejskiej, które mogą wymagać konsultacji z Inspektorem.

Ostatnim środkiem reakcji, z którego korzysta EIOD, są komentarze (ang. *comments*) odnoszące się do zagadnień ochrony danych osobowych zawartych w rożnych instrumentach czy środkach prawnych stosowanych przez instytucje unijne. Komentarze mogą poprzedzać spotkania Parlamentu Europejskiego czy odnosić do komunikatów Komisji Europejskiej, chociaż nie jest ona zobowiązana do przedstawiania ich w celu konsultacji z Inspektorem. Komentarze zawierają analizę polityczną i wskazówki co do zgodności proponowanych działań z zasadami ochrony.

---

[268] Pierwsza formalna opinia w tym zakresie została wydana 22 października 2004 r. Europejski Inspektor Ochrony Danych podczas wystąpienia w polskim parlamencie w dniu 26 maja 2004 r. uznał, iż zadania w zakresie konsultacji z EIOD projektów aktów prawnych odnoszących się do procesów przetwarzania i ochrony danych osobowych są strategiczne i umożliwiają mu przyjrzenie się, jaki odnoszą wpływ na prywatność jednostki we wczesnym etapie oraz umożliwiają mu przedyskutowanie wszelkich dostępnych rozwiązań alternatywnych.

Europejski Inspektor otrzymał także prawo interweniowania w sprawach dotyczących wszelkich kwestii wspólnotowych mających wpływ na ochronę danych, tak na poziomie Unii Europejskiej jak i państw członkowskich rozpatrywanych przez Trybunał Sprawiedliwości Wspólnot Europejskich, Sąd Pierwszej Instancji oraz przez Europejski Trybunał Służby Cywilnej[269].

Kolejnym zadaniem podejmowanym przez EIOD jest nawiązywanie współpracy z różnymi organami, co ma na celu zapewnienie i wzmocnienie procesów ochrony przetwarzania danych osobowych w Unii Europejskiej. Ten obszar działalności Europejskiego Inspektora obejmuje głównie kooperację nad określonymi zagadnieniami, np. wykładnię dyrektywy 95/46/WE.

Europejski Inspektor bierze udział w działalności Grupy Roboczej utworzonej na podstawie art. 29 dyrektywy 95/46/WE, która skupia krajowe organy ochrony danych i stanowi „główne forum współpracy pomiędzy organami ds. ochrony danych w Europie"[270]. W skład Grupy Roboczej wchodzą przedstawiciele krajowych organów nadzoru ze wszystkich państw członkowskich UE, a od stycznia 2004 r. także i Europejski Inspektor Ochrony Danych oraz przedstawiciele Komisji. Grupa Robocza art. 29 bada każdą kwestię dotyczącą stosowania krajowych środków przyjętych na mocy dyrektywy, aby przyczynić się w ten sposób do jednolitego i harmonijnego stosowania środków ochrony danych, przekazuje Komisji opinie na temat stopnia ochrony we Wspólnocie i w państwach trzecich, a także doradza Komisji w sprawie wszelkich proponowanych zmian dotyczących dyrektywy, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych rozwiązań wspólnotowych dotyczących praw i wolności (art. 30 dyrektywy 95/46/WE).

Współpraca EIOD dotyczy również kooperacji z organami nadzoru ochrony danych ustanowionych w ramach współpracy policyjnej i sądowej w Unii Europejskiej (Europol, Schengen czy Eurojust), krajowymi organami nadzoru, a także- na poziomie międzyinstytucjonalnym- z Inspektorami Ochrony Danych. Europejski Inspektor Ochrony Danych w zakresie nadzoru nad różnymi procesami przetwarzania danych jest także organem kontrolnym w stosunku do jednostki centralnej Eurodac[271].

---

[269] A. Szczerba, *op. cit.*, s. 223.
[270] *Europejski Inspektor Ochrony Danych, Sprawozdanie roczne za rok 2006, streszczenie*, s. 5.
[271] Rozporządzenie Rady nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania konwencji dublińskiej, dostępne na stronie: http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32000R2725&from=PL. Eurodac to system identyfikacji odcisków palców, który pozwala państwom członkowskim Unii Europejskiej zidentyfikować osoby

Analizując działalność Europejskiego Inspektora Ochrony Danych w zakresie ochrony i kontroli przetwarzania danych osobowych w Unii Europejskiej warto jeszcze zwrócić uwagę na czynny udział EIOD w konferencjach o zasięgu europejskim i międzynarodowych. Celem tego typu spotkań są głównie konsultacje, a także i popularyzacja oraz uświadamianie znaczenia zagadnień związanych z ochroną danych osobowych i ochroną prywatności jednostki na całym świecie.

Konferencje o zasięgu europejskim to głównie spotkania, w których biorą udział przedstawiciele ds. ochrony danych państw członkowskich UE i Rady Europy. Podejmowane są tam zwykle tematy dotyczące omówienia przeprowadzonych dotąd interwencji przez organy kontrolne ds. ochrony danych, analiza istniejących czy potencjalnych zagrożeń procesów ochrony danych we Wspólnocie czy wdrażanie propozycji prawnych rozwiązań w zakresie bezpieczeństwa danych jednostki mające na celu udoskonalenie procedur ochrony danych w UE.

Współpraca w obszarze międzynarodowym ma już znacznie szerszy zasięg i tym samym oddźwięk. Podczas konferencji międzynarodowych, w których obecne są krajowe i regionalne organy czy instytucje ds. ochrony danych, aktywnie uczestniczą także przedstawiciele nauki i eksperci reprezentujący środowiska naukowe z różnych dziedzin a także największe światowe podmioty gospodarcze i samorządy gospodarcze. Konferencje są najważniejszymi, corocznymi spotkaniami stanowiącymi platformę wymiany poglądów, a także wymianę i prezentację najlepszych praktyk w dziedzinie ochrony danych osobowych. Celem zaakcentowania ważności problemów ochrony danych osobowych, tradycyjnie także zaproszenie na konferencję otrzymują przedstawiciele instytucji publicznych i organizacji praw człowieka z państw – „nowych demokracji" tworzących instytucje demokratyczne, dla których uczestnictwo w konferencji stało się okazją do bliższego poznania problematyki ochrony danych osobowych"[272].

---

występujące o azyl oraz osoby zatrzymane przy próbie nielegalnego przekroczenia zewnętrznej granicy Unii. Dzięki porównaniu danych daktyloskopijnych państwa członkowskie mogą stwierdzić, czy ubiegający się o azyl lub cudzoziemiec, którego pobyt w państwie członkowskim okazał się nielegalny, nie ubiegał się poprzednio o azyl w innym państwie członkowskim, albo też czy ubiegający się o azyl nie przedostał się na terytorium Unii nielegalnie. Eurodac składa się z jednostki centralnej w obrębie Komisji, wyposażonej w skomputeryzowaną centralną bazę danych do porównywania odcisków palców, oraz systemu elektronicznego przesyłania danych pomiędzy państwami członkowskimi UE a bazą danych. Dane pobierane są od osób w wieku co najmniej 14 lat, a następnie przesyłane do jednostki centralnej za pośrednictwem krajowych punktów dostępu. System umożliwia gromadzenie odcisków palców, przechowywanych przez okres nie dłuższy niż 10 lat, a dotyczące cudzoziemców zatrzymanych przy próbie nielegalnego przekroczenia zewnętrznej granicy przez okres 2 lat i automatycznie kasowanych po upływie tego czasu.

[272] Więcej na temat konferencji, w tym międzynarodowych znajduje się na stronie: http://www.giodo.gov.pl/153/j/pl/.

Międzynarodowe konferencje są okazją do dyskusji nad nowymi problemami z zakresu ochrony danych i prywatności oraz dają możliwość prezentacji nowych technologii, które mogą być wykorzystywane w naruszaniu prywatności oraz technologii służących ochronie prywatności. W czasie konferencji przygotowywane są propozycje nowych, międzynarodowych regulacji prawnych w dziedzinie ochrony prywatności.

W ramach kooperacji międzynarodowej Europejski Inspektor aktywnie podejmuje też współpracę z organizacjami międzynarodowymi mającymi swoje siedziby w Europie[273].

Z uwagi na wyłączenie działalności takich organizacji spod krajowych systemów prawnych konieczne stało się uświadomienie istnienia uniwersalnych zasad prawnych w zakresie przetwarzania danych w organizacjach i konieczność legalnego przetwarzania danych osobowych, w tym danych wrażliwych.

Obecnie proces przeglądu ram prawnych w zakresie ochrony danych UE nabiera kształtu i przyciąga coraz większą uwagę. Jak zostało wskazane w sprawozdaniu Europejskiego Inspektora Ochrony Danych za rok 2011, „dwa podstawowe programy polityczne, program sztokholmski w sprawie przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz agenda cyfrowa – kamienie węgielne pod strategię „Europa 2020" – dowodzą, że ochrona danych to zasadniczy element legitymacji oraz skuteczności w obu dziedzinach"[274].

Europejski Inspektor Ochrony Danych jest i pozostanie aktywnie zaangażowany w działania w zakresie ochrony danych osobowych w różnych dziedzinach. Cały czas jest kładziony nacisk, aby rola Europejskiego Inspektora jako niezależnego organu nadzorczego była wykonywana we wszystkich podstawowych obszarach działalności, dbając również o jego w pełni odpowiednią organizację. Doprowadziło to do znaczących postępów zarówno w obszarze nadzoru nad przetwarzającymi dane osobowe instytucjami i organami UE, jak i w obszarze konsultacji dotyczących nowej polityki oraz działań legislacyjnych, a także w zakresie ścisłej współpracy z innymi organami nadzorczymi w celu zapewnienia spójniejszej ochrony danych. Mocna pozycja i efektywność działania europejskiego organu nadzoru wpływa także znacząco na sprawne i aktywne działanie krajowych organów nadzoru nad przestrzeganiem procesów przetwarzania danych osobowych w państwach członkowskich Unii Europejskiej.

---

[273] We wrześniu 2005 r. EIOD we współpracy z Radą Europy i OECD był gospodarzem warsztatu na temat ochrony danych w organizacjach międzynarodowych.

[274] *Europejski Inspektor Ochrony Danych, Sprawozdanie roczne za rok 2011*, streszczenie, s. 5.

5. Perspektywy ochrony danych osobowych w Unii Europejskiej

Rozwój nowych technologii i globalnej gospodarki w drugiej dekadzie XXI w. wciąż wskazuje na konieczność modernizacji mechanizmów prawnych w zakresie problematyki ochrony prywatności człowieka, które okazują się być niewystarczające i przebrzmiałe na tle rozwoju i przekazu informacji we współczesnym świecie. W Unii Europejskiej pojawiały się już od dłuższego czasu pomysły wprowadzenia nowych rozwiązań prawnych z zakresu ochrony danych osobowych, mających na celu nowelizację obowiązującej dyrektywy 95/46/WE. Wskazywano w nich na konieczność zmiany obowiązujących rozwiązań prawnych, które dogoniłyby potrzeby globalnego społeczeństwa i których stosowanie chroniłoby skutecznie jednostkę przed potencjalnymi zagrożeniami. Komisja Europejska stwierdziła, że prawo do prywatności i prawo do ochrony danych osobowych należą do zasadniczych praw Unii Europejskiej i muszą być skutecznie egzekwowane również w Internecie, przy użyciu wielu środków: od szerokiego zastosowania zasady poszanowania prywatności już od początku w stosowanych technologiach informacyjnych, po zastosowanie w stosownych przypadkach zniechęcających sankcji[275].

Propozycje Komisji Europejskiej dotyczą kompleksowej reformy przepisów o ochronie danych osobowych, tak aby zwiększyć kontrolę użytkowników nad swoimi danymi oraz by ograniczyć koszty ponoszone chociażby przez przedsiębiorstwa w związku z przetwarzaniem danych[276]. Wprowadzenie silnych i jednolitych ram prawnych na szczeblu unijnym pozwoli wzmocnić rynek cyfrowy i zapewni możliwość wprowadzania innowacji technologicznych na jeszcze większą skalę. Wnioski Komisji aktualizują i modernizują zasady zawarte w dyrektywie 95/46/WE wprowadzając je do ery cyfrowej i opierając się na wysokim poziomie ochrony danych, która obowiązuje w Europie od 1995 r.[277]

Unia Europejska podjęła próbę reformy prawa danych osobowych, co ma doprowadzić do ulepszenia prawa do ochrony prywatności jednostki w Internecie, a także stanowić impuls do rozwoju gospodarki cyfrowej w Europie[278]. Istotne jest również to, że nowe rozwiązania prawne mają zaradzić obecnemu rozdrobnieniu i kosztownym obciążeniom administracyjnym

---

[275] Zob. W. R. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, *Ochrona danych osobowych. Aktualne problemy prawnej ochrony danych osobowych*, „Monitor Prawniczy" 2012, nr 7, s. 2.
[276] Zob. E. Kuczma, *Perspektywy ochrony danych osobowych w Unii Europejskiej*, [w:] *25 Jahre Teutsch-Polnische Juristen- Vereinigung e.V.- Festschrift zum Jubiluj. Niemiecko - polskie Stowarzyszenie Prawników - Ksiega pamiątkowa z okazji 25-letniego jubileuszu,* red. E. Tuora- Schwierskott, Regensburg 2015, s. 18-29.
[277] Notatka Komisji Europejskiej z 12.04.2014 r., str. 2, http://www.giodo.gov.pl/259/id_art/7714/j/pl [dostęp: 8.04.2015].
[278] *GIODO: unijna reforma to szansa na lepsza ochronę danych*, „Dziennik Gazeta Prawna" z 18.09.2015 r.

zwłaszcza w przedsiębiorstwach, gdyż 27 państw członkowskich Unii Europejskiej wdrożyło przepisy z 1995 r. na różne sposoby, co doprowadziło do rozbieżności w ich egzekwowaniu.

Komisja Europejska w dniu 25 stycznia 2012 r. przedstawiła propozycję pakietu legislacyjnego zawierającego nowe ramy prawnej ochrony danych osobowych w Unii Europejskiej. Pakiet obejmował komunikat polityczny określający cele Komisji oraz dwa wnioski: rozporządzenie określające ogólne unijne ramy ochrony danych oraz dyrektywę Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych. Obowiązującą obecnie dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych miałoby zastąpić rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dalej określane jako: projekt rozporządzenia)[279]. Zgodnie zatem z propozycją zmian obowiązywać będą dwa akty prawne regulujące ochronę danych osobowych w Unii Europejskiej: rozporządzenie (zastępujące obecną dyrektywę 95/46/WE) i wspomniana nowa dyrektywa.

Najważniejsze kierunki zmian koncentrują się na zmianie formy prawnej aktów regulujących przetwarzanie danych osobowych we wszystkich krajach Unii, na przebudowie narzędzi, które posiadać będzie Komisja Europejska, europejskie organy ochrony i krajowe organy ochrony, a także na konstrukcji organów odpowiedzialnych za ochronę danych osobowych. Planowane zmiany objąć mają też międzynarodowy transfer danych osobowych i zasady ochrony danych w sektorze policji i wymiaru sprawiedliwości w sprawach karnych.

Opisywana reforma nie ma jednak wpływu na najważniejsze założenie ochrony danych, zgodnie z którym najistotniejszym podmiotem jest osoba, której dane dotyczą. W pierwszych przepisach projektu rozporządzenia powtórzony został przedmiot i cel wskazane w art. 1 dyrektywy 95/46/WE, koncentrujące się właśnie na zapewnieniu ochrony podstawowym prawom i wolnościom osoby fizycznej, w szczególności ich prawu do prywatności w odniesieniu do przetwarzania danych osobowych.

---

[279] Projekt Rozporządzenia dostępny na stronie: https://mac.gov.pl/files/wp-content/uploads/2013/11/TABELA-zbiorcza-GDPR-stan-31-10-2013.doc

Najistotniejszą przewidywaną zmianą jest zastąpienie obowiązującej dyrektywy rozporządzeniem. Niesie to za sobą wszelkie skutki prawne w postaci bezpośredniego obowiązywania przepisów dotyczących ochrony danych osobowych w krajach członkowskich, w tym i w Polsce, bezpośredniego stosowania rozporządzenia przez wszystkie organy publiczne oraz bezpośredniego skutku norm wynikających z takiego aktu bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego[280]. Rozporządzenie to akt, który obowiązywałby bezpośrednio w krajach członkowskich, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Dzięki jego wprowadzeniu nastąpiłaby pełna harmonizacja prawa materialnego w ramach UE i swobodnego przepływu danych[281].

Zakres przedmiotowy nowego rozporządzenia nie zmieni się nadmiernie w stosunku do obowiązujących obecnie przepisów dyrektywy 95/46/WE, gdyż dotyczyć będzie przetwarzania danych dokonywanego częściowo lub całkowicie w sposób zautomatyzowany. Obejmować będzie przetwarzanie danych w innych zbiorach, chyba że rozporządzenie zawierać będzie wyjątki, jak przetwarzanie danych w sektorze bezpieczeństwa czy polityki zagranicznej. Pojawienie się jednak takiego wyjątku nie wyklucza, że w przyszłości przetwarzanie danych dla tych celów zostałoby uregulowane jeszcze w innym akcie prawnym (np. w decyzji); jednak obecnie taki projekt nie istnieje.

W nowej dyrektywie pojawiły się także postanowienia dotyczące przetwarzania danych w związku z przeciwdziałaniem, zwalczaniem i ściganiem przestępstw oraz wykonywaniem kar nakładanych na podstawie prawa karnego państw członkowskich. Ogólne zasady ochrony danych mają zostać zastosowane w odniesieniu do współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, a przepisy dyrektywy będą miały zastosowanie do przekazywania danych zarówno w kraju, jak i do transferów transgranicznych[282].

Zasady przetwarzania danych w projekcie rozporządzenia i dyrektywy są takie same, a różnice pojawiają się odnośnie narzędzi prawnych, procedur i organów, które służą zabezpieczeniu praw osoby, której dane dotyczą[283].

---

[280] Zob. S. Wikariak, *Ochrona danych osobowych wymaga przeglądu setek aktów prawnych*, „Rzeczpospolita" z 21.09.2015.
[281] http://www.giodo.gov.pl/1520142/id_art/4587/j/pl/ [dostęp: 8.04.2015].
[282] *Sprawozdanie nr 78/2012 na temat ochrony danych osobowych* - informacje o pracach w Parlamencie Europejskim, s. 3.
[283] W. R. Wiewiórowski, *op. cit.,* s. 3.

W projekcie rozporządzenia dotyczącym ochrony danych osobowych została także uregulowana kwestia wyłączeń związanych z przetwarzaniem danych osobowych do celów osobistych i domowych. Rozporządzenie nie ma zastosowania do działań osób fizycznych, które nie mają charakteru zarobkowego (ang. *gain full interes*) i są prowadzone wyłącznie w celach osobistych i domowych. Inny reżim prawny obowiązywać jednak będzie w przypadku przekazania tych danych przez przetwarzającego nieoznaczonemu kręgowi osób.

Pozornie w projekcie rozporządzenia nie ulega zmianie również zakres terytorialny ochrony danych osobowych, gdyż przepisy unijne odnoszą się do podmiotów i zdarzeń ściśle związanych z obszarem Unii Europejskiej, jednak w praktyce zostaną wprowadzone trzy istotne zmiany.

Po pierwsze, jeśli projekt rozporządzenia wejdzie w życie, powstanie jeden obszar swobodnego przepływu danych i jednolitej ochrony danych osobowych. Kraje członkowskie będą musiały wprowadzić własne regulacje prawne w tych obszarach, które nie zostały objęte zakresem tego rozporządzenia. Jednym z takich obszarów, gdzie rozporządzenie pozostawia swobodę ustawodawcy krajowemu jest notyfikacja przetwarzania danych osobowych[284].

Drugim aspektem odnośnie zakresu terytorialnego ochrony danych jest miejsce prowadzenia działalności przez podmiot, który przetwarza dane. Projekt rozporządzenia przewiduje wprowadzenie rozwiązania *„one stop shop”,* które prowadzi do podkreślenia roli siedziby administratora danych i przetwarzającego (ang. *main establishment* – art. 51 ust. 2 projektu rozporządzenia). Koncepcja ta oparta jest na założeniu, że w przypadku prowadzenia działalności w więcej niż jednym państwie członkowskim, stosuje się jeden system prawa oraz odpowiada się wobec jednego organu nadzorczego, tj. organu do spraw ochrony danych osobowych w państwie, w którym administrator lub przetwarzający mają główną siedzibę (za taką uważa się miejsce podejmowania najważniejszych decyzji dotyczące celów, warunków i sposobów przetwarzania danych). Odpowiedzialność przed organem nadzoru kraju, w którym znajduje się siedziba administratora czy przetwarzającego, nie wyklucza możliwości współudziału przy podejmowaniu decyzji skierowanych ku takiemu administratorowi przez organy nadzorcze w innych państwach członkowskich UE.

Po wtóre, regulacjami wynikającymi z nowego aktu prawnego zostaną objęci także administratorzy spoza Unii Europejskiej, o ile operacje przetwarzania danych obejmować będą oferowanie dóbr lub usług albo kontaktowanie się z podmiotami zamieszkującymi na

[284] W Polsce ustawa wdrożeniowa będzie konieczna w zakresie np. organizacji Biura Generalnego Inspektora Ochrony Danych Osobowych, który to obszar znajduje się poza regulacją rozporządzenia unijnego.

terytorium Unii (dotyczy to np. takich dostawców jak *Linkedin* czy *Facebook*)[285]. Regulacja obejmie także nadzór nad działalnością takich podmiotów[286]. Art. 25 projektu rozporządzenia nakłada na administratorów danych spoza Unii Europejskiej, do których stosuje się rozporządzenie, obowiązek wyznaczenia przedstawiciela na terytorium Unii Europejskiej. Obowiązek ten nie dotyczy administratora z państwa trzeciego, które zapewnia odpowiedni poziom ochrony zgodnie z decyzją Komisji Europejskiej oraz administratora, który zatrudnia mniej niż 250 pracowników, a także administratora okazjonalnie oferującego produkty albo usługi na terytorium Unii, a także organów publicznych państw trzecich.

Przewidywane zmiany zapewnić mają łatwiejszy proces przetwarzania i ochrony danych przede wszystkim dla przedsiębiorców. Identyczne rozwiązania prawne obowiązujące w całej Unii zlikwidują rozbieżności ustawodawcze i niespójną strukturę ochrony danych. Zniesienie uciążliwych wymogów administracyjnych, jak np. obowiązku zawiadomienia, przyniesie znaczne oszczędności i ułatwi spełnianie wszelkich prawnych procedur. W zamian za ograniczenie obciążeń biurokratycznych zostaje zwiększona odpowiedzialność i rozliczalność *(*ang. *accountability*) administratorów danych i podmiotów przetwarzających dane osobowe.

Rozporządzenie wprowadza również kolejną zmianę w odniesieniu do obecnego stanu prawnego. Polega ona na rozróżnieniu administratora publicznego od administratora prywatnego. Z tym podziałem związany będzie odmienny katalog obowiązków spoczywający na administratorze. Dokonując pewnego skrótu można wskazać, że podmioty publiczne musiały realizować wszystkie obowiązki wynikające z treści projektu rozporządzenia, niezależnie od ilości zatrudnionych i rodzaju przetwarzanych danych. Natomiast wśród podmiotów prywatnych istniałby podział na: a) administratorów danych będących małymi przedsiębiorcami (SME), którzy nie musieliby respektować i spełniać wszystkich obowiązków; b) dużych przedsiębiorców (zatrudniających więcej niż 250 pracowników), którzy byliby zobowiązani do spełnienia wszystkich ciążących na nich wymogów w zakresie ochrony danych osobowych.

Projekt rozporządzenia ma zapewnić bezwzględne bezpieczeństwo przetwarzania powierzanych i przekazywanych danych osobowych, aby osoby, których dane dotyczą, miały zapewnioną ochronę i gwarancję swojego prawa do prywatności. Ujednolicone i unowocześnione procedury mają przede wszystkim zapewniać bezpieczeństwo przetwarzania

---

[285] M. Kluska, *Dane chronione na nowo,* „IT w administracji" 2012, czerwiec, s. 49.
[286] Takie podejście zbliża rozwiązania proponowane w nowych projektach do zasad znanych już w europejskim prawie konkurencji i ochrony konsumentów. W. R. Wiewiórowski, *op. cit.,* s. 3.

danych *on line* czy poprzez aplikacje mobilne, aby możliwe było korzystanie ze wszystkich nowości technologicznych bez obaw o bezpieczeństwo informacji w sieci.

Osoba fizyczna ma również zyskać nowe narzędzia kontroli swoich danych: prawo do zapomnienia i usunięcia danych (ang. *the right to be forgotten and to erasure* - art. 17 projektu rozporządzenia)[287]. Gdy obywatel nie chce, by jego dane były dalej przetwarzane i gdy brak jest podstaw prawnych do ich zatrzymania, dane zostaną usunięte. Jest to prawo osoby, której dane dotyczą, by nakazała administratorowi danych, w sytuacji, gdy odpowiada ona za upublicznianie danych osoby, nie tylko ich usunięcie, ale również poinformowania innych podmiotów o takim żądaniu dysponenta danych, jeżeli inne podmioty przejęły od niego dane[288]. Z kolei prawo do bycia zapomnianym to uprawnienie pozwalające kontrolować zasadność obrotu danymi przez obce podmioty i umożliwiające lepiej zarządzać ryzykiem związanym z ochroną danych w Internecie[289].

Projekt nowego rozporządzenia przewiduje także wyposażenie jednostki w prawo do przenoszenia swoich danych (art. 21), które ułatwi dostęp do swoich danych, a także usprawni przekazywanie swoich danych pomiędzy dostawcami usług.

Zmiana dotychczasowych ram prawnych ochrony danych osobowych dotyczyć ma także wprowadzenia procesu wrażliwego przetwarzania (ang. *risky processing*) zamiast ochrony danych wrażliwych. Polega on na wprowadzeniu zakazu, z pewnymi wyjątkami, przetwarzania danych osobowych ujawniających rasę lub pochodzenie etniczne, poglądy polityczne, religię lub przekonania, przynależność do związków zawodowych oraz przetwarzania danych genetycznych lub danych dotyczących zdrowia lub seksualności, wyroków skazujących lub powiązanych środków zabezpieczających (art. 9 projektu rozporządzenia).

---

[287] Rozwiązanie takie było już przewidziane w art. 12 dyrektywy 95/46/WE, ale art. 17 projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (SEC 2012/72 final, SEC 2013/ 73 final) jest znacznie bardziej wyczerpujący i rozbudowany. Projekt rozporządzenia dostępny na stronie: https://mac.gov.pl/files/wp-content/uploads/2013/11/TABELA-zbiorcza-GDPR-stan-31-10-2013.doc

[288] Zob. G. Santor, *The Right to be Forgotten. Dynamics of Privacy and Publicity*, [w:] *Protection of Information and the Right to Privacy- A new Equilibrium?*, red. L. Floridi, Law, Governance and Technology Series, Vol. 17, s. 1-15; U. Pagallo, M. Durante, *Legal Memories and the Right to be Forgotten*, [w:] *Protection of Information and the Right to Privacy- A new Equilibrium?*red. L. Floridi, Law, Governance and Technology Series, Vol. 17, s. 17-30.

[289] Pomysł ten jest szeroko krytykowany zwłaszcza przez właścicieli serwisów społecznościowych. Zwracają oni uwagę, że jedynym technicznym rozwiązaniem umożliwiającym realizacje takiego uprawnienia byłoby dołączanie *cookies* do wszystkich materiałów wprowadzonych przez osobę do ich serwisów. Tymczasem operowanie takimi *trackig cookies* jest poddane szczegółowemu reżimowi prawnemu innych przepisów unijnych. Dochodzi zatem do swoistej kolizji przepisów unijnych, kiedy Unia Europejska daje możliwość śledzenia, co się dzieje z danymi użytkownika, podając w innym akcie prawnym, że śledzenie takie nie jest wskazane. W. R. Wiewiórowski, *op. cit.,* s. 4.

Już w preambule do projektu rozporządzenia zostało wskazane, że ochrona praw i wolności osób fizycznych w zakresie przetwarzania ich danych wymaga, by „odpowiednie środki techniczne i organizacyjne" zostały wykorzystane dla wypełnienia zasad wynikających z rozporządzenia tak na etapie projektowania zasad przetwarzania danych, jak i podczas właściwego procesu przetwarzania danych. Zasadom tym poświęcony jest cały art. 23 projektu rozporządzenia (i odpowiadający mu art. 21 dyrektywy), w którym wskazane jest „uwzględnienie ochrony danych już w fazie projektowania oraz ochrona jako opcja domyślna"[290]. Nowe ramy ochrony proponowane przez Komisje Europejską, opierające się na wskazaniach Europejskiej Agendy Cyfrowej[291] oraz Komunikatu Komisji w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności[292], uznają, że przy przygotowaniu do przetwarzania danych osobowych niezbędne jest także uwzględnienie ochrony prywatności w fazie projektowania.

Ochrona danych już w fazie projektowania (ang. *privacy by design*) oraz ochrona danych jako opcja domyślna (ang. *privacy by default*) staną się nieodzownymi zasadami w przepisach unijnych odnoszących się do ochrony danych. Oznacza to, iż gwarancje ochrony danych powinny być wbudowane w produkty czy usługę począwszy od najwcześniejszego etapu ich tworzenia, realizacji, wykorzystania i ostatecznie usunięcia oraz, że domyślne ustawienia ochrony prywatności powinny być normą i standardem w przypadku sprzedaży usług czy produktu. Kwestia prywatności oraz ochrony danych ma zatem być uwzględniania w całym cyklu technologicznym, poczynając od etapu wczesnego projektowania technologii, po ich wdrożenie, wykorzystanie i ostateczne usunięcie. Preambuła do projektu rozporządzenia wraz z jego art. 23 nakazują administratorowi danych, by wdrożył odpowiednie polityki i środki celem wypełnienia zasad ochrony danych *by design* oraz *by default*. Obie te zasady powinny być brane pod uwagę także przy tworzeniu przez Komisję

---

[290] Art. 23 „Uwzględnienie ochrony danych już w fazie projektowania oraz ochrona danych jako opcja domyślna. Ust. 1. Uwzględniając najnowsze osiągnięcia techniczne oraz koszty wdrożenia, administrator, zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, wdraża odpowiednie środki i procedury techniczne i organizacyjne, tak by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia oraz gwarantowało ochronę praw podmiotu danych. Ust. 2. Administrator wdraża mechanizmy służące zapewnieniu, by domyślnie przetwarzane były jedynie te dane osobowe, które są niezbędne dla realizacji każdorazowego szczególnego celu przetwarzania, oraz by w szczególności nie były one zbierane lub zatrzymywane dłużej niż przez okres niezbędny do realizacji tych celów, zarówno jeśli chodzi o ilość danych, jak i okres ich przechowywania". Mechanizmy te zapewniają w szczególności, by dane osobowe nie były domyślnie udostępniane nieograniczonej liczbie osób.

[291] Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie „Europejskiej Agendy Cyfrowej" COM (2010) 245.
Dostępny na stronie: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PL:PDF.

[292] Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności- COM (2007) 228, dostępny na stronie : http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52007DC0228&from=PL

Europejską aktów wykonawczych do niniejszego rozporządzenia (art. 23 ust. 3 i 4 projektu rozporządzenia).

W projekcie nowego rozporządzenia pojawiły się także zmiany dotyczące zasad profilowania (art. 20 projektu rozporządzenia). Profilowaniem określa się dwie grupy czynności podejmowanych przez przetwarzającego dane. W pierwszej zbierane są dane z różnych źródeł, o których wiadomo, że dotyczą tej samej zidentyfikowanej osoby. Jest to więc operacja obejmująca zespół technik *data miningu*[293] dokonywana na zbiorach, w których przetwarzamy dane, co do których istnieją silne podstawy, by sądzić, iż dotyczą one tej samej osoby i są one wystarczająco dobrej jakości, aby wspólnie tworzyć wartość dodaną[294]. Według drugiego ujęcia profilowanie odnosi się do pojedynczej osoby i polega na wnioskowaniu o cechach nieznanych dla *data minera* z cech przypisanych już wcześniej danej osobie. Ta metoda obejmuje zazwyczaj tworzenie profili grupowych, na których gromadzone są cechy wielu osób. Z pewnym uproszczeniem można zatem przyjąć, iż „profil" jest to zestaw danych charakteryzujący kategorię osób, który ma zostać zastosowany w odniesieniu do danej osoby, a „tworzeniem profili" określa się automatyczną technikę przetwarzania danych polegającą na przypisaniu danej osobie „profilu" w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw[295].

Projekt rozporządzenia wprowadza zakazy oraz ograniczenia w zakresie profilowania. I tak każda osoba fizyczna ma prawo nie podlegać środkowi, który wywołuje skutki prawne dotyczące tej osoby fizycznej lub ma istotny wpływ na tę osobę fizyczną, a który opiera się wyłącznie na automatycznym przetwarzaniu danych mającym służyć ocenie niektórych aspektów osobistych tej osoby fizycznej lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej (art. 20 ust. 1 projektu rozporządzenia).

Projekt rozporządzenia określa także przypadki, gdy dana osoba może zostać poddana jednemu ze środków, o których mowa w art. 20 ust. 1. Ich zastosowanie możliwe jest jednak tylko wtedy, gdy przetwarzanie odbywa się w trakcie zawierania lub wykonania umowy (jeśli wniosek w sprawie zawarcia lub wykonania umowy złożony przez podmiot danych został zrealizowany) lub jeśli: przewidziano właściwe środki w celu zabezpieczenia słusznych

---

[293] W języku angielskim *data mining* oznacza proces eksploracji danych określany także jako pozyskiwanie danych, wydobywanie danych. Jest to jeden z etapów procesów odkrywania wiedzy z baz danych.
[294] W. R. Wiewiórowski, *op. cit.*, s. 5.
[295] *Ibidem*, s. 5.

interesów podmiotu danych (jak np. prawo do uzyskania interwencji ze strony człowieka) albo przetwarzanie jest wyraźnie dozwolone przez prawo Unii lub państwa członkowskiego, które ustanawia również właściwe środki w celu zabezpieczenia słusznych interesów podmiotu danych albo odbywa się na podstawie zgody podmiotu danych, z zastrzeżeniem warunków określonych w art. 7 oraz właściwych gwarancji.

Kolejne zmiany przepisów unijnych w zakresie ochrony danych osobowych dotyczyć mają także zniesienia nałożonego dyrektywą 95/46/WE generalnego obowiązku rejestracji zbiorów danych. Art. 28 projektu rozporządzenia zakłada, że administrator danych oraz przetwarzający dane mają obowiązek przechowywać dokumentacje dotyczącą zbioru, który musi zostać ujawniony organowi ochrony danych na jego żądanie. Reforma notyfikacji ma na celu uproszczenie systemu zgłaszania przetwarzania danych osobowych. Służyć temu ma również uprzednia zgoda i uprzednia konsultacja przetwarzania danych. Zgodnie z treścią art. 34 projektu rozporządzenia uprzednia zgoda udzielona przez organ ochrony danych jest wymagana w dwóch przypadkach przekazania danych za granicę, tj. gdy: a) stosowane są tzw. klauzule umowne, b) nie ma odpowiednich środków ochronnych zagwarantowanych przez państwo przekazujące. Uprzednia konsultacja, którą także zakłada art. 34 projektu rozporządzenia, wymagana jest, gdy w wyniku oceny wpływu na prywatność przeprowadzonej przez administratora danych wynika, że przetwarzanie danych wiąże się z wysokim stopniem ryzyka z uwagi na charakter danych, ich zakres czy cele przetwarzania. Organ ochrony danych może uznać taką konsultację za konieczną, gdy istnieje prawdopodobieństwo, że przetwarzanie danych stanowi konkretne ryzyko dla praw oraz wolności osób, których dane dotyczą przez jego naturę, zakres i/lub cel przetwarzania[296]. Jednocześnie organ ochrony danych ma obowiązek przygotowania listy spraw, które będą przedmiotem uprzedniej konsultacji.

W celu bezwzględnego respektowania unijnych przepisów w zakresie ochrony danych, projekt rozporządzenia (w rozdziale IV „Administrator i podmiot przetwarzający") zakłada obowiązek powoływania inspektora ochrony danych[297]. Ma on być powołany przez administratora lub podmiot przetwarzający w każdym podmiocie, który jest organem publicznym, a także w jednostkach zatrudniających więcej niż 250 stałych pracownikach i w jednostkach, w których przetwarzanie danych wiąże się z systematycznym nadzorem nad osobami, których dane dotyczą (art. 35 projektu rozporządzenia). W ten sposób obecna

[296] W. R. Wiewiórowski, *op. cit.*, s. 5.
[297] Obecnie na mocy polskiej ustawy o ochronie danych osobowych istnieje możliwość powołania zgodnie z art. 36a u.o.d.o. administratora bezpieczeństwa informacji (ABI), ale nie jest to obowiązek a jedynie uprawnienie.

pozycja administratora bezpieczeństwa informacji (ABI) zostanie znacząco wzmocniona, gdyż uzyska on nowe uprawnienia. Do najważniejszych zadań nowego ABI należeć będzie: ułatwianie działań i doradzanie administratorowi danych i przetwarzającemu, monitorowanie wdrażania dokumentacji z zakresu ochrony danych, monitorowanie wykonywania i stosowania przepisów rozporządzenia, a w szczególności zasad ochrony danych *by design* i *by default*, zapewnienie prowadzenia i właściwego zabezpieczenia dokumentacji związanej z przetwarzaniem danych osobowych, monitorowanie zgłoszeń i zawiadomień dotyczących naruszeń ochrony danych osobowych, pełnienie roli „punktu kontaktowego" dla organu nadzorczego w kwestiach związanych z przetwarzaniem i ochroną danych osobowych (art. 37 projektu rozporządzenia).

Z kolei w gestii administratora lub podmiotu przetwarzającego będzie kontrola, czy ABI terminowo i właściwie wykonuje swoje obowiązki związane z zapewnieniem ochrony danych osobowych i w tym względzie oficer ds. ochrony podlegać będzie bezpośrednio kierownictwu administratora lub podmiotu przetwarzającego. Nie oznacza to jednak możliwości wydawania mu poleceń, gdyż powinien on zachować niezależność w swoich działaniach w stosunku do administratora danych (art. 36 ust. 2 projektu rozporządzenia).

Reforma europejskich ram prawnych ochrony danych osobowych służyć ma wzmocnieniu roli organów nadzorczych. Przewiduje się również zacieśnienie współpracy między tymi organami oraz koordynacja ich działań. Projekt nowego rozporządzenia wymaga, aby w przepisach krajowych został wskazany organ nadzorczy, którego celem ma być nadzorowanie przestrzegania przepisów projektowego rozporządzenia i przyczynienie się do jego jednolitego stosowania na terytorium całej Unii Europejskiej. Właściwość miejscowa organu nadzorczego ma obejmować terytorium państwa członkowskiego (art. 51 ust. 1 projektu rozporządzenia). W przypadku, gdy przetwarzanie danych odbywać się ma w kontekście działalności administratora lub podmiotu przetwarzającego ustanowionych na terytorium UE, a administrator lub podmiot przetwarzający prowadzą działalność w więcej niż jednym państwie członkowskim, organ nadzorczy głównej siedziby administratora lub podmiotu przetwarzającego jest odpowiedzialny za nadzór nad działalnością administratora lub podmiotu przetwarzającego we wszystkich państwach członkowskich (procedura „*one stop shop*", czyli „punkt kompleksowej usługi"; art. 51 ust. 2 projektowanego rozporządzenia).

Projekt rozporządzenia zakłada także wymóg zagwarantowania całkowitej niezależności organów nadzorczych przy wykonywaniu powierzonych im uprawnień i

obowiązków[298]. W stosunku do organów nadzorczych istnieje niepołączalność stanowisk i funkcji (*incompatibilitas*), zakaz zwracania się do innych podmiotów o instrukcje i zakaz przyjmowania instrukcji związanych z wykonywaniem swojego stanowiska. Organ nadzoru ma obowiązek postępować w sposób uczciwy i ostrożny w odniesieniu do obejmowania stanowisk i obowiązuje go zakaz przyjmowania korzyści także po zakończeniu sprawowania kadencji. Członkowie organu nadzorczego powinny powstrzymywać się od wszelkich czynności niezgodnych ze swoimi obowiązkami i podczas swojej kadencji nie mogą podejmować żadnej funkcji, zarobkowej lub niezarobkowej, stojącej w sprzeczności z tymi obowiązkami. Organ ten powinien zostać wyposażony w odpowiednie zasoby ludzkie, techniczne i finansowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wypełniania swoich zadań i personelu powołanego przez szefa organu nadzorczego i podlegającego jego kierownictwu. W stosunku do organu nadzorczego przewidziany ma być także odrębny roczny budżet i kontrola finansowa, która nie może naruszać jego niezależności.

Członkowie organu nadzorczego powinni być wybierani przez parlament albo przez rząd danego państwa członkowskiego. Kandydaci powinni być osobami, których niezależność jest niekwestionowana i których doświadczenie oraz umiejętności wymagane do wykonywania obowiązków, w szczególności w dziedzinie ochrony danych osobowych, zostały wykazane. Członek organu przestaje pełnić swoje obowiązki w razie upływu kadencji, rezygnacji lub przymusowego pozbawienia funkcji. Szczegóły dotyczące powyższych wymogów mają zostać doprecyzowane w przepisach krajowych. Członkowie i personel organu nadzorczego związani są także tajemnicą służbową. Podczas kadencji i po jej zakończeniu podlegają oni obowiązkowi zachowania tajemnicy służbowej w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wykonywania obowiązków służbowych.

Kompetencje organów nadzorczych projekt rozporządzenia ujmuje jako obowiązki (art. 52 projektu rozporządzenia) i uprawnienia (art. 53 projektu rozporządzenia).

Podstawowymi obowiązkami organu nadzorczego ma być: nadzorowanie (monitorowanie) i zapewnienie stosowania rozporządzenia, rozpatrywanie skarg osób, których dane poddawana są przetwarzaniu (lub zrzeszeń reprezentujących takie osoby), prowadzenie postępowania w sprawie skarg oraz informowanie o wynikach takiego postępowania, dzielenie się informacjami oraz zapewnianie pomocy innym organom

[298] Artykuł 47 wyjaśnia warunki niezależności organów nadzorczych, co stanowi realizację orzeczeń Trybunału Sprawiedliwości Unii Europejskiej, i zostało także zainspirowane art. 44 rozporządzenia (WE) nr 45/2001.

nadzorczym oraz spójność stosowania rozporządzenia, prowadzenie postępowań kontrolnych (dochodzenia) z własnej inicjatywy lub na podstawie skargi czy wniosku innego organu nadzorczego i informowanie podmiotu danych w rozsądnym czasie, jeżeli skierował on skargę do tego organu nadzorczego, o wyniku postępowania, nadzorowanie (monitorowanie) zmian w odpowiednich dziedzinach, o ile mają one wpływ na ochronę danych osobowych, w szczególności rozwoju technologii informacyjnych i komunikacyjnych oraz praktyk handlowych. Organ nadzorczy ponadto udziela konsultacji instytucjom i organom państw członkowskich na temat środków prawnych i administracyjnych dotyczących ochrony praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych. Udziela on także zwolnień (ang. *prior authorisation*) na operacje przetwarzania, o których mowa w art. 43 oraz udziela konsultacji w tym zakresie. Ponadto wydaje opinie na temat projektów kodeksów postępowania i uczestniczy w działalności Europejskiej Rady Ochrony Danych[299].

Na mocy art. 53 organy nadzoru zostały wyposażone w uprawnienie do zawiadamiania administratora lub podmiotu przetwarzającego o domniemanym naruszeniu przepisów regulujących przetwarzanie danych osobowych; stosownych przypadkach organ nadzoru może nakazać administratorowi lub podmiotowi przetwarzającemu usunięcie naruszenia w konkretny sposób w celu poprawy ochrony podmiotu danych. Organ nadzoru ma prawo nakazać administratorowi lub podmiotowi przetwarzającemu dane spełnienia żądań przedstawionych przez podmioty danych dotyczących skorzystania z praw przewidzianych w rozporządzeniu oraz nakazać tym podmiotom (lub ich przedstawicielom) dostarczania każdej informacji istotnej w toku wykonywania jego obowiązków. Organ nadzoru ma także uprawnienie do ostrzegania i upominania administratora i podmiotu przetwarzającego, nakazania poprawienia, usunięcie czy zniszczenia wszystkich danych, jeżeli były one przetwarzane z naruszeniem przepisów rozporządzenia oraz powiadomienia o takich działaniach osób trzecich, którym dane zostały ujawnione. Ponadto ma możliwość nałożenia czasowego lub ostatecznego zakazu przetwarzania, zawieszenia przepływu danych do odbiorcy w państwie trzecim lub w organizacji międzynarodowej a także wydawania opinii na każdy temat związany z ochroną danych osobowych.

Na skutek reformy przepisów unijnych w zakresie ochrony danych osobowych, w polskim systemie prawnym zastosowanie będą mieć także przypisy dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych

---

[299] Na mocy art. 64 i art. 66 projektu rozporządzenia podstawowym celem działalności Europejskiej Rady Ochrony Danych jest zapewnienie spójnego stosowania rozporządzenia.

osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych, (jako drugi z proponowanych przez reformą przepisów unijnych akt prawnych z zakresu ochrony danych osobowych). Zasady zawarte w zaprezentowanym projekcie nie są obecne w istniejących dziś polskich przepisach prawa. Celem wprowadzenia nowej dyrektywy jest ujednolicenie zasad przetwarzania danych osobowych w policji i w wymiarze sprawiedliwości. Będzie mieć ona zastosowanie do przetwarzania danych osobowych przez właściwe organy w celu przeciwdziałania, zwalczania dochodzenia przestępstw oraz wykonywania kar. Komisja Europejska nie zdecydowała się jednak na wprowadzenie aż tak daleko idącego ujednolicenia jak w przypadku rozporządzenia, gdyż projekt dyrektywy ma zastąpić decyzję ramową 2008/997/WSiSW, która podobna jest w swym charakterze do projektu dyrektywy. W projekcie dyrektywy nie uregulowano kwestii dostępu policji do danych w sektorze prywatnym[300]. Reguły przekazywania danych za granicę mają znacznie niższy poziom ochrony, a organy ochrony danych nie uzyskały tak mocnej pozycji prawnej, jak to zostało ujęte chociażby w projekcie rozporządzenia. Projektowana dyrektywa nie ma zastosowania do instytucji, organów i agencji Unii Europejskiej, nie wpływa na przyjęte wcześniej akty prawne ustanawiające systemy wymiany informacji w zakresie współpracy policyjnej i sądowej. Definicje legalne zawarte w projekcie dyrektywy zostały po części zaczerpnięte z dyrektywy 95/46/WE i z decyzji ramowej 2008/997. Część z nich pozostała w swym pierwotnym kształcie, inne zostały zmodyfikowane albo uzupełnione o nowe elementy. Pojawiły się jednak też zupełnie nowe definicje pojęć takich jak: „naruszenie danych osobowych", „dane genetyczne", „dane biometryczne", „dane dotyczące zdrowia, czy „dziecko".

Nowa dyrektywa wprowadza obowiązek rozróżniania pomiędzy danymi osobowymi różnej kategorii osób, nawiązując tym samym do rekomendacji Komitetu Ministrów Rady Europy (87)15 oraz do przepisów o Europolu i Eurojustu. Wprowadza też zasady dotyczące realizacji obowiązku informacyjnego i realizacji praw osób bazując na dyrektywie 95/46/WE i decyzji ramowej 2008/997, a także obowiązek powołania oficera ds. ochrony danych, określając jego status i zakres obowiązków.

W odniesieniu do organów ochrony danych, ich status i kompetencje zostały określone w podobny sposób jak i w projekcie rozporządzenia, obejmując prowadzenie postępowań

---

[300] Decyzja Ramowa Rady 2008/997/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. Urz. L Nr 350 z 20.12.2008 r., s. 60).

wyjaśniających i inspekcyjnych, z wyłączeniem ich właściwości co do nadzoru przetwarzania danych przez sądy w ramach ich działalności orzeczniczej. Projekt dyrektywy zawiera bardzo ograniczone przepisy w zakresie wzajemnej pomocy pomiędzy organami ochrony i nakazuje powołanie Rady Ochrony Danych, która ma tylko uprawnienia doradcze.

6. Ochrona prywatności informacyjnej w wybranych państwach

a) uwagi ogólne

Idea prawa do ochrony prywatności kształtowała się dynamicznie acz różnorodnie w poszczególnych państwach na świecie. W ramach ochrony prywatności sukcesywnie powstawały uregulowania prawne zapewniające ochronę informacjom osobowym o obywatelach danych państw i nie tylko. Interpretacja prawa do prywatności, w tym granice ochrony danych osobowych i regulacje stanowiące jej konkretyzację, różnią się w poszczególnych częściach świata, stąd trudno jest uzyskać międzynarodową harmonię w tym zakresie. Odmienne kultury, istnienie różnorodnych systemów politycznych i prawnych, prymat indywidualizmu bądź kolektywizmu często bywają uzasadnieniem, akceptowanym społecznie, do zwiększenia uprawnień różnych organów czy instytucji kosztem prywatności jednostki[301]. Nie bez znaczenia pozostaje też wrażliwość jednostek i grup społecznych oraz ich chęć do wprowadzania zmian. W konsekwencji tych okoliczności nie w każdym kraju musi być zapewniona ochrona tych samych wartości dla spełnienia społecznego postulatu ochrony prywatności[302].

Zagadnienia związane z bezpieczeństwem prywatności informacyjnej cechuje różnorodność przyjętych rozwiązań, a różnice pojawiają się chociażby w zakresie zadań organu odpowiedzialnego za ochronę danych. Wspólną cechą natomiast większości systemów jest to, że ochrona danych osobowych i prywatności jednostki nie jest przedmiotem wyłącznie jednego aktu prawnego, a zwykle przepisy szczególne dotyczące tych materii znajdują się w regulacjach sektorowych.

Dla potrzeb niniejszej pracy warto zaznaczyć, że to właśnie rozwój odmiennych koncepcji z zakresu prawa do prywatności wyodrębnił wiele innych wartości wpisujących się w idee ochrony prywatności jednostki. I tak obok ochrony dobrego imienia, czci, godności,

---

[301] M. Krzysztofek, *op. cit*., s. 20.
[302] J. Braciak, *Prawo do prywatności…,* s. 30.

korespondencji czy miru domowego na przestrzeni lat rozwinęła się koncepcja prawnej ochrony danych osobowych człowieka. Pomijając więc wnikliwe i całościowe analizy dotyczące ochrony prywatności informacyjnej człowieka w systemach prawnych państw na świecie, przedstawię te, które, moim zdaniem, są najbardziej znaczące.

b) Stany Zjednoczone

Jak już była mowa, w doktrynie toczą się spory nie tylko o definicję prawa do prywatności, ale także o to, kto jest jego autorem. Według najszerszej rozpowszechnionego stanowiska, prawo do prywatności ma swoje początki w Stanach Zjednoczonych wraz z opublikowaniem artykułu pt. *The Right to Privacy*. Z tego tez względu pokrótce ale w pierwszej kolejności skupię się na przedstawieniu amerykańskich regulacji z zakresu ochrony danych osobowych człowieka.

W zakresie wyznawanych wartości i rozwiązań ustrojowych, między USA a Unią Europejską istnieje bardzo dużo podobieństw, ale są jednak i różnice. Jedną z nich jest podejście do ochrony danych osobowych. Podejście do ochrony danych w Stanach Zjednoczonych jest odmienne od panującego na terytorium Unii Europejskiej[303]. Unia Europejska przykłada bardzo dużą rolę do dbania o prawa jednostki, w tym o ochronę danych osobowych i prawa do prywatności. Każdy kraj członkowski ma obowiązek powołać własnego regulatora ds. Ochrony Danych Osobowych. W Polsce taką rolę pełni Generalny Inspektor Ochrony Danych Osobowych.

W Stanach Zjednoczonych podejście do prawa do prywatności różni się od europejskiego. Sam fakt, że nie istnieje tam chociażby odpowiednik polskiego GIODO, powoduje daleko idące konsekwencje. Brakuje organu czy instytucji, której celem byłaby kontrola i nadzór nad procesami przetwarzania informacji o charakterze osobowym i ochrona prawa do prywatności człowieka. W USA prywatność uznaje się jako wartość równą wszelkim innym wartościom, konkurującą z nimi, a nawet traktowaną niekiedy jako drugorzędną w stosunku np. do wolności słowa. W UE prywatność traktuje się zaś jako prawo podstawowe. Niewątpliwie można pokusić się o stwierdzenie, iż prywatność w Stanach Zjednoczonych wywodzi się z założeń biznesu, gdyż ochrona danych osobowych traktowana jest jako element prawa konsumenckiego, zaś podejście europejskie czerpie z praw

[303] Zob. D. J. Solove, Ch. J. Hoofnagle, *A Model Regime of Privacy Protection*, "University of Illinois Law Review", Vol. 2006, No. 2, s. 358 i n.

podstawowych człowieka. Tym samym prawo unijne związane z ochroną prywatności jest chronione przy użyciu rozległych uregulowań i wyrażane z użyciem aktów prawnych obejmujących zarówno sektor prywatny jak i publiczny. W USA obowiązują wąskie regulacje skupione na określonych gałęziach gospodarki lub specyficznych kontekstach użycia danych osobowych. Tylko te wybrane sektory[304] i dziedziny, zidentyfikowane jako narażone na ryzyko naruszeń ochrony danych, są poddane określonej prawem ochronie danych osobowych. Główny nacisk w USA położony jest na tzw. autoregulację przeprowadzaną przez samych operatorów, poprzez wydawanie tzw. kodeksów lub kart postępowania, co jest wynikiem silnej inicjatywy prywatnych organizacji zajmujących się ochroną danych osobowych, a bardzo często stanowi część wewnętrznej polityki przedsiębiorstwa[305].

Niezależnie od ochrony danych osobowych na szczeblu federalnym, sfera prywatności jest także regulowana w przepisach stanowych[306]. Administracja federalna pod wpływem Kongresu i silnych grup nacisku wielokrotnie odmawiała głosowania nad ogólnym aktem prawnym dotyczącym ochrony danych osobowych, stąd w USA brak jest ogólnych uregulowań prawnych w zakresie ochrony danych osobowych. W 2012 r. prezydent B. Obama złożył w dokumencie „*Consumer data Privacy in Networked Word: A Framework for Protecting Pricay and Promoting Innovation in the Globar Digital Economy*" deklarację dążenia do uchwalenia federalnych przepisów o ochronie danych osobowych, obejmujących zarówno elementy samoregulacji podmiotów przetwarzających dane osobowe, jak i zawierających powszechnie obowiązujące ramy ochrony danych[307].

Biorąc pod uwagę prawną sytuację Stanów Zjednoczonych w zakresie ochrony danych osobowych, Komisja Europejska uznała, iż USA nie zapewniają odpowiedniego poziomu ochrony wymaganego dyrektywą (w EU prawo zakazuje przetwarzania danych osobowych w

---

[304] Do amerykańskich ustaw federalnych określających zasady gromadzenia i dalszego przetwarzania danych osobowych w ramach działalności gospodarczej należą m. in: *Driver's Privacy Protection Act* (ustawa o ochronie prywatności kierowcy, 18 U.S.C § 2721), *Electronic Founds Transfer Act* (ustawa o elektronicznym przekazywaniu środków pieniężnych, 15 U.S.C § 1693 i n.), *Rright to Financial Privacy Act* (ustawa o prawie do prywatności finansowej, 12 U.S.C § 3401 i n.), *Telephone Consumer Protection Act* (ustawa o ochronie konsumentów usług telefonicznych, 47 U.S.C § 227), *Children's Online Privacy Protection Act* (ustawa o ochronie prywatności dzieci w sieci, 15 U.S.C § 6501-6506- M. Krzysztofek, *Ochrona…*, s. 49; oraz regulacje prawa prywatności odnoszące się do tajemnicy bankowej- *Bank Secrecy Act of 1970 (Currency and Foreign Transactions Reporting Act.* Zob. R. Kraemer, M. Porzycki, Ochrona *danych osobowych w instytucjach finansowych z amerykańskiej perspektywy*, „Transformacja Prawa Prywatnego" 2001, nr. 4.

[305] K. Kowalik, *Safe Harbour - porozumienie dotyczące wymiany danych osobowych miedzy krajami Unii Europejskiej a Stanami Zjednoczonymi*, „Przegląd Prawa Europejskiego" 2002, nr 1 (11), s. 40.

[306] Np. Floryda nie ma żadnej ustawy zawierającej definicję danych osobowych, a np. Arizona ma ich pięć.

[307] Biały Dom, 23 lutego 2012 r., http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. Szerzej: M. Krzysztofek, *op. cit.,* s. 50.

przypadku braku podstawy prawnej, zaś w USA przetwarzanie jest dopuszczalne do momentu powodowania szkody lub pojawienia się zakazu wynikającego z przepisu prawa).

Według unijnych standardów wprowadzonych dyrektywą 95/46/WE, dane osobowe mogą opuścić obszar Unii Europejskiej, jeśli przekazywane są do państwa, w którym panuje adekwatny poziom ochrony danych. Dyrektywa zakazuje przekazywania danych osobowych do krajów niezapewniających odpowiedniego poziomu zabezpieczeń. Dyrektywa ta jednak nie okazała się jednak aż tak bardzo radykalna, gdyż w art. 25 dopuszcza wyjątki, poprzez wyliczenie sytuacji, w których pomimo braku należytej ochrony dopuszczalne jest przekazywanie danych. Przekazywanie danych z Unii Europejskiej do USA, które nie mieściło się w granicach wyjątku z art. 25 dyrektywy, w rzeczywistości zatem można było uznać za nielegalne. Z uwagi na różnice pomiędzy prawodawstwem Unii Europejskiej a Stanów Zjednoczonych i brak ogólnych uregulowań prawnych w zakresie ochrony danych osobowych, państwo to nie mogło zostać uznane za gwarantujące odpowiedni poziom ochrony danych osobowych. Mając na uwadze, że sytuacja taka w znacznym stopniu hamuje wymianę gospodarczą pomiędzy Unią Europejską, a USA Departament Handlu Stanów Zjednoczonych w zapewnieniu możliwości transferu informacji o charakterze handlowym, głównie danych o klientach i pracownikach, wypracował w porozumieniu z Komisją Europejską program *Safe Harbour* (ang. bezpieczna przystań)[308], tj. umowę regulującą możliwość wymiany danych i umożliwiającą amerykańskim podmiotom gospodarczym sprostanie wymaganiom wskazanym w Dyrektywie[309]. Uzyskanie certyfikatu programu *Safe Harbour* przez uczestniczące w nim podmioty zapewnia, że gwarantują one odpowiedni poziom ochrony danych osobowych, o którym mowa w dyrektywie 95/46/WE[310].

Porozumienie to jest przeznaczone wyłącznie dla organizacji amerykańskich (przedsiębiorstw), otrzymujących dane o charakterze osobowym z UE. Nie zastępuje ono przepisów krajowych przyjętych w celu wykonania dyrektywy, stosowanych w związku z przetwarzaniem danych w pastwach członkowskich Unii Europejskiej[311]. *Safe Harbour* nie ma charakteru wiążącego dla państwa amerykańskiego. Ma charakter wiążący raczej „indywidualnie", co oznacza, że zaczyna obowiązywać przedsiębiorstwo dopiero wówczas,

---

[308] Prawidłowa pisownia słowa *„harbor"* (co oznacza zatokę lub przystań) to *„harbour",* zaś w języku amerykańskim „*harbor*".

[309] Zob. A. Genz, *Datenschutz in Europa und den USA: Eine Rechtsvergleichende Untersuchung unter Besonderer Berücksichtigung der Safe-Harbor-Lösung (DuD-Fachbeiträge)*, Jnuar 2004.

[310] Program *Safe Harbour* został zatwierdzony przez Unię Europejską decyzją Komisji 2000/520/WE z dnia 26 lipca 2000 r. (O.J. L 215, 25.08.2000 s. 0007 – 0047). Więcej informacji o programie *Safe Harbour*; można znaleźć na stronie: http://www.export.gov/safeharbor. Treść decyzji Komisji 2000/520 dostępna jest na stronie: http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32000D0520&from=en

[311] K. Kowalik, *op. cit.*, s. 41.

gdy się do niego formalnie przyłączy[312]. Przedsiębiorstwa amerykańskie na zasadzie dobrowolności przystępowały zatem do programu ochrony danych gwarantującego odpowiedni poziom zabezpieczenia, zobowiązując się do przestrzegania siedmiu zasad (ang. *principles*) ochrony życia prywatnego Europejczyków, których dane są przekazywane. Od tego momentu przedsiębiorstwo mogło obracać danymi osobowymi, przy zachowaniu warunków przewidzianych w porozumieniu i pod groźbą sankcji.

W praktyce stosowanie zasad programu *Safe Harbour* nie okazało się jednak doskonałe i bezproblemowe. Wprawdzie w celu badania i rozpatrywania skarg na naruszenie zasad ochrony danych osobowych przewidzianych programem *Safe Harbour* powołany został specjalny panel składający się z przedstawicieli różnych organów ochrony danych osobowych działających w Unii Europejskiej ale to okazało się niewystarczające. Z uwagi na brak istnienia w USA instytucji czy organu, który specjalizowałby się w ochronie prawa do prywatności, nie istnieją specjalistyczne procedury w zakresie ochrony danych osobowych. To zatem właśnie brak realnej kontroli nad certyfikowanymi podmiotami okazuje się największą słabością *Safe Harbor*.

Obecnie w wyniku wydania przez Trybunał Sprawiedliwości UE w październiku 2015 r. wyroku w sprawie *Maximilian Schrems* vs. *Data Protection Commissioner*[313], w którym stwierdził on nieważność decyzji Komisji Europejskiej z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach "bezpiecznej przystani" przez Stany Zjednoczone, administratorzy danych nie mogą przekazywać danych do USA na podstawie unieważnionej przez TSUE decyzji Komisji Europejskiej. W konsekwencji, aktualnie uczestnictwo importera danych z USA w programie *Safe Harbour* nie pozwala już na uznanie, że przekazanie do niego danych oznacza przekazanie danych do państwa trzeciego[314].

Na dziś dzień postanowienia programu pozostały utrzymane w mocy, jednak nieważna jest decyzja, która uznawała, że organizacje z USA, wpisane listę *Safe Harbor*, gwarantują „odpowiedni poziom ochrony danych". W praktyce jednak bez przedmiotowej decyzji, cały amerykański program staje się mało użyteczny. Członkowstwo w programie nie umożliwi już

---

[312] Przystąpienie do „strefy bezpieczeństwa" powoduje, że przedsiębiorstwo zostaje wpisane na listę prowadzoną przez ministra handlu lub transportu w USA. Dotychczas do programu przystąpiło ponad 5 tys. amerykańskich przedsiębiorstw. Aktualną listę można sprawdzić pod adresem: http://safeharbor.export.gov/list.aspx

[313] Orzeczenie ETS w sprawie C-362/14 z dnia 6 października 2015 r.

[314] Zob. Stanowisko GIODO w sprawie przekazywania danych do USA. Dostępne na str. http://www.giodo.gov.pl/560/id_art/9054/j/pl

firmom z USA przetwarzania danych z Unii Europejskiej na tych zasadach, co przed wydaniem orzeczenia przez ETS. Na mocy oświadczenia europejskich urzędów ochrony danych osobowych zrzeszonych w ramach Grupy Roboczej Artykułu 29 ds. Ochrony Danych, od 16 października 2015 r. biegnie trzymiesięczny okres karencji w sprawie egzekwowania wyroku ETS unieważniającego unijne gwarancje dla programu *Safe Harbor*.

c) Wielka Brytania

Prace nad prawną regulacją ochrony danych osobowych w Wielkiej Brytanii zapoczątkowane zostały już w latach 70. XX w. W 1984 r. uchwalono ustawę o ochronie danych osobowych (*Data Protection*), jednak potrzeba dostosowania nowoczesnych technologii przetwarzania danych, a także konieczność implementacji norm prawa wspólnotowego sprawiły, że wspomniana regulacja prawna została zastąpiona nową ustawą o ochronie danych osobowych w 1998 r. (*Data Protection Act 1998*- DPA), która weszła w życie 1 marca 2000 r[315]. Dodatkowo uzupełniały ją akty wykonawcze do ww. ustawy[316].

Na mocy przepisów dotyczących ochrony danych osobowych uregulowano podstawowe zasady przetwarzania danych, prawa osób, których dane dotyczą, obowiązki podmiotów przetwarzających dane, zadania organów ochrony danych oraz zasady odpowiedzialności za naruszenie przepisów o ochronie danych osobowych[317]. Także w przepisach o ochronie danych osobowych zawarto zagadnienia dotyczące różnych typów kontroli i zapewnienia tym samym odpowiedniego poziomu ochrony danych zgodnie z założeniami Dyrektywy 95/46/WE.

Brytyjski organ do spraw ochrony danych osobowych korzysta z mechanizmów kontroli instytucjonalnej, funkcjonalnej, indywidualnej i uzupełniającej. Kontrola instytucjonalna sprawowana jest obecnie przez dwa podmioty: Komisarza (Rzecznika) ds. Informacji (ang. *Information Commissioner*) oraz Trybunał ds. Informacji (ang. *Information Tribunal*)[318]. Komisarz jest niezależnym organem nadzorczym dysponującym własnymi

---

[315] Zob. D. Banisar, *op. cit.,* s. 30-32.
[316] P. Fajgielski, *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno- prawne*, Lublin 2008, s. 116.
[317] P. Fajgielski, *Kontrola…,* s. 116.
[318] Nazwy opisywanych organów zmieniały się na mocy nowelizacji przepisów. W ustawie z 1984 r. organ właściwy w sprawach ochrony danych nazwany był Urzędnikiem ds. Ochrony Danych (ang. *data Protection Registrar*), w ustawie z 1998 r. zmieniono jego nazwę na Komisarza ds. Ochrony Danych (ang. *data Protection Commissioner*), a ustawą z 2000 r. o wolności informacji (ang. *Freedom of Information Act 2000, chapter 36*) jeszcze raz zmieniono nazwę organu na Komisarza ds. Informacji (ang. *Information Commissioner*). Podobnie w

pracownikami oraz biurem. Sprawuje on kontrolę, wykorzystując do tego różne instrumenty prawne, jak chociażby notyfikację zbiorów danych osobowych[319]. Podmiot, który zamierza rozpocząć przetwarzanie danych, powinien poinformować o tym Komisarza. Ustawa zwalnia z obowiązku informowania podmioty prowadzące rejestry publiczne, przewiduje także możliwość określenia w przepisach wykonawczych innych zwolnień (*Data Protection Act, chapter* 17). Dokonane zgłoszenie wiąże się z obowiązkiem wniesienia opłaty. Komisarz prowadzi rejestr, do którego wpisuje dane zawarte w zgłoszeniu. Rejestr jest jawny i każda zainteresowana osoba może uzyskać dostęp do informacji w nim zawartych[320]. Celem powstania tego rejestru jest zapewnienie przejrzystości procesów przetwarzania danych. Aby zapewnić aktualność danych osobowych w rejestrze, ustawa nakłada na administratorów danych obowiązek zawiadamiania Komisarza o zmianach danych objętych obowiązkiem zgłoszeniowym. Niedopełnienie obowiązku powiadomienia oraz uaktualnienia się zgłoszonych danych stanowi wykroczenie. Cała procedura przyjmowania zgłoszenia oraz prowadzenie rejestru zapewnia Komisarzowi możliwość prowadzenia kontroli uprzedniej procesu przetwarzania danych osobowych.

Obowiązkiem Komisarza jest także bieżąca kontrola przestrzegania przez administratorów przepisów o ochronie danych osobowych i promowanie dobrych praktyk w tym zakresie. Każda osoba, której dane poddawane są przetwarzaniu, może zwrócić się do Komisarza z wnioskiem o dokonanie oceny przetwarzania danych (ang. *requests for assessment*). Komisarz wówczas kontroluje, czy podmiot przetwarza owe dane zgodnie z przepisami przedmiotowej ustawy. W przypadku stwierdzenia naruszenia przepisów ustawy, w szczególności podstawowych zasad ochrony danych, Komisarz jest uprawniony do wydania noty nakazującej (ang. *enforcement notice*)[321], zawierającej w sobie żądanie podjęcia określonych działań lub powstrzymanie się od określonych działań w ramach zgodności z zasadami ochrony danych osobowych.

W przypadku, gdy istnieją uzasadnione powody do przypuszczenia, że doszło do naruszenia przepisów ustawy lub może do tego dojść, Komisarz może przeprowadzić inspekcję. Przed planowaną inspekcją jest wysyłana do podmiotu kontrolującego nota z

---

2000 r. zmieniono nazwę z Trybunał ds. Ochrony Danych (ang. *data Protection Tribunal*) na Trybunał ds. Informacji (ang. *Information Tribunal*). Zob. P. Fajgielski, *Kontrola…*, s. 116- 125.

[319] Szczegółowe zagadnienia dotyczące procedury notyfikacyjnej zostały określone w przepisach wykonawczych do ustawy DTA tj. ang. *The Data Protection* (*Notyfication and Notyfication Fees*) *Regulations 2000* (Statutory Instrument No.1088).

[320] Komisarz publikuje rejestr na swojej stronie internetowej, pod adresem: http:// www.ico.gov.uk.

[321] W polskim systemie prawnym brak jest dokładnego odpowiednika takiego środka prawnego, stąd mogą pojawić się trudności w precyzyjnym tłumaczeniu jego nazwy. Zob. P. Fajgielski, *op. cit.*, s. 118.

zawiadomieniem o przeprowadzeniu kontroli. Jeśli podmiot odmówi spełnienia żądań wskazanych w nocie, to wówczas Komisarz zwraca się do właściwego sądu o uzyskanie nakazu wstępu i przeszukania miejsca, w którym mogą znajdować się dowody. Jak wskazuje P. Fajgielski, „właśnie zapewnienie «uprzedniej sądowej autoryzacji» w tym zakresie uznaje się w literaturze za charakterystyczną cechę brytyjskiej regulacji, dotyczącej kontroli przetwarzania i ochrony danych osobowych"[322].

Oprócz typowych uprawnień kontrolnych przepisy brytyjskiej ustawy przyznają Komisarzowi także inne uprawnienia i nakładają na niego określone obowiązki. Komisarz jest uprawniony do wydawania kodeksów dobrych praktyk w zakresie ochrony danych osobowych, ma obowiązek konsultowania się z zainteresowanymi podmiotami przy tworzeniu tego rodzaju regulacji. Szczególnym uprawnieniem brytyjskiego Komisarza ds. Informacji jest także dokonywanie oceny zgodności procesów przetwarzania danych z kodeksami dobrych praktyk, przy czym tego rodzaju audyt możliwy jest jedynie za zgodą administratora danych (sekcja 51 (7) DPA). Do zadań Komisarza należy także współpraca z organami nadzorczymi innych państw w spawach dotyczących ochrony danych. Komisarz składa raz na rok sprawozdanie ze swej działalności przed każdą z izb parlamentu[323].

W ramach omawiania zagadnień odnoszących się do kontroli instytucjonalnej warto także wspomnieć o pracach legislacyjnych zmierzających do zwiększenia skuteczność działań Komisarza ds. Informacji. Przedmiotem procedury legislacyjnej są przepisy *Criminal Justice and Information Act*, przewidujące możliwość nakładania kar pieniężnych na podmioty, które w sposób zamierzony bądź lekkomyślny naruszają przepisy ustawy o ochronie danych osobowych.

Kontrola funkcjonalna w zakresie przetwarzania danych nie została wyraźnie wskazana w przepisach brytyjskiej ustawy. Obowiązek jej sprawowania wynika jednak z siódmej zasady ogólnej określonej przepisami DPA, na podstawie której należy podjąć odpowiednie środki techniczne i organizacyjne w celu zapobieżenia nieuprawnionemu lub bezprawnemu przetwarzaniu danych orz przypadkowej utracie, uszkodzeniu bądź zniszczeniu danych. Taka kontrola wewnętrzna stanowi rodzaj środków organizacyjnych, które są konieczne do zapewnienia należytej ochrony przetwarzania danych. Komisarz ds. Informacji, przedstawiając wykładnię przepisu zawierającego siódmą zasadę ochrony danych, uznał, że wskazanie konkretnej osoby lub departamentu odpowiedzialnego za politykę bezpieczeństwa

---

[322] P. Fajgielski, *Kontrola…,* s. 120.

[323] Sprawozdanie jest także publikowane i udostępniane na stronie internetowej Komisarza, pod adresem: http://ico.gov.uk.

w danej organizacji jest jednym z istotnych elementów zarządzania bezpieczeństwem, obok ustanowienia polityki bezpieczeństwa, wprowadzenia mechanizmów kontroli dostępu oraz określenia procedur przetwarzania danych. Wyznaczona osoba lub wskazany departament powinien wypełniać obowiązki z zakresu kontroli funkcjonalnej przetwarzania i ochrony danych. Jednocześnie Komisarz wskazuje, iż owe zagadnienia traktowane są jako szczegółowe kwestie techniczne i w tym zakresie odsyła do norm i standardów technicznych: BS 7799 oraz ISO/IEC 17799[324]. Wdrożenie adekwatnych i koniecznych środków natury organizacyjnej i technicznej zostałp powierzone administratorom danych, którzy na podstawie analizy okoliczności i konkretnego przypadku najlepiej dostosują zabezpieczenia do istniejących lub potencjalnych zagrożeń.

Kontrola indywidualna przetwarzania i ochrony danych ściśle związana jest z realizacją uprawnień osób, których dane dotyczą i są poddane przetwarzaniu. Przepisy omawianej ustawy wyposażają osoby zainteresowane w szereg uprawnień, dających możliwość sprawowania faktycznej kontroli w zakresie przetwarzania ich danych przez inne podmioty. Są to m. in: prawo dostępu do danych na swój temat i informacji o przetwarzaniu tych danych; prawo żądania zaprzestania przetwarzania danych; prawo żądania odszkodowania oraz prawo domagania się poprawienia, zablokowania lub usunięcia nieprawidłowych danych[325]. Uprawnienia te zapewniają rzetelność oraz uczciwość przetwarzania danych osób zainteresowanych, a także dają możliwość wpływu na nieprawidłową politykę przetwarzania danych u administratorów. Ponadto, jeśli podmiot danych uważa, że administrator danych przetwarza jego dane w sposób niewłaściwy, co wpływa lub może wpłynąć na szkodę jego lub innej osoby, to podmiot danych jest uprawniony, aby wysłać do administratora notę (ang. *data subject notice*) zawierającą żądanie zaprzestania w określonym czasie przetwarzania tych danych[326]. Dotyczy to zarówno sytuacji, gdy podmiot danych sprzeciwia się w ogóle przetwarzaniu danych, jak i gdy osoba zainteresowana kwestionuje jedynie przetwarzanie danych dla konkretnego celu albo przetwarzanie w określony sposób. Administrator w terminie 2 dni ma obowiązek ustosunkować się do treści noty i wskazać, czy spełnił lub zamierza spełnić jego żądanie lub że uważa żądanie za bezpodstawne. Uprawnienie do żądania zaprzestania przetwarzania danych nie przysługuje jednak w następujących sytuacjach:

a) podmiot danych wyraził wcześniej zgodę na przetwarzanie danych:

---

[324] Zob. T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Gliwice 2006.
[325] P. Fajgielski, *Kontrola…,* s. 122.
[326] *Ibidem,* s. 123.

b) przetwarzanie danych jest niezbędne do zawarcia lub realizacji umowy na podstawie uprzedniego wniosku podmiotu danych;

c) przetwarzanie jest niezbędne do zawarcia; realizacji umowy na podstawie uprzedniego wniosku podmiotu danych;

d) przetwarzanie jest niezbędne do spełnienia obowiązku wynikającego z przepisów prawa lub gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów określonej osoby[327].

Osoba, której została wyrządzona szkoda lub krzywda w związku z nieprawidłowym przetwarzaniem danych, uprawniona jest do uzyskania odszkodowania i zadośćuczynienia (przepisy sekcji 13 DPA). Jeśli podmiot danych i administrator nie dojdą jednak do porozumienia w kwestii odszkodowania czy zadośćuczynienia, wówczas podmiot danych może wystąpić w tej sprawie do sądu (a także, gdy podmiot uważa, ze jego dane przetwarzane przez administratora są nieprawidłowe). Jest to charakterystyczny dla brytyjskiej regulacji mechanizm prawny, gdy sądy rozstrzygają w kwestii poprawienia, zablokowania, skasowania lub zniszczenia danych. Działalność brytyjskich sądów jest określana w aspekcie ochrony danych jako kontrola uzupełniająca, kiedy to sądy orzekają w kwestiach odpowiedzialności za naruszenie przepisów ustawy. Rozstrzygają one spory, są władne oceniać zgodność przetwarzania danych z przepisami obowiązującego prawa, a uznając osobę winną naruszenia przepisów mogą nakazać usunięcie danych, z którymi wiązało się naruszenie. Zakres kontroli sądowej w świetle przepisów brytyjskiej ustawy jest więc bardzo rozległy. Charakter kontroli uzupełniającej sprawują także częściowo prokuratorzy, którzy są uprawnieni do wniesienia oskarżenia przed właściwy sąd w przypadku podejrzenia, że administrator danych, naruszając przepisy o ochronie danych, popełnił przestępstwo.

W Wielkiej Brytanii wprowadzono też rozwiązania prawne kumulacyjnie regulujące ochronę danych osobowych oraz dostęp do informacji publicznej. Takie rozwiązanie jest jak najbardziej uzasadnione, gdyż przedmiotem regulacji w obu przypadkach jest dostęp do informacji. Brytyjski organ powołany do ochrony danych osobowych Rzecznik Informacji (ang. *Information Commissioner*) czuwa nad przestrzeganiem przepisów o ochronie danych osobowych i o wolności informacji (*Freedom of Information Act* z 2000 r. i *Data Protection Act* z 1998 r.); jednocześnie zapewnia jednolite orzecznictwo dotyczące granic prawa do prywatności osób sprawujących funkcje publiczne"[328].

---

[327] *Ibidem*, s. 124.

[328] A. Mednis, *Ustawa o ochronie danych osobowych a zagraniczne regulacje w tym zakresie*, [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008, s. 101-102.

Przykładem anglosaskiego modelu ochrony prywatności jednostki jest także regulacja obowiązująca w Australii. Australijskim aktem prawnym regulującym tematykę związaną z ochroną prywatności i ochroną danych osobowych jest *Privacy Act* z 1988 r., który reguluje nie tylko podstawowe ogóle zasady ochrony danych osobowych, ale także zasady przetwarzania danych w niektórych sektorach, m. in: informacji kredytowej, podatkowej i medycznej. Organem ochrony prawa jest Rzecznik Prywatności (*Privacy Commissioner*). Zakres właściwości Rzecznika wynika głównie z *Privacy Act* , który to akt wbrew tytułowi chroni wyłącznie aspekt ochrony danych osobowych[329]. Rzecznik został wyposażony w uprawnienia do działania w sprawach naruszeń innych niż tajemnica danych aspektów prywatności, np. tych, które pojawiają się w komunikacji elektronicznej[330].

d) Niemcy

System ochrony prywatności informacyjnej w Niemczech jest wart przedstawienia, a to chociażby z uwagi na fakt, że pierwsze kroki w kierunku prawnego uregulowania zagadnień z zakresu ochrony danych osobowych poczynione zostały właśnie w 1970 r. w Hesji (RFN)[331], gdzie uchwalono pierwszą na świecie ustawę o ochronie danych osobowych[332]. Obecnie w Niemczech cały system ochrony danych osobowych składa się z trzech współpracujących ze sobą elementów, przy czym ustawa o ochronie danych osobowych jest podstawowym aktem prawnym w zakresie ogólnej regulacji w systemie prawnej ochrony danych osobowych[333].

Pierwszym z elementów niemieckiego systemu ochrony danych osobowych jest konstytucyjna ochrona praw zasadniczych. W Ustawie Zasadniczej z 1949 r. brak jest

---

[329] A. Mednis, *Ustawa…*, s. 101-102.
[330] W Polsce sprawami tego zakresu zajmuje się np. Prezes Urzędu Komunikacji Elektronicznej. Zob. *Ibidem,* s. 102.
[331] Zob. G. Gonzáles Fuster, *The Emergencje of Personal Data Protection as a Fundamental Wright of the EU,* Law, Gevernance and Technology Series, Vol. 16, s. 56.
[332]Kolejne ustawy uchwaliły parlamenty: Szwecji (1973 r.), Kanady (1977 r.), w 1978 r. Francji, Austrii, Danii i Norwegii, a w 1979 r. parlament Luksemburga. Nieco później regulacje tego tupu wprowadziły niemal wszystkie kraje Europy Zachodniej i niektóre Środkowoeuropejskie. I tak przykładowo ustawa o ochronie danych osobowych i dostępie do danych publicznych została uchwalona w 1992 r. na Węgrzech, 29 kwietnia 1992 r. Republika Czeska i Słowacka przyjęły czesko-słowacką ustawę o ochronie danych osobowych w systemach informacyjnych, a w Słowenii od 7 marca 1990 r. obowiązuje ustawa o bezpieczeństwie danych osobowych. T. Justyński, *Ochrona obywatela i konsumenta w świetle niemieckiej ustawy o ochronie danych osobowych*, „Państwo i Prawo" 1998, z. 3, s. 74; S. Sagan, *Generalny Inspektor Ochrony Danych Osobowych*, [w:] *Organy i korporacje ochrony prawa*, red. S. Sagan, J. Ciechanowska, Warszawa 2010, s. 121.
[333] Zob. G. Gonzáles Fuster, *op. cit*., s. 60; *Datenschutz- und Informationsrecht. Ausgabe für Hessen*, Juris Lex 2015.

indywidualnie sformułowanego i wyodrębnionego prawa każdego obywatela do ochrony jego danych osobowych (niem. *Recht auf informationelle Selbstbestimmung*)[334]. Trybunał Konstytucyjny RFN (niem. *Bundesverfassungsgericht*) wyprowadził prawo do ochrony danych osobowych z prawa podstawowego, tj. ogólnego prawa osobistości (niem. *Persönlichkietsrecht*), na które składa się zasada nienaruszalności godności człowieka (art. 1 niemieckiej Ustawy Zasadniczej) oraz prawo do swobodnego rozwoju osobowości (art. 2 ust. 1 niemieckiej Ustawy Zasadniczej)[335]. Trybunał nazwał to prawo jako prawo do samostanowienia w sferze informacji (*Recht auf informationelle Selbstbestimmung*), które stanowi niejako reakcję na nowoczesne metody pozyskiwania, przetwarzania i gromadzenia danych osobowych i ma chronić jednostkę przed nadużyciami w tym zakresie[336].

Drugą istotną sferą systemu ochrony informacji w Niemczech jest ustawodawstwo federalne. Najważniejszym aktem w tym zakresie jest obecnie obowiązująca ustawa o ochronie danych osobowych (niem. *Bundesdatenschutzgeset*-BDSG), ogłoszona w dniu 14 stycznia 2003 roku[337], ostatnio zmieniona artykułem 1 ustawy z dnia 14 sierpnia 2009 roku[338].

Zgodnie z § 1 II BDSG niemiecka ustawa o ochronie danych osobowych odnosi się do gromadzenia, przetwarzania i wykorzystywania danych osobowych przez federalne instytucje publiczne, władze publiczne krajów związkowych oraz podmioty niepubliczne.

Niemiecka ustawa federalna została podzielona na trzy części, a niemieccy eksperci ds. ochrony danych osobowych skoncentrowali się na wprowadzeniu nowych rozwiązań prawnych, stąd zawiera ona pewne swoiste uregulowania w zakresie ochrony danych osobowych.

W części pierwszej ustawy został określony jej cel i zakres, najważniejsze definicje oraz ogólne przepisy dotyczące przetwarzania danych osobowych. Wśród nowych definicji, adekwatnych do wymogów dyrektywy 95/46/WE znalazły się takie pojęcia, jak: „pseudonimizacja" („*aliasing*"), „anonimizacja" („*rendering anonymous*") oraz „osobiste, przenośne media do przechowywania i przetwarzania danych" („*mobile personal storage and processing media*"), których przykładem mogą być coraz bardziej rozpowszechnione karty chipowe. Artykuł 6c znowelizowanej ustawy federalnej określa obowiązki ciążące na

---

[334] Zob. D. Janicka, Ustawa zasadnicza w praktyce Republiki Federalnej Niemiec (1948-1989)…., s. 140 i n.
[335] B. Banaszak, M. Bernaczyk, *Aktywizm sędziowski we współczesnym państwie demokratycznym*, Warszawa 2012, s. 195 oraz T. Justyński, *op. cit.*, s. 75.
[336] B. Banaszak, M. Bernaczyk, *op. cit.*, s. 195.
[337] Federalny Dziennik Ustaw I str 66.
[338] Zob. Federalny Dziennik Ustaw I str 2.814; G. Verlag, *Bundesdatenschutzgesetz: Bundesdatenschutzgesetz (BDSG),*Auflage 2015.

podmiocie wydającym tego rodzaju media w zakresie powiadomienia podmiotu danych (o ile podmiot danych nie posiada poniższych informacji) o nazwie i adresie, uproszczonym sposobie funkcjonowania medium i rodzaju danych, jakie mogą być na nim przetwarzane, sposobie wykonywania przysługujących praw, środkach jakie zostają podjęte w przypadku zgubienia lub zniszczenia medium. Należy zapewnić również podmiotom danych odpowiedni, bezpłatny dostęp do danych zapisanych na medium oraz określić jasno procedurę inicjującą przetwarzanie danych na tego rodzaju nośnikach. Szczególnie interesującym, nowym rozwiazaniem w niemieckiej ustawie federalnej jest art. 6b dotyczący monitorowania miejsc publicznych z wykorzystaniem optycznych urządzeń elektronicznych. Na podstawie tego przepisu, video nadzór („*video-surveillance"*) jest dopuszczalny tylko wówczas, gdy jest to konieczne dla: wykonania zadań publicznych, realizacji prawa określenia przyznania lub odmowy dostępu, realizacji słusznych interesów dla szczegółowo określonych celów; jeżeli brak wskazania, że słuszny interes podmiotu danych jest w tym przypadku przeważający.

W zakresie zaś kontroli procesów przetwarzania danych zgodnie z art. 9 istnieje możliwość kontrolowania podmiotów przetwarzających dane osobowe przez niezależnych i autoryzowanych przez organ ochrony danych inspektorów. Kontrola dotyczy zarówno administratorów danych, jak i podmiotów dostarczających odpowiednie oprogramowanie systemowe wykorzystywane przy przetwarzaniu danych. Ocenie podlega ogólna koncepcja ochrony, jak i środki techniczne zastosowane w celu ochrony danych. Jeżeli w toku kontroli stwierdzono, że dany podmiot spełnia niezbędne wymogi w zakresie ochrony danych osobowych, przyznawany jest wówczas odpowiedni certyfikat (*privacy labels*).

W federalnej ustawie o ochronie danych osobowych oddzielnie została uregulowana ochrona przetwarzania danych przez instytucje publiczne i prywatne, co stanowi konsekwencję oceny ryzyka wynikającego z procesu przetwarzania danych. Ustawodawca niemiecki uznał, iż przetwarzanie danych przez instytucje publiczne stanowi większe niebezpieczeństwo dla obywatela i społeczeństwa niż analogiczna działalność jednostek prywatnych[339]. Jest to odmienne stanowisko niż występujące w regulacjach wspólnotowych, gdzie instytucje publiczne i prywatne zostały objęte takim samym reżimem prawnym.

W drugiej części ustawy federalnej określone zostały zasady przetwarzania danych przez podmioty publiczne, w tym w szczególności: podstawy prawne przetwarzania danych, zasady gromadzenia, przechowywania, zmiany, wykorzystywania danych, przekazywania

[339] Podobne uregulowania znaleźć można w szwajcarskiej ustawie o ochronie danych osobowych z 19 czerwca 1992 r.

danych za granicę, przekazywania do podmiotów prywatnych i do krajów, w których ustawa nie ma zastosowania, a także prawa podmiotu danych tj. prawo do informacji o przetwarzanych danych, powiadomienia o rozpoczęciu przetwarzania, poprawienia, usunięcia, zablokowania danych, prawo sprzeciwu, wniesienia skargi.

Część trzecia ustawy zawiera zaś przepisy dotyczące przetwarzania danych osobowych przez podmioty prywatne, funkcjonowania organów nadzorczych kontrolujących zgodność przetwarzania z prawem, a także przepisy szczególne dotyczące ograniczonego zakresu przetwarzania danych podlegających tajemnicy zawodowej, przetwarzania danych przez instytuty badawcze, gromadzenia i wykorzystywania danych przez media.

W doktrynie niemieckiej panuje przekonanie, iż właściwa ochrona danych osobowych wymaga także dodatkowych regulacji obejmujących już wąskie i wyspecjalizowane obszary; dlatego też powstało szereg sektorowych[340] aktów prawnych zapewniających daleko idącą ochronę danych osobowych. BDSG uzyskało tym samym charakter subsydiarny, co oznacza, że ochrona danych osobowych przewidziana w ustawie jest zapewniona, gdy brak jest uregulowań szczegółowych. Co więcej, omawiana ustawa nie narusza przepisów o tajemnicy zawodowej (np. tajemnicy lekarza, notariusza, doradcy podatkowego czy tajemnicy bankowej), gdyż przetwarzanie danych osobowych możliwe jest przy jednoczesnym zachowaniu przepisów ustawy, jak i przepisów o tajemnicy[341].

Ostatnim elementem niemieckiego systemu ochrony danych jest ustawodawstwo poszczególnych krajów, będące konsekwencją federalnej struktury państwa. Wszystkie kraje, zarówno stare, jak i nowe[342], mają swoje odrębne ustawy o ochronie danych osobowych. Odpowiadają one uregulowaniom ustawy federalnej, ale nie są z nią identyczne. Istnienie odrębnych ustaw nie pozbawia znaczenia ustawy federalnej, która w wielu sytuacjach znajduje zastosowanie również w poszczególnych landach[343].

W Niemczech istnieje podział kompetencji w zakresie ochrony danych osobowych pomiędzy organem federalnym a organami landowymi. Federalny Komisarz Ochrony Danych

---

[340] Przykładem takich regulacji jest: ustawa z 18 marca 1993 r. o statystyce mieszkaniowej- *Wohnungsstatistikgesetz,* ustawa ramowa Prawo meldunkowe z 16 sierpnia 1980 r. – *Melderechtsrahmengesetz,* ustawa o dowodach osobistych z 21 kwietnia 1986 r. – *Gesetz über Personalausweise*, ustawa z 19 grudnia 1952 r. prao o ruchu drogowym- *Strassenverkehrsgesetz.*

[341] T. Justyński, *op. cit*, s. 76.

[342] Stare kraje (*alte Länder*) to landy RFN sprzed zjednoczenia, nowe kraje (*neue Länder*) to kraje wchodzące od niedawna w skład RFN, tj. od czasu zjednoczenia się Niemiec.

[343] BDSG obejmuje działalność wszystkich instytucji publicznych krajów związkowych, o ile realizują one prawo federalne i nie prowadza działalności gospodarczej opartej na wolnej konkurencji lub działają jako organy ochrony prawnej, o ile nie jest to działalność administracyjna. Poza tym BDSG ma także zastosowanie do wszelkich instytucji niepublicznych, gdyż nie jest to przedmiotem regulacji krajowych. Zob. T. Justyński, *op. cit.*, s. 76.

i Wolności Informacji (niem. *Bundesbeauftragten für Datenschutz*) kontroluje zgodność z federalną ustawą o ochronie danych osobowych oraz innymi przepisami, przetwarzania danych przez federalne podmioty publiczne, w tym również podmioty publiczne i prywatne świadczące usługi telekomunikacyjne i pocztowe. Każdy może wnieść odwołanie do Federalnego Komisarza Ochrony Danych i Wolności Informacji, jeśli tylko uważa, że jego prawa zostały naruszone poprzez gromadzenie, przetwarzanie lub wykorzystanie jego danych osobowych przez organy publiczne Federacji (Roz. II, sekcja 21 federalnej ustawy).

Status prawny Federalnego Komisarza określony został w rozdziale III federalnej ustawy o ochronie danych osobowych. Federalny Komisarz powinien być niezależny w wykonywaniu swoich obowiązków i podlegać tylko prawu. Nadzór nad jego działalnością sprawuje rząd federalny, a hierarchicznie jest on podporządkowany federalnemu ministrowi spraw wewnętrznych (Roz. III, sekcja 22, pkt 4 i 5 ustawy federalnej). Komisarz Federalny nie może zajmować innego płatnego urzędu lub prowadzić działalności zarobkowej lub zawodowej w uzupełnieniu do swoich obowiązków służbowych, nie może także należeć do zarządu, rady nadzorczej lub zarządu przedsiębiorstwa, ani do rząd lub organu prawodawczy Federacji lub landu (Roz. III, sekcja 23 ustawy federalnej). Jedynym wyjątkiem jest możliwość wydawania przez niego odpłatnych opinii w sprawach pozasądowych (Roz. III, sekcja 23, pkt 2 ustawy federalnej).

Głównym zadaniem Federalnego Komisarza Ochrony Danych i Wolności Informacji jest monitorowanie instytucji publicznych Federacji w zakresie zgodności ich działania z przepisami federalnej ustawy oraz innych przepisów dotyczących ochrony danych osobowych. W tym celu przeprowadza on kontrole w zakresie zgodności przetwarzania danych osobowych oraz prawidłowego stosowania federalnej ustawy o ochronie danych osobowych. Instytucje publiczne Federacji są zobowiązane do udzielania pomocy i wspierania Federalnego Komisarza w wykonywaniu ustawowych obowiązków, w szczególności udostępniania stosownej dokumentacji, udzielania koniecznych informacji i odpowiedzi na pytania czy udostępnianie w każdym czasie oficjalnych pomieszczeń. Jeżeli w toku kontroli Federalny Komisarz stwierdzi naruszenie zasad ochrony danych osobowych czy wykryje nieprawidłowości w zakresie przetwarzania danych osobowych przez instytucję Federacji, kieruje wówczas oficjalną skargę do właściwego organu Federacji (Roz. III, sekcja 25 federalnej ustawy).

Federalny Komisarz Ochrony Danych i Wolności Informacji przedkłada co dwa lata do Bundestagu sprawozdanie ze swojej działalności. W sprawozdaniu tym poinformuje Bundestag oraz opinię publiczną o najważniejszych osiągnięciach w dziedzinie ochrony

danych osobowych (Roz. III, sekcja 26 federalnej ustawy). Na wniosek Bundestagu lub rządu federalnego, Komisarz Federalny sporządza także opinie i raporty oraz może wydawać zalecenia w sprawie poprawy ochrony danych do rządu federalnego i do organów Federacji , a także może doradzać im w sprawach dotyczących ochrony danych. Jego zadaniem jest również dążyc do aktywnej współpracy z współpracę z instytucjami publicznymi odpowiedzialnymi za kontrolę przestrzegania przepisów dotyczących ochrony danych w krajach związkowych (Roz. III, sekcja 26 federalnej ustawy).

Rzecznicy Landowi z kolei sprawują nadzór w zakresie prawnej ochrony danych osobowych, w odniesieniu do wszystkich podmiotów landowych, w tym organów władz miejskich i samorządowych. Niektóre organy landów (jak np. Berlin, Brema, Hamburg, Dolna Saksonia i Północna Westfalia) nadzorują dodatkowo przetwarzanie danych osobowych przez podmioty sektora prywatnego.

e) Szwajcaria

Prawna ochrona danych osobowych funkcjonuje w systemie prawnym Szwajcarii od powstania w 1976 r. w Genewie pierwszej ustawy kantonalnej. Kolejne ustawy o ochronie danych osobowych sukcesywnie powstawały w pozostałych kantonach, jednak dopiero 19 lipca 1992 r. uchwalona została obowiązująca na terytorium całego kraju federalna ustawa o ochronie danych (niem. *Bundesgesetz über den Datenschutz*)[344]. Szwajcaria ratyfikowała postanowienia Konwencji nr 108 w 1997 r., co wiązało się z dostosowaniem rozwiązań krajowych do postanowień konwencyjnych. Ten proces udał się na szczeblu federacyjnym, jednak w poszczególnych kantonach nie został w pełni zrealizowany. Pomimo, że Szwajcaria nie należy do struktur Unii Europejskiej, rozwiązania z zakresu ochrony danych w niej wprowadzone w pełni odpowiadają wymogom art. 25 dyrektywy 95/46/WE, zapewniając adekwatny poziom ochrony danych osobowych.

Szwajcarska federalna ustawa o ochronie danych ma zastosowanie do przetwarzania danych osobowych przez organy federalne i podmioty prywatne. W poszczególnych kantonach obowiązują ustawy kantonalne, wzorowane na ustawie federalnej i odnoszące się do przetwarzania danych przez organy kantonów, organy komunalne, a jeśli w danym

[344] W skrócie: DSG; 14 czerwca 1993 r. zostało wydane rozporządzenie wykonawcze do federalnej ustawy o ochronie danych (niem. *Verodrnung zum Bundesgesetz über den Datenschutz* , dalej: VDSG). Zob. P. Fajgielski, *Kontrola…,* s. 125-126.

kantonie brak jest ustawodawstwa w tym zakresie zastosowanie mają przepisy ustawy federalnej (Art. 37 DSG).

Na mocy szwajcarskiej ustawy o ochronie danych osobowych pojęciem „danych osobowych" objęte są nie tylko informacje o osobach fizycznych, ale także i o osobach prawnych (Art. 3b DSG). Odmienne regulacje z zakresu ochrony danych obowiązują względem podmiotów prywatnych i organów publicznych. Zarówno ustawa federalna jak i ustawy kantonalne zawierają przepisy odnoszące się do kontroli przetwarzania i ochrony danych. Kontrolę instytucjonalną na szczeblu federalnym sprawuje Konfederacyjny Rzecznik Ochrony Danych i Jawności Publicznej (niem. *Eidgenössischer Datenschuts- und Öffentlichkeitsbeauftragter*), a w kantonach kantonalni Rzecznicy Ochrony Danych (niem. *kantonalen und kommunalen Datenschutzbeauftragten*). Do kantonalnych organów kontroli stosuje się bezpośrednio przepisy federalne w zakresie kontroli (art. 37 DSG).

Podstawowym zadaniem Konfederacyjnego Rzecznika Ochrony Danych jest sprawowanie nadzoru nad działalnością organów federalnych i podmiotów prywatnych w zakresie przetwarzania danych (z zakresu kontroli wyłączony jest jednak rząd). Rzecznik Konfederacyjny kontroluje przestrzeganie ustawy federalnej i innych przepisów o ochronie danych osobowych. Prowadzi rejestr zbiorów danych, gdyż w Szwajcarii organy federalne i organy prywatne na mocy DSG mają obowiązek zgłaszania zbiorów danych do rejestru. Sprawuje on ponadto poradnictwo w zakresie ochrony danych i wspiera organy kantonalne i komunalne w sprawach związanych z ochroną danych, przedstawia swoje stanowisko odnośnie projektów aktów prawnych dotyczących ochrony danych i wyraża opinię w zakresie zapewnienia odpowiedniego poziomu ochrony. Rzecznik sprawdza także, czy podmioty przekazujące dane osobowe za granicę zapewniają odpowiedni poziom ochrony danych. Szczególne zadania tego organu ochrony odnoszą się do badań medycznych. Rzecznik doradza komisji ds. tajemnicy zawodowej w badaniach medycznych i zapewnia, że pacjenci będą informowani o przysługujących ich prawach.

Dla poprawy ochrony danych osobowych i właściwego zabezpieczenia danych na mocy art. 11 ustawy federacyjnej przewidziana jest w Szwajcarii procedura certyfikacyjna (niem. *Zertifizierungsverfahren*). Przedmiotem certyfikacji jest ocena systemów, procedur postępowania i organizacji w zakresie przetwarzania danych, a proces ten dotyczy zarówno producentów sprzętu i oprogramowania służącego do przetwarzania danych osobowych, jak również i podmiotów i organów przetwarzających dane[345]. Kontrolę w zakresie właściwego i

[345] P. Fajgielski, *Kontrola…,* s. 136.

legalnego certyfikowania przeprowadza Rzecznik Ochrony Danych, który ma uprawnienia do wydawania zaleceń w tym zakresie.

f) Francja

Francuski system ochrony danych osobowych opiera się na uchwalonej 6 stycznia 1978 r. ustawie o Bezpieczeństwie IT i Wolności nr 78-17 (fr. *Loi Informatique et Libértes Act N° 78-17*; zwanej DPA)[346]. Ustawa ta była wielokrotnie nowelizowana, przy czym najistotniejszą nowelizację wprowadzono 6 sierpnia 2004 r., tak by francuskie ustawodawstwo w zakresie ochrony danych osobowych i prywatności zgodne było z wymogami dyrektywy 95/46/WE.

Na mocy francuskiego DPA dane osobowe są zdefiniowane standardowo jako wszelkie informacje dotyczące osoby fizycznej, która jest lub może być zidentyfikowana bezpośrednio lub pośrednio, przez powołanie się na numer identyfikacyjny albo jeden lub więcej czynników specyficznych dla nich (art. 2 DPA). Pojęcie to jest bardzo szerokie, stąd już gromadzenie wszelkich danych, dzięki którym można zidentyfikować osobę, bezpośrednio lub pośrednio (np. imię i nazwisko, data urodzenia, numer telefonu, adres *e-mail*), musi być zgodne z zasadami DPA. Przepisy DPA odnoszą się tylko do informacji o osobach fizycznych, nie zapewniając ochrony osobom prawnym i mogą mieć zastosowanie do każdej osoby działającej wedle prawa francuskiego jako jednoosobowa firma lub jako członek partnerstwa.

Przetwarzanie na mocy art. 2 DPA jest zdefiniowane jako działania lub całość operacji w związku z tymi danymi, niezależnie od zastosowanego mechanizmu. W szczególności jest to: uzyskanie, nagranie, organizacja, zatrzymywanie, wyszukiwanie, modyfikacja, konsultacja, ujawnienie poprzez transmisję, układanie lub kompilowanie, usuniecie lub zniszczenie danych. Dane osobowe mogą być zatem przetwarzane, gdy podstawowe warunki przetwarzania danych osobowych są spełnione. Wyjątki zawarte w ustawie dotyczą przetwarzania danych osobowych przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze oraz w odniesieniu do działalności na rzecz bezpieczeństwa publicznego, obronności lub bezpieczeństwa państwa. DPA dotyczy także automatycznego przetwarzania danych osobowych, jak i nieautomatycznego przetwarzania danych osobowych, które są lub mogą być zawarte w zbiorze danych osobowych. Nie

[346] Zob. http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

traktuje jednak np. informacji na temat przestępstw, wyroków lub środków bezpieczeństwa jako wrażliwych danych osobowych, ale przewiduje bardzo ścisłą kontrolę nad ich przetwarzaniem wymagając uprzedniego zezwolenia do ich przetwarzania.

Francuskim krajowym organem regulacyjny w zakresie ochrony danych osobowych i prywatności jest Francuski Urząd Ochrony Danych *(fr. Komisja Nationale de l'Informatique et des* Libertés; dalej: CNIL). CNIL jest niezależnym organem administracji, który ma gwarantować, iż przetwarzanie danych osobowych odbywać się ma zgodnie z postanowieniami DPA oraz który jest odpowiedzialny za zapewnienie, że stosowane technologie informatyczne nie zagrażają ludzkiej tożsamości i nie naruszają praw człowieka, prywatności lub indywidualnych lub publicznych wolności. DPA określa zasady funkcjonowania CNIL oraz jego główne zadania w art. 11-21.

CNIL jest organem kolegialny, składającym się z siedemnastu członków. Dla respektowanie przestrzegania zasad zawartych w DPA w zakresie ochrony danych osobowych CNIL może korzystać z szerokiego wachlarzu kar, w tym stosować ostrzeżenie, formalne żądanie, wydawać nakaz zaprzestania przetwarzania, nakładać kary finansowe w wysokości do 150.000 euro dla pierwszego naruszenia (i do 300.000 EUR w przypadku powtórnego naruszenia w ciągu pięciu lat) oraz cofać wydane wcześniej przez siebie zezwolenia. W nagłych przypadkach, np. naruszenia praw człowieka, prawa do prywatności i wolności jednostki, CNIL może zdecydować nakazanie zaprzestania przetwarzania danych maksymalnie przez okres trzech miesięcy lub informowania premiera aby podjąć odpowiednie środki bezpieczeństwa. Sankcje karne mogą zostać nałożone także jako pozbawienia wolności do maksymalnie pięciu lat i kara grzywny do 300.000 euro (i do 1,5 milionów EUR dla osób prawnych przetwarzających niezgodnie z DPA dane osobowe osób fizycznych).

CNIL we Francji ma także prawo do podejmowania działań egzekucyjnych i wydawania sankcji finansowych (kary administracyjne). Sankcje CNIL mogą być podane do publicznej wiadomości (zwykle na swojej stronie internetowej) i publikowane w gazetach kosztem administratora danych, który dopuścił się zarzucanych naruszeń.

g) Szwecja

Szwecja jest państwem z bogatymi doświadczeniami w zakresie ochrony danych osobowych, a nagromadzenie danych przetwarzanych elektronicznie w porównaniu do liczby

mieszkańców jest największe[347]. To właśnie Szwecja jako jeden z pierwszych krajów podjął się wprowadzenia kompleksowej regulacji ochrony danych osobowych na poziomie ustawy (1973 r.) i nadal jest w czołówce państw tworzących podstawy prawne dla bezpieczeństwa danych i dostosowujących regulacje do rozwijających się potrzeb społeczeństwa[348]. W systemie szwedzkiego prawa dość szybko wprowadzono odrębny system ochrony prywatności, poza istniejącymi gwarancjami na gruncie prawa cywilnego, co zaowocowało właśnie już w latach 70. XX w. powstaniem odrębnej ustawy. W kolejnych latach sukcesywnie wprowadzano zmiany i udoskonalano regulacje z zakresu ochrony danych z uwagi na rozwój technologii, a także wzrost świadomości i potrzeby samego społeczeństwa. Szwedzki system ochrony danych jednostki zdaje się być naturalnie ewaluującym systemem, a nie pospiesznie i sztucznie utworzoną legislacją wymuszoną procedurami i naciskami unijnymi. Także postawa szwedzkiego społeczeństwa, które jest społeczeństwem świadomym i widzi potencjalne zagrożenie ze strony nowoczesnych technologii i narzędzi szybszego przetwarzania danych, jest czynnikiem mającym duży wpływ na jakość i funkcjonowanie szwedzkiego systemu ochrony danych osobowych, z czego należałoby czerpać wzór.

Pierwsza prawna regulacja odnosząca się do ochrony danych osobowych, zawarta w ustawie o danych z 1973 r., powstała w celu należytej ochrony prywatności osobistej oraz uregulowania właściwego korzystania ze zbiorów danych osobowych[349]. Ustawa zdefiniowała pojęcie zbioru danych osobowych w szeroki sposób, określając także, że za dane osobowe uznaje się każdą informację dotyczącą osoby fizycznej, niezależnie od wymienienia tej osoby z imienia i nazwiska. Dane osobowe mogły być przetwarzane jedynie przez osobę, która wcześniej wystąpiła i otrzymała od Urzędu Ochrony Danych stosowną licencję[350].

Istotne postanowienia w zakresie ochrony danych osobowych zawiera również Konstytucja Szwecji składająca się z kilku aktów normatywnych. Na szczególna uwagę zasługuje art. 2 Aktu o Formie Rządu z 28 lutego 1974 r., zapewniający ochronę prywatności jednostki[351]. W rozdziale II pt: „Podstawowe prawa i wolności", art. 1 odnosi się do praw przysługujących obywatelowi w stosunku do społeczeństwa i wśród nich znajduje się wolność wypowiedzi i informacji. Nie są to prawa absolutne, gdyż mogą ulec ograniczeniu, niemniej

---

[347] Zob. S. Sagan, *Szwedzkie doświadczenia w zakresie gromadzenia i wykorzystywania danych osobowych*, [w:] *Prawa jednostki w społeczeństwie informacyjnym*. *Materiały Ogólnopolskiej Konferencji Naukowej*, red. M. Grzybowski, Rzeszów 1999, s. 99.

[348] Zob. M. Grzybowski, *Systemy konstytucyjne państw skandynawskich*, Warszawa 1998, s. 125.

[349] K. Szwed, *Ewolucja ochrony danych osobowych na przykładzie Polski i Szwecji*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego. Seria prawnicza", Zeszyt 71/2011, Prawo 10, s. 199.

[350] Art. 1 ustawy o danych (*The Data act*, 1973). Tłumaczenie z języka szwedzkiego na angielski dostępne na stronie: http://archive.bild.net/dataprSw.htm.

[351] *Konstytucja Szwecji*, tłum. M. Grzybowski, K. Dembiński, Warszawa 1991.

przy określaniu ich granic powinno się uwzględniać zachowanie szerokiej wolności wypowiedzi i informacji o zagadnieniach politycznych, religijnych, zawodowych, naukowych i kulturalnych[352].

Istotną gwarancją przestrzegania prawa w zakresie praw jednostki jest otwartość dostępu do dokumentów publicznych. W 1766 r. w Szwecji wprowadzono Akt o Wolności Druku zapewniający obywatelowi wolność druku, powtórzoną analogicznie w aktach z 1810 r. i 1949 r.[353]. Akt o Wolności Wypowiedzi natomiast zapewniał wolność wypowiedzi, wyrażoną za pomocą różnych mediów czy form przekazu.

Art. 3 rozdziału II Aktu o Formie Rządu wprost stanowi o ochronie każdego obywatela przed naruszeniem integralności osobistej w związku z automatycznym przetwarzaniem danych osobowych[354]. Na mocy art. 6 zapewnia się każdemu obywatelowi nietykalność osobistą, gwarantuje się ochronę przed przeszukaniem mieszkania lub podobnym wtargnięciom oraz przed naruszeniem tajemnicy korespondencji, tajnymi podsłuchami czy rejestrowaniem rozmów telefonicznych lub innych poufnych wiadomości[355].

Gwarancje prawne związane z ochroną jednostki zawarte w szwedzkiej Konstytucji wyznaczają jedynie ogólne zasady, zaś szczegółowe regulacje zawarte są w stosownych ustawach. Na dalszą ewolucję prawnej ochrony danych osobowych w Szwecji niewątpliwie miało wpływ utworzenie oraz obowiązywanie dyrektywy 95/46/WE. Stworzenie jednolitego aktu europejskiego, który deklarował powstanie wspólnego rynku, gwarantującego swobodny przepływ towarów, usług i kapitału, poniosło za sobą także stworzenie wolnego przepływu danych między państwami Unii Europejskiej. Dyrektywa nakazywała ujednolicenie regulacji prawnych w zakresie ochrony danych, co nastąpiło w Szwecji, lecz dopiero w 1998 r. wraz z wydaniem ustawy o danych osobowych, która zastąpiła obowiązującą dotąd ustawę z 1973 r.

Ustawa o danych z 1973 r. obowiązywała do października 2001 r. w odniesieniu do przetwarzania danych osobowych zapoczątkowanych przed dniem 24 października 1998 r., tj.

---

[352] Ograniczenia te mają na względzie bezpieczeństwo Królestwa, zaopatrzenie ludności, porządek publiczny i bezpieczeństwo, godność osobistą, życie prywatne lub zapobieganie i ściganie przestępstw, a także znajdują zastosowanie w odniesieniu do działalności gospodarczej. W innych przypadkach - jedynie z ważnych powodów. Zob. *Konstytucja Szwecji*, tłum. M. Grzybowski, K. Dembiński, Warszawa 1991.

[353] Akt prawny gwarantujący dostęp do dokumentów publicznych i wolność druku został przyjęty w Finlandii w 1951 r. , w Norwegii w 1968 r., a w Danii częściowe rozwiązanie w tym zakresie wprowadziła ustawa z 1964 r. W latach 70. XX w. akty te zostały ściślej sprecyzowane, jednak nadal utrzymuje się różnica między Szwecją i Finlandią, gdzie dostęp do dokumentacji publicznej jest szeroki, a Norwegią i Danią, gdzie należy wskazać rodzaje dokumentów, z którymi osoba chce się zapoznać i gdzie swobodny dostęp nie obejmuje dokumentów o charakterze roboczym.

[354] Ten sam artykuł zakazuje np. umieszczania danych obywatela, bez jego zgody, w jakimkolwiek spisie publicznym, jedynie na podstawie jego sympatii politycznych.

[355] *Konstytucja Szwecji*, tłum. M. Grzybowski, K. Dembiński, Warszawa 1991.

dniem wejścia w życie nowej ustawy o danych osobowych. Konieczne stało się z uwagi na międzynarodową współpracę gospodarczą i naukową uregulowanie w ustawie kwestii transgranicznego obrotu danymi. W 1999 r. zmieniono zatem treść art. 33 ustawy o danych osobowych w aspekcie wytycznych unijnej dyrektywy odnoszących się do przekazywania danych osobowych do państw trzecich. Zmiana ta weszła w życie styczniu 2000 r. i wedle opinii Urzędu Inspekcji Danych miała przyczynić się do ułatwienia przepływu danych przez międzynarodowe sieci łączności, takie jak Internet[356].

Szwedzka ustawa o danych osobowych definiuje dane osobowe jako informacje odnoszące się do osób fizycznych w sposób bezpośredni lub pośredni, zapewniając ochronę danych tylko osobie fizycznej żyjącej[357]. Ustawa odnosi się zarówno do przetwarzania danych automatycznie, ale w przeciwieństwie do poprzedniej ustawy z 1973 r. zapewnia także ochronę w przypadku przetwarzania danych w zbiorach tradycyjnych, tj. manualnych. Najważniejszymi założeniami ustawy jest zabezpieczenie naruszenia integralności osobistej w wyniku przetwarzania danych. Przesłanką warunkująca możliwość legalnego przetwarzania danych jednostki jest korzystanie z danych jedynie ze względu na konkretny, wyraźnie określony i uzasadniony cel, a osoba, która jest dysponentem danych, musi wyrazić na to zgodę[358]. Zakazane jest jednak wykorzystywanie danych ujawniających poglądy polityczne, przekonania religijne czy stan zdrowia; a takie dane zawarte w zbiorze udostępniać można tylko podmiotom uprawnionym do ich przetwarzania. Co więcej, szwedzka ustawa nie jest właściwa dla działalności dziennikarskiej, artystycznej i literackiej, gdyż w tym przypadku należy odwoływać się do stosownych przepisów konstytucyjnych.

Specyfiką szwedzkiej ustawy o danych osobowych jest szczególne wyeksponowanie ich zależności w stosunku do prawa do wolności słowa. Ich zastosowanie jest moderowane w zależności od stopnia, w jakim mogłoby naruszać konstytucyjne zasady dotyczące wolności prasy i słowa czy też ograniczać zasadę dostępności do informacji publicznych[359]. W Szwecji każdy jest uprawniony do wglądu w dokumenty publiczne, stąd nie bez przyczyny mówi się, iż „zasada jawności" jest rozumiana wprost[360].

---

[356] K. Szwed, *op. cit., s. 202.*
[357] Zob. *Personal Data Protection. Information on the Personal Data Act*, Brochure Swedish Ministry Of Justice, s. 7.
[358] Od tej zasady przewidziano wyjątki, m. in jeżeli jest to konieczne z uwagi na wykonywanie władzy przez organy publiczne oraz celem umożliwienia inspektorowi wykonywania czynności przypisanych prawem. Zob. art. 1 szwedzkiej ustawy o danych osobowych. Tekst ustawy w tłumaczeniu na język angielski dostępny jest na stronie: http://www.sweden.gov.se.
[359] K. Szwed, *op. cit,* s. 204.
[360] S. Sagan, *Szwedzkie…,* s. 101.

Zgodnie z treścią pkt 62 preambuły do Dyrektywy 95/46/WE państwa członkowskie Unii Europejskiej, w tym i Szwecja, zobowiązane zostały do utworzenia niezależnego organu do spraw ochrony danych osobowych, a mającego służyć miało zapewnieniu jak najwłaściwszej ochrony praw jednostki. Szwedzki Urząd Inspekcji Danych Osobowych (*Data inspektionen* lub DIB) powstał już w latach 70. XX w jako odpowiedź na społeczne zapotrzebowanie ochrony przed możliwym zagrożeniem, z jakim utożsamiano postępującą komputeryzację i rozwój technologii prowadzących do ograniczenia prywatności. Ustawa z 1998 r. nie wymienia wprost nazwy tego organu, a posługuje się jedynie ogólnym terminem - organ kontroli. Na mocy art. 3 niniejszej ustawy organ ten został zdefiniowany jako organ powołany przez rząd do sprawowania kontroli. Jest to organ kolegialny działający w postaci niezależnych komisji. Zadania postawione mu przez rząd sprowadzają się w głównej mierze do stworzenie odpowiednich warunków przetwarzania danych osobowych, w taki sposób, by uniknąć sytuacji nieuzasadnionego naruszenia prywatności jednostki; jego zadaniem jest również stanie na straży zgodności i spójności legislacji w zakresie ochrony danych osobowych[361]. Pod względem organizacyjnym obecnie Urząd Inspekcji Danych Osobowych dzieli się na cztery jednostki: Biuro Generalnego Dyrektora, które jest odpowiedzialne za sprawy administracyjne, komisję nadzorczą, zajmującą się kontrolą i skargami, komisję informacyjną, do której zadań należy zarządzanie oficjalną stroną internetową Urzędu, publikacjami, wykładami i seminariami, oraz komisję prawną odpowiedzialną za działania nadzorujące Urzędu, wydawanie opinii na temat propozycji legislacyjnych z zakresu ochrony danych osobowych oraz koordynowanie współpracy na szczeblu międzynarodowym[362]. Zniesiona została komisja finansowa, a jej zadania zostały rozdzielone pomiędzy pozostałe jednostki Urzędu[363].

Zadania Urzędu dotyczą także monitorowania bezpieczeństwa przetwarzania danych w innych aktach prawnych odnoszących się do ochrony danych. Poza ustawą o danych osobowych w systemie szwedzkiego prawa istnieje wiele innych aktów, które sektorowo odnoszą się do zagadnień przetwarzania danych, chociażby ustawa o informacjach kredytowych czy ustawa o odzyskiwaniu długów. Związane jest to ze specyfiką szwedzkich regulacji w określonych materiach, jednak niewątpliwie wiąże się z procesem przetwarzania

---

[361] *Ibidem*, s. 205.
[362] *Ibidem*, s. 205.
[363] W 2003 r. w skład Urzędu wchodziło 40 pracowników, głównie z wykształceniem prawniczym, oraz trzech specjalistów ds. technologii informacyjnych. W 2002 r. całkowita liczba złożonych do Urzędu skarg wynosiła 406, z czego większość dotyczyła bezprawnego publikowania danych osobowych w Internecie czy wykorzystywania danych konsumentów w calach marketingowych- Dane za: *Privacy and Human Rights* 2003: Sweden, dostępne na stronie internetowej:http://www.privacyinternational.org/survey/phr2003/countries/sweden

danych osobowych obywateli w różnych celach, czy to gospodarczych czy handlowych oraz z naruszaniem prywatności jednostki[364].

Urząd Ochrony Danych Osobowych pełni także rolę doradczą (jednak nie decyzyjną) w zakresie przygotowywania przez rząd projektów ustaw, monitorując czy prywatność jednostek jest chroniona w najwłaściwszy sposób.

Prezentując wybrane zagadnienia dotyczące ochrony prywatności w kontekście ochrony danych osobowych, warto także zwrócić uwagę na jeszcze kilka zagranicznych regulacji.

[364] W Szwecji organizacje zajmujące się badaniem zdolności kredytowej mają prawo zbierać informacje dotyczące sytuacji finansowej przedsiębiorstw oraz sytuacji osobistej i materialnej osób fizycznych. W Szwecji każda osoba powyżej 15 roku życia znajduje się w rejestrach takich organizacji. Organizacje te dla swojego działania wymagają zgody Urzędu, który przeprowadza tez inspekcje mające na celu sprawdzenie prawidłowego zbierania tych informacji. Szczegółowe dane dotyczące jednostki mogą zostać przekazane osobie trzeciej tylko w uzasadnionych przypadkach, np. badania zdolności kredytowej, niemniej jednak za każdym razem dana osoba musi otrzymać kopie zebranych informacji. Procedury związane z odzyskiwaniem długów także wymagają dla swego działania pozwolenia Urzędu. Zob. K. Szwed, *op. cit.,* s. 205.

ROZDZIAŁ III
OCHRONA DANYCH OSOBOWYCH W POLSKIM PORZĄDKU PRAWNYM

1. Kształtowanie się prawa do prywatności w prawie polskim

Prawo do prywatności, w tym także w aspekcie ochrony informacji o osobach, nie było przez długi czas kompleksowo uregulowane w polskim systemie prawnym, ani na poziomie konstytucji, ani na poziomie ustaw zwykłych. Do czasu uchwalenia Konstytucji RP w 1997 r. żadna z wcześniejszych ustaw zasadniczych nie zawierała postanowień odnoszących się do prawa do prywatności. Takie podejście ustrojodawców mogło wynikać z tego, że nie dostrzegano wówczas konieczności jej ochrony z uwagi na brak szczególnych zagrożeń, a prawo to nie było także proklamowane w konstytucjach państw obcych. Ani Konstytucja marcowa[365], ani Konstytucja kwietniowa[366] do chwili uchwalenia Konstytucji RP z 2 kwietnia 1997 r. nie zawierała postanowień, które dotyczyłyby prawa do prywatności człowieka. Jedynie w Konstytucji PRL z 1952 r.[367] zostały zawarte postanowienia, które korelowały z ochroną prywatności człowieka, lecz regulacje te nie miały większego znaczenia w praktyce[368]. Z uwagi na założenia aksjologiczne przyświecające ustrojodawcy, sugestie W. Sokolewicza, który dowodził, jakoby z całego szeregu przepisów konstytucyjnych wynikało, iż Konstytucja zawierała gwarancje swobodnego rozwoju osobowości, choć uzasadnione, nie spotkały się z szerszą akceptacją doktryny i judykatury[369].

Uchwalony w 1964 r. kodeks cywilny[370] także nie zawiera żadnych uregulowań, które wprost definiowałyby prywatność. Jak zostało ugruntowane w literaturze i w orzecznictwie, podstawę dla ogólnie sformułowanej ochrony sfery życia prywatnego stanowi tylko art. 23 k.c.[371]. Jest to unormowanie o charakterze klauzuli generalnej, gdyż treść art. 23 k.c. deklaruje zasadę cywilnoprawnej ochrony dóbr osobistych, nie wyznaczając jednak jej zakresu, ani

---

[365] Ustawa z dnia 17 marca 1921 r. (Dz. U. Nr 44, poz. 267).
[366] Ustawa z dnia 23 kwietnia 1935 r. (Dz. U. Nr 30, poz. 227).
[367] Ustawa z dnia 22 lipca 1952 r. (Dz. U. Nr 33, poz. 232).
[368] Art. 82 proklamował wolność sumienia, a w art. 87 ust. 2 zagwarantowano nienaruszalność mieszkania i tajemnicę korespondencji.
[369] W. Sokolewicz*, Le droit de „privacy" et ses limitations*, [w:] *Rapports Polonais, presentés au IX Congrès International de Droit Comparé*, Warszawa-Wrocław 1974, s. 307. Cyt. za: J. Braciak, *Prawo do prywatności*, s. 125.
[370] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93).
[371] M. Safjan, *Prawo do ochrony życia prywatnego*, [w:] *Szkoła Praw Człowieka. Teksty wykładów*, Warszawa 1996, s. 211-222; A. Szpunar, *O ochronie sfery życia prywatnego,* „Nowe Prawo" 1982, nr 3-4, s. 25.

wśród wymienionych dóbr nie zawierając prawa do prywatności[372]. Wyliczenie zawarte w art. 23 k.c. nie jest wyczerpujące. „Zapatrywanie, iż wyliczenie dóbr osobistych w art. 23 dokonane zostało *exempli modo* jest powszechne i nie było przez nikogo kwestionowane”[373]. W literaturze zgodny jest pogląd, iż katalog dóbr osobistych zawarty w art. 23 k.c. nie jest zamknięty, a lista dóbr osobistych stale się poszerza pod wpływem dokonań doktryny i judykatury. Potrzeba ochrony coraz to nowych sfer życia ludzkiego przez zaliczenie ich do katalogu dóbr osobistych staje się koniecznością, gdyż wciąż pojawiają się nowe sytuacje, w których te prawa mogą być i są naruszane[374].

Przed uchwaleniem obowiązującej Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. ochrona prywatności zagwarantowana była tylko fragmentarycznie na gruncie nielicznych regulacji ustawowych. Pomimo niesprzyjających okoliczności systemowych, które nastawione były na krępowanie swobody jednostki, a nie ochronę jej pozycji, pierwsza normatywna wzmianka dotycząca cywilnoprawnej ochrony prywatności pochodziła z 1984 r. Na podstawie art. 14 ust. 6 prawa prasowego[375] wprowadzono w Polsce zakaz publikowania informacji oraz danych dotyczących prywatnej sfery życia bez zgody osoby zainteresowanej, chyba że wymagałaby tego obrona społecznie uzasadnionego interesu lub wiązałoby się to bezpośrednio z publiczną działalnością danej osoby[376].

Tylko w polskim orzecznictwie sfera życia prywatnego zyskała trwałe miejsce jako wyodrębnione dobro osobiste. Przełomowe okazało się orzeczenie Sądu Najwyższego z 18 stycznia 1984 r., w którym SN stwierdził, iż „otwarty katalog dóbr osobistych pozwala na włączenie do ich zakresu dóbr, które spełniają wszystkie wymagania odnoszące się do pojęcia dobra osobistego według obowiązującego prawa, które są związane ze sferą życia prywatnego, rodzinnego, ze sferą intymności. Ochrona w tym zakresie może się odnosić do wypadków ujawniania faktów z życia osobistego i rodzinnego, nadużywania uzyskanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać. Z tego bynajmniej nie wynika, że ochrona ustalona w formach prawnych panującego porządku prawnego nie może w niektórych przypadkach uzasadniać wkraczania w pewne sfery życia prywatnego, sfery jego intymności przez uprawnione podmioty. Niemniej jednak ogólnie można stwierdzić, że prawidłowe

---

[372] B. Kordasiewicz, *op. cit.*, s. 22-23.
[373] *Ibidem*, s. 23.
[374] Zob. J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie…,* s. 336.
[375] Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24).
[376] Art. 49 ustawy przewidywał sankcje grzywny za naruszenie jej przepisów, a art. 40 gwarantował zadośćuczynienie pieniężne za krzywdę doznana w razie umyślnego naruszenia dóbr osobistych przez publikację materiałów prasowych.

relacje miedzy interesem ogólnym a interesem jednostki w sferze dóbr osobistych jednostki nie mogą być naruszone w sposób krzywdzący jednostkę ludzką w jej własnym odczuciu i w odczuciu społecznym środowiska, w którym człowiek żyje"[377]. Orzeczenie to otworzyło drogę do domagania się ochrony prywatności człowieka, a stanowisko SN w połączeniu z przyjętą przez ustawodawcę konstrukcją art. 24 k.c. (ochrona dóbr osobistych) umożliwiło pokrzywdzonym stosunkowo łatwe dochodzenie roszczeń z tytułu naruszenia prywatności[378].

Zasadnicza zmiana w zakresie rozumienia prawa do prywatności nastąpiła dopiero wraz z transformacją ustrojową. W 1990 r. dokonano nowelizacji wspomnianego art. 14 ust. 6 prawa prasowego poprzez skreślenie z treści artykułu słów zezwalających na publikację danych dotyczących prywatnej sfery życia, jeśli przemawia za tym obrona społecznie uzasadnionego interesu[379]. W 1991 r. Polska przystąpiła do Rady Europy i tego samego dnia podpisała Europejską Konwencję Praw Człowieka, co było politycznym wymogiem uzyskania członkostwa w Radzie. 19 stycznia 1993 r. Konwencja została ratyfikowana i weszła w życie w stosunku do Polski. Decyzja ta w oczywisty sposób zmieniła konieczność podejścia do sfery prywatności, gdyż wiązała się z akceptacją postanowień Europejskiej Konwencji oraz poddaniem polskiej judykatury kontroli Europejskiego Trybunału Praw Człowieka, co było jednoznaczne z przyjęciem dorobku ETPCz w zakresie ochrony życia prywatnego i rodzinnego.

Zanim obecnie obowiązująca Konstytucja RP z 1997 r. *expressis verbis* uznała prawo każdego człowieka do poszanowania jego sfery życia prywatnego, potrzeba jego ochrony została dostrzeżona w orzecznictwie Trybunału Konstytucyjnego. Fundamentalna zmiana w postrzeganiu prawa do prywatności nastąpiła wraz z wydaniem przez Trybunał Konstytucyjny orzeczenia z 24 czerwca 1997 r. [380]. Prawo do prywatności, które nie było wprost określone na gruncie Konstytucji PRL, zostało wydobyte przez TK z ogólnych zasad konstytucyjnych, w szczególności w wyniku powiązania zasady demokratycznego państwa prawnego z ochroną tajemnicy korespondencji (art. 87 ust. 2 poprzednio obowiązującej Konstytucji PRL). TK, uznając argumentację Rzecznika Praw Obywatelskich, przyznał prawu do prywatności *de lege lata* rangę konstytucyjną. Jak wskazał Trybunał, uznanie prawa do prywatności przez

---

[377] Orzeczenie SN z dnia 18 stycznia 1984 r., I CR 400/83-OSN 11/84, nr 195.
[378] Z. Radwański, *Prawo cywilne-część ogólna,* Warszawa 1997, s. 150-151.
[379] Nowelizacja ta miała jedynie charakter techniczny, a to z tego powodu, że doktryna i judykatura, ukształtowane na tle podstawowych dla ochrony dóbr osobistych art. 23 i art. 24 k.c., od dawna i to powszechnie przyjmowały, iż do przesłanek wyłączających bezprawny charakter naruszenia dóbr osobistych należą: działanie w ramach porządku prawnego lub w wykonaniu prawa podmiotowego za zgodą uprawnionego lub w obronie zasługującego na obronę interesu. Zob. B. Kordasiewicz, *op. cit*., s. 25, 30 i n.
[380] Orzeczenie TK z dnia 24 czerwca 1997 r., K 21/96, OTK ZU 2 (11)1997, poz. 23.

międzynarodowe regulacje dotyczące praw człowieka i powiązanie – przez orzecznictwo europejskie – tego prawa z ogólną zasadą rządów prawa pozwala przyjąć, że uznanie i zapewnienie należytej ochrony prawu do prywatności jest koniecznym elementem demokratycznego państwa prawa. W konsekwencji dało to podstawę do sformułowania konstytucyjnego prawa do prywatności rozumianego jako m in. prawo do zachowania w tajemnicy informacji o swoim życiu prywatnym[381]. Na gruncie wskazanego orzeczenia TK, możliwe było także wyprowadzenie innych praw, jak np. prawa jednostki do sądu[382], prawa do godności[383] czy prawa do życia[384]. W omawianym wyroku TK odnotował też fakt, że istnienie prawa do prywatności w polskim porządku prawnym znalazło już potwierdzenie w orzecznictwie Sądu Najwyższego[385].

2. Ochrona prywatności i ochrona danych osobowych na gruncie Konstytucji RP z dnia 2 kwietnia 1997 r.

Zwieńczeniem procesu implementacji prawa do prywatności do polskiego porządku prawnego było ujęcie prawa do prywatności w Konstytucji RP z dnia 2 kwietnia 1997 r. Polska ustawa zasadnicza formułuje podmiotowe prawo do ochrony życia prywatnego w art. 47. Artykuł ten stanowi swoiste *lex generalis* dla pozostałych norm konstytucyjnych dotyczących prywatności, które zawarte są m. in. w art. 49 (ochrona tajemnicy komunikowania), w art. 50 (gwarancja nienaruszalności mieszkania), w art. 51 (prawo do ochrony danych osobowych) czy w art. 53 ust. 7 (wyłączenie możliwość zobowiązania obywatela przez organy władzy publicznej do ujawniania swojego światopoglądu, przekonań religijnych lub wyznania) Konstytucji; stanowią one dopełnienie norm z art. 47. Ochrona prywatności jest także jedną z przesłanek wyłączenia jawności rozprawy z art. 45 ust. 2 Konstytucji i jednym z podstawowych składników ochrony konsumentów gwarantowanej przez organy władzy publicznej (art. 76).

---

[381] J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie…,* s. 347.
[382] Orzeczenie TK z dnia 7 stycznia 1992 r., K 8/91, OTK w 1992 r., cz. I, s. 76 i n.
[383] Uchwała z dnia 17 marca 1993 r., W 16/92, OTK w 1993 r., cz. I, s. 165.
[384] Orzeczenie z dnia 27 maja 1997 r., K 26/96, OTK ZU Nr 2/1997.
[385] Sąd Najwyższy stwierdził w wyroku z 18 stycznia 1984 r., iż „otwarty katalog dóbr osobistych (art. 23 i art. 24 k.c.) obejmuje także dobra osobiste związane ze sferą życia prywatnego, rodzinnego, ze strefą intymności. Ochrona w tym zakresie może odnosić się do wypadków ujawnienia faktów z życia osobistego i rodzinnego, nadużywania uzyskanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać". Zob. wyrok TK z dnia 28 września 2008 r., SK 52/05, Z.U. 125/7/A/2007.

Prawo do prywatności zostało zaliczone do kategorii praw niederogowalnych, co oznacza, że nie może ono podlegać żadnym ograniczeniom w stanie wojennym i stanie wyjątkowym (art. 233 ust. 1 Konstytucji RP). Wzmacnia to jego charakter i rangę pośród innych praw[386]. Wyraźne zagwarantowanie tego prawa, niezależnie od postanowień zawartych w art. 51 Konstytucji, pełni doniosłą funkcję i oznacza, że życie prywatne zasadniczo podlega ochronie; tylko wyjątkowo, na podstawie Konstytucji lub ustaw, można tę ochronę uchylić[387].

Zgodnie z treścią art. 47 Konstytucji każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowaniu o swoim życiu osobistym. W artykule tym zostało uregulowane prawo jednostki do prawnej ochrony jej sfer życia, a także przyznano jej prawo do decydowania o swojej „wolności osobistej" poprzez wykluczenie wszelkiej postronnej ingerencji w sferę życia osobistego jednostki[388]. Prawo do prywatności w tym kontekście oznacza, iż państwo zobowiązuje się z jednej strony do nieingerencji w konstytucyjnie określony zakres życia jednostek, a z drugiej strony zapewnia stosowną ochronę w przypadku, gdy działania takie zostały już podjęte[389]. Z użytej w art. 47 stylizacji wynika, iż prawo to dotyczy wszystkich osób fizycznych, w tym przebywających w Polsce, niezależnie od posiadanego obywatelstwa, gdyż tylko ludzie są zdolni do posiadania życia rodzinnego, prywatnego, czci i dobrego imienia. Nie ma zatem żadnej różnicy pomiędzy obywatelem państwa polskiego, cudzoziemcem czy bezpaństwowcem [390].

Według art. 47 Konstytucji na całokształt prawa do prywatności składają się trzy elementy precyzujące owe prawo: „życie prywatne", „życie rodzinne" oraz „życie osobiste"[391]. Pojęcia te powinny być rozumiane zgodnie ze standardami funkcjonującymi w tym kręgu cywilizacyjnym, w którym żyje społeczeństwo polskie. Jak słusznie wskazuje B. Banaszak, „zakładając racjonalność działania ustrojodawcy, należy przyjąć, że świadom tego, co łączy poszczególne użyte w art. 47 terminy, nie pragnął nadać ich wyróżnieniu cech rozłącznych, a zaakcentowawszy różnice między nimi, podkreślił, że można je traktować jako elementy samoistne. Uczynił to, aby tym pełniej objąć ochroną to, co rozumie pod pojęciem prywatności"[392].

---

[387] J. Boć, *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, Wrocław 1998, s. 94.
[388] P. Sarnecki, *Art. 47*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom III, red. L. Garlicki, Warszawa 2003, s. 1.
[389] J. Boć, *Konstytucje…,* s. 94.
[390] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, s. 245.
[391] Zob. J. Sieńczyło-Chlabicz, *op. cit.*, s. 110.
[392] B. Banaszak, *Konstytucja…*, s. 245-246.

Pojęcie życia prywatnego rozumieć można chyba najtrafniej przeciwstawiając je życiu publicznemu[393]. Życie prywatne to przymioty, wewnętrzne przeżycia osobiste (jednostkowe) człowieka i ich oceny, refleksje dotyczące wydarzeń zewnętrznych i jego wrażenia zmysłowe, także stan zdrowia[394] oraz sytuacja majątkowa[395]. Nie są one w założeniu przeznaczone do upowszechniania i sam zainteresowany decyduje o kręgu osób, z którymi zechce się nimi podzielić. Tak rozumiane życie prywatne odnosi się do życia osobistego, towarzyskiego, nienaruszalności mieszkania, tajemnicy korespondencji i ochrony informacji dotyczących danej osoby (jako „prawo do pozostawania w spokoju" czy „prawo jednostki do bycia pozostawiana samej sobie").

Życie rodzinne, związane po części z życiem prywatnym, oznacza pozostawanie w kręgu rodziny, przyjaciół czy bliskich znajomych. Obejmuje ono relacje do współmałżonka oraz osób pozostających w stosunku pokrewieństwa oraz powinowactwa[396]. Życie rodzinne dotyczy już szerszej sfery przeżyć i zdarzeń związanych z rodziną (nie tylko osób prowadzących z danym człowiekiem wspólne gospodarstwo domowe), ale także pewne doświadczenia czy tajemnice przeszłych pokoleń danej rodziny, pamięć o nich, przeżycia, wrażenia, przyzwyczajenia[397]. Będąc jednym z przejawów życia prywatnego, życie rodzinne objęte jest powszechnie używanym określeniem „prawa do pozostawienia w spokoju".

Za życie osobiste z kolei należy uznać pozostałe niż dotychczas przedstawione wymiary życia prywatnego czy życia rodzinnego. Jako aspekt życia osobistego należałoby w związku z tym uznać prawo jednostki do nieskrępowanego decydowania o sobie i swoim życiu, postępowaniu, a także decydowanie o spędzaniu wolnego czasu, zawieraniu znajomości, przedmiocie osobistych zainteresowań, o miejscu i sposobie zamieszkania, stylu ubioru, kwestii zawierania i utrzymywania określonych znajomości i relacji z innymi ludźmi.

---

[393] Życie publiczne jednostki obejmuje na pewno życie polityczne, tj. działanie jednostki jako cząstki suwerennego narodu, wszelkie dalsze relacje jednostki ze współmieszkańcami kraju, podczas których pozostają oni jednak wobec niej osobami anonimowymi, często nieznanymi, niepowiązanymi żadnymi szczególnymi więzami o charakterze osobistym (życie społeczne zawierające w sobie zasadniczo też życie zawodowe). Zob. P. Sarnecki, *Art. 47*…, s. 2.

[394] Wyrok TK z dnia 19 maja 1998 r., U 5/97, OTK 1998, Nr 4 poz. 46.

[395] Orzeczenie TK z dnia 24 czerwca 1997 r., K 21/96, OTK 1997, Nr 2, poz. 23.

[396] W Konstytucji RP małżeństwo i rodzina potraktowane są jako podstawowa komórka społeczna, przez to w pewnym sensie pełnią też walor publiczny (na mocy art. 18 zapewnione są im ochrona i opieka). „Ustrojowa" rola rodziny skupiać się będzie na jej rozmaitych przywilejach w życiu społecznym, zaś prawna ochrona życia rodzinnego polegać będzie na budowaniu pewnych barier prawnych ograniczających ingerencję w tę sferę życia wszelkich czynników postronnych. Regulacja statusu małżeństwa i rodziny zawiera w sobie jakby dwa ciągi: jeden, polegający na stabilizowaniu i uprzywilejowaniu ich, mając swój punkt wyjścia w art. 18, a drugi, polegający na traktowaniu osobistych aspektów małżeństwa i rodziny, w szczególności sfery uczuciowej tam funkcjonującej, jako pewnej specyficznej „niszy", do której wkraczanie czynników postronnych jest wyłączone. Zob. B. Banaszak, *Konstytucja…,* s. 246.

[397] *Ibidem*, s. 246.

Swoboda (prawo) do decydowania o swoim życiu osobistym, wywiedziona z art. 47 Konstytucji RP, związana jest z integralnością istnienia sfery prywatnej, której immanentnym składnikiem jest przyznanie człowiekowi prawa do życia układanego według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej. Każdy ma swobodę decydowania o swoim życiu, nie jest to jednak prawo bezwzględne z uwagi na ograniczenie go przez inne zasady konstytucyjne. Przepis ten należy zatem rozumieć jako zakaz wkraczania w sferę prywatności każdego człowieka i jednocześnie jako zakaz podejmowania przez organy państwa działań naruszających tę sferę[398]. Tylko wyjątkowo, na podstawie Konstytucji czy na podstawie ustawy, można uchylić ochronę gwarantowaną w treści art. 47, albo poprzez wyrażenie dobrowolnej, wyraźnej zgody przez zainteresowany podmiot. Ograniczenia ustawowe dotyczyć mogą na przykład obowiązków informacyjnych (statystycznych, meldunkowych, medycznych) nakładanych na obywatela w zakresie niezbędnym w demokratycznym państwie prawnym lub mogą być zastosowane w stosunku do osób sprawujących funkcje publiczne lub gospodarujących środkami publicznymi, o ile ma to związek z ich działalnością.

Art. 47 Konstytucji RP zabrania ingerencji państwa w ustalony prawnie zakres życia człowieka, zaś w przypadku naruszenia tej sfery nakazuje państwu zapewnić ochronę jednostce. Trybunał Konstytucyjny wielokrotnie wskazywał, że „prawo do prywatności, podobnie jak inne prawa i wolności, nie ma charakteru absolutnego i z tej też racji może podlegać ograniczeniom. Ograniczenia te winny jednak czynić zadość wymaganiom konstytucyjnym. Przemawiać za nimi muszą inne normy, zasady lub wartości konstytucyjne. Stopień ograniczenia powinien pozostawać w odpowiedniej proporcji do rangi interesu, któremu ograniczenie to służy. Ze względu na zasadę proporcjonalności niezbędne jest porównanie dobra chronionego i poświęconego oraz zharmonizowanie kolidujących interesów”[399].

Prawo do prywatności, wyrażone w art. 47 Konstytucji RP, rozciąga się także w swej konstrukcji na dobre imię i cześć konkretnej osoby. Cześć definiowana jest jako wewnętrzne przekonanie jednostki o jej wartości w społeczeństwie i wynikającym z tego, należnym jej szacunku, zaś dobre imię to dbałość jednostki o dobrą opinię o niej wśród innych członków społeczeństwa[400]. Naruszenie tych wartości związane jest z działaniem osób trzecich i polega zwykle na rozpowszechnianiu czy publikowaniu nieprawdziwych informacji, które mogą

---

[398] J. Boć, *Konstytucje…,* s. 94.
[399] Wyrok TK z dnia 21 października 1998 r., K 24/98, OTK 1998, Nr 6, poz. 97.
[400] Por. B. Banaszak, *Konstytucja…*, s. 246.

zaszkodzić imieniu lub wizerunkowi określonej osoby. O ile naruszenie sfery prywatności dotyczy informowania o rzeczywistym życiu prywatnym określonej osoby, oczywiście bez jej zgody, o tyle naruszenie czci i dobrego imienia dotyczy sytuacji, w której informacje są nieprawdziwe, i których celem jest wyłącznie wyrządzenie krzywdy czy szkody[401]. Takie elementy jak dobre imię i cześć, definiujące prywatność, chronione są jako dobra samoistne (art. 23 k.c.), co nie zmienia jednak faktu, że ich ochrona stanowi gwarancję nienaruszalności życia prywatnego, zapewniając jednocześnie poszanowanie godności człowieka i jego egzystencji[402]. Jak wskazuje B. Banaszak, „można się nawet pokusić o stwierdzenie, iż dla zachowania godności niezbędna jest ochrona prywatności człowieka wyrażająca się w nieingerencji (ze strony państwa, ale i innych podmiotów) w określoną konstytucyjnie sferę życia jednostki i zabezpieczeniem jej przed nieuprawnionymi działaniami zmierzającymi do naruszenia owej sfery. Wiąże się z tym także zapewnienie jednostce prawa dostępu do danych dotyczących jej szeroko rozumianej tożsamości (łącznie z uprawnieniami do ich poprawiania czy usuwania), jeśliby takie znajdowały się w posiadaniu innych niż ona podmiotów (zapewnieniu prywatności najlepiej służyłoby zagwarantowanie jednostce prawa do „samookreślenia informacyjnego", a więc do jej wyłącznej decyzji pozostawiono, by sprecyzowanie tego, kto, o czym i w jaki sposób może się o niej dowiedzieć)"[403].

Generalne postanowienia art. 47 są na tyle ogólne, że występuje niewątpliwa potrzeba bliższego określenia tego prawa i płynących stąd konsekwencji prawnych, czego jednak Konstytucja nie zapowiada[404]. Ochrona prywatności na gruncie art. 47 ma charakter subsydiarny. Jeżeli więc jakaś materia nie została objęta szczegółowymi unormowaniami o konkretnych elementach prywatności, to gwarancje poszanowania życia prywatnego można wyprowadzać bezpośrednio z art. 47 Konstytucji RP[405]. W taki zatem sposób z prawa do prywatności wywieść można prawo jednostki do ochrony danych osobowych, które na gruncie Konstytucji RP zawarte jest m. in. w art. 51. W krajach, w których konstytucje nie wspominają wprost o zagadnieniu ochrony danych osobowych, nadanie ich ochronie rangi konstytucyjnej odbywa się niekiedy właśnie przez odpowiednią interpretację norm poświęconych ochronie dóbr osobistych czy prywatności[406].

---

[401] Por. J. Boć, *Konstytucje…,* s. 94.
[402] B. Banaszak, *Konstytucja…*, s. 247.
[403] *Ibidem*, s. 247.
[404] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, s. 51.
[405] Zob. J. Braciak, *Prawo do prywatności…,* s. 164.
[406] Zob. M. Wild, *op. cit.*, s. 55.

Konstytucja RP zapewnia w art. 47 prawo do prywatności, a jego konsekwencje widoczne są właśnie w treści art. 51. Trybunał Konstytucyjny wskazał, że przytoczone przepisy art. 47 i art. 51 Konstytucji „pozostają w określonej relacji wzajemnej: prawo do prywatności, statuowane w art. 47 Konstytucji, zagwarantowane jest m. in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51 Konstytucji. Ten ostatni, rozbudowany przepis, odwołując się aż pięciokrotnie do warunku legalności - *expressis verbis* w ust. 1 i ust. 3-5 oraz pośrednio przez powołanie się na zasadę demokratycznego państwa prawnego w ust. 2 - stanowi konkretyzację prawa do prywatności w aspektach proceduralnych” [407]. To właśnie wśród norm art. 51 zostały zawarte bezpośrednie gwarancje ochrony danych osobowych.

Art. 51 ustawy zasadniczej stanowi m. in., że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą”. Ochrona danych osobowych przed ich niewłaściwym, tj. szkodliwym dla jednostki wykorzystaniem, stała się jedną z podstawowych wartości chronionych we współczesnym świecie. Konstytucja w treści art. 51 zagwarantowała prawo jednostki do ochrony danych osobowych, w zakres którego wchodzi m. in.: warunek ustawowej podstawy ujawnienia przez jednostkę informacji dotyczących jej osoby (art. 51 ust. 1), zakaz pozyskiwania, gromadzenia i udostępniania o obywatelach innych informacji niż niezbędne w demokratycznym państwie prawnym (art. 51 ust. 2), a także prawo dostępu jednostki do odnośnych dokumentów i zbiorów danych oraz żądania sprostowania bądź usunięcia danych nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (art. 51 ust. 3 i 4)[408]. Artykuł ten zawiera ponadto generalną zapowiedź konstytucyjną, zgodnie z którą „zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa” (art. 51 ust. 5)[409].

Wyrażona w art. 51 ust. 1 zasada, że nikt (a więc nie tylko obywatel) nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby sprawia, że dla wszystkich obowiązków informacyjnych każdego podmiotu prawa

---

[407] Zob. M. Zubik, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego*, Kraków 2000, s. 399.
[408] Zob. M. Zubik, *Konstytucja III RP w tezach orzeczniczych Trybunału Konstytucyjnego i wybranych sądów*, Warszawa 2011, s. 291.
[409] Wyrok TK z dnia19 maja 1998 r., U 5/97.

wymagana będzie w naszym kraju podstawa ustawowa[410]. Tylko zatem regulacja na gruncie ustawy może zobowiązywać do podawania informacji o sobie. Wskazana w art. 51 ust. 1 Konstytucji wolność jednostki do ujawniania informacji dotyczących swej osoby, oznacza prawo jednostki do nieujawniania informacji innym podmiotom, a zwłaszcza władzom publicznym. Konsekwencją tego jest zakaz skierowany do wskazanych podmiotów podejmowania jakichkolwiek prób uzyskania tego typu informacji poprzez indagację tych osób. Ponadto wskazana wolność obejmuje wolność od ujawniania wszelkich informacji dotyczących każdego nie tylko ściśle osobistego, lecz także publicznego zachowania się jednostki, a jej szczególnym wyrazem jest wolność od ujawniania władzom publicznym swojego światopoglądu, przekonań religijnych lub wyznania[411].

Rozważania dotyczące treści autonomii informacyjnej jednostki pojawiły się również w orzecznictwie Trybunału Konstytucyjnego. W wyroku z 19 lutego 2002 r. Trybunał zdefiniował to pojęcie wskazując, że jest to „prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, znajdującymi się w posiadaniu innych podmiotów”[412]. W wyroku z 20 listopada 2002 r. Trybunał orzekł, że autonomia informacyjna (art. 51 Konstytucji) stanowi jeden z komponentów prawa do prywatności, w szerokim, przyjętym w art. 47 Konstytucji, tego słowa znaczeniu i gwarantuje ją przede wszystkim art. 51 Konstytucji[413]. Trybunał uznał także, że „art. 51 ust. 1 Konstytucji potwierdza prawo jednostki do samodzielnego decydowania o ujawnianiu informacji o sobie. Obowiązek ujawniania informacji o sobie stanowi ograniczenie autonomii informacyjnej. Ograniczenie takie może zostać wprowadzone tylko w drodze ustawy, przy czym nałożenie takiego obowiązku powinno mieścić się w granicach ingerencji państwa w sferę konstytucyjnych wolności i praw człowieka i obywatela, wyznaczonych przez art. 31 ust. 3 Konstytucji”[414].

W wyroku z 29 stycznia 2002 r. Trybunał Konstytucyjny z kolei zwrócił uwagę, iż art. 51 ust. 1 Konstytucji RP „nie określa w sposób jednoznaczny podmiotu zobowiązanego do realizacji prawa zagwarantowanego w tym przepisie. Oznacza to, że wymieniony przepis

---

[410] W doktrynie starano się już wcześniej wywodzić ten obowiązek z ogólnej zasady legalizmu działania administracji (zasady, że prawa i obowiązki obywatela muszą mieć podstawę ustawową), ale przez umieszczenie działań informacyjnych w sferze działań wewnętrznych lub działań nieformalnych obchodzono ten obowiązek, np. w związku z nadaniem numeru identyfikacyjnego PESEL. Zob. J. Boć, *Konstytucje…,* s. 98.
[411] P. Sarnecki, *Art. 51..,* s. 1-2.
[412] Wyrok TK z dnia19 lutego 2002 r., U 3/01.
[413] Wyrok TK z dnia 20 listopada 2002 r., K 41/02.
[414] Wyrok TK z dnia 19 lutego 2002 r., U 3/01.

konstytucyjny dotyczy wszelkich przypadków, w których jednostka zobowiązana zostaje do ujawniania informacji o sobie innym podmiotom, a więc także podmiotom prywatnym"[415].

Zasada zawarta w art. 51 ust. 1 wskazuje, że zobowiązania do ujawniania informacji na swój temat mają zawsze wyjątkowy charakter, co wyklucza dokonywanie ich interpretacji w sposób rozszerzający oraz że muszą mieć one ustawowe umocowanie[416]. Nie mogą zatem wynikać np. z aktów wewnątrzzakładowych, ani z układów zbiorowych pracy, norm deontologicznych czy nawet z prawa zwyczajowego[417]. Zasada ta odnosi się też do wszelkich tego rodzaju informacji i nie została zawężona do informacji szczególnego charakteru albo dotyczących szczególnych kwestii.

Prawo do decydowania o ujawnianiu swoich danych osobowych przysługuje „każdemu". Art. 51 ust. 1 szeroko określa zakres podmiotowy gwarantowanego w nim prawa. Użyte określenie „nikt" należy rozumieć jako „każdy", a więc mamy tu do czynienia z prawem człowieka[418]. Jak słusznie zauważają J. Barta, P. Fajgielski i R. Markiewicz, „Konstytucja nie nakłada konieczności spełnienia przez osobę fizyczną jakichkolwiek warunków, np. dotyczących wieku, stanu psychicznego, zdolności do czynności prawnych"[419]. Nie jest to też prawo należące do „praw publicznych", a zatem sądowe pozbawienie osoby takich praw nie odbiera jej możliwości decydowania o udostępnianiu danych osobowych.

W celu wzmocnienia ochrony praw jednostki Konstytucja formułuje w art. 51 ust. 2 wyraźne ograniczenie skierowane pod adresem władz publicznych, a dotyczące pozyskiwania, gromadzenia i udostępniania informacji o obywatelach wyłącznie w takim zakresie, w jakim jest niezbędne w demokratycznym państwie prawnym[420]. Jeśli chodzi o zakres art. 51 ust. 2 Konstytucji to według Trybunału Konstytucyjnego chroni on obywateli polskich, wprowadzając dla władz publicznych (ustawodawczej, wykonawczej, sądowniczej) zakaz wkraczania w autonomię informacyjną jednostki w sposób zbędny z punktu widzenia standardów demokratycznego państwa prawa. Ani więc względy celowości, ani wygody władzy nie uzasadniają naruszenia autonomii informacyjnej[421]. Tak zatem zakres podmiotowy

---

[415] Wyrok TK z dnia 29 stycznia 2002 r., K 19/01, OTK-A 2002, Nr 1, poz. 1.
[416] Musi być to uzasadnione interesem publicznym dla celów statystycznych, gospodarczych itp. Zob. W. Skrzydło, *Konstytucja…*, s. 53.
[417] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 94.
[418] B. Banaszak, *Konstytucja…*, s. 261.
[419] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 95.
[420] P. Litwiński, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa 2009, s. 22.
[421] J. Oniszczuk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego*, Kraków 2000, s. 469.

określony w art. 51 ust. 2 jest odmienny niż w ust. 1, gdyż odnosi się tylko do obywateli (art. 51 ust. 2 Konstytucji RP „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym"). Można więc wyprowadzić wniosek, iż władze publiczne mogą przetwarzać informacje dotyczące innych osób, a dane poddane przetworzeniu nie muszą spełniać jednocześnie warunku niezbędności w demokratycznym państwie prawnym[422].

Postanowienia art. 51 ust. 2 Konstytucji są adresowane głównie do organów państwa (mowa jest o władzach publicznych czy urzędowych dokumentach i zbiorach danych), nie można jednak na tej podstawie wnioskować, że podmioty niepubliczne nie podlegają ograniczeniom narzuconym przez art. 51[423]. I. Lipowicz podnosi, iż „nie ma miejsce w ust. 1 art. 51 podziału na sektor publiczny i prywatny. Oznacza to, że również żądanie informacji ze strony elektrowni czy telekomunikacji wymaga - jeżeli ma stać się obowiązkiem informacyjnym - podstawy ustawowej. Udzielenie informacji o osobie może być częścią umowy, musi jednak pozostawać w jej granicach i dawać swobodę wyboru"[424].

Niezwykle istotne jest wprowadzenie określonych granic co do możliwości pozyskiwania i przetwarzania informacji o osobach przez władze publiczne, nawet za zgodą ustawodawcy. Jak pokazują doświadczenia, władze publiczne skłonne są do nieograniczonego, lecz zbędnego i bezcelowego niejednokrotnie gromadzenia informacji o osobach, wkraczając przy tym w ich życie prywatne, rodzinne i osobiste. Potrzeba gromadzenia danych o charakterze informacyjnym o innych jednostkach winna być uzasadniona potrzebami wspólnoty oraz interesem demokratycznego państwa prawnego. Określenie informacji „niezbędnych w demokratycznym państwie prawnym" na potrzeby omawianego artykułu należałoby interpretować z punktu widzenia władz publicznych i za niezbędną uznać każdą informację, bez posiadania której władza publiczna nie będzie zdolna do podjęcia (czy zakończenia) działań w ramach przyznanych im kompetencji[425].

Niezbędnym składnikiem państwa demokratycznego jest zakaz podejmowania działań przez państwo ponad potrzebę, co na gruncie ochrony danych osobowych można interpretować jako udział obywateli w podejmowaniu decyzji w zakresie ochrony danych osobowych. Niekontrolowane przetwarzanie danych osobowych, kiedy obywatel nie wie, kto i w jakim celu przetwarza jego dane osobowe, rodzi niebezpieczeństwo ograniczenia pełnej

---

[422] *Ibidem*, s. 261.
[423] B. Banaszak, *Konstytucja…*, s. 261.
[424] I. Lipowicz, *Konstytucyjne prawo do informacji a wolność informacji*, [w:] *Wolność informacji i jej granice*, red. G. Szpor, Katowice 1997, s. 14.
[425] B. Banaszak, *Konstytucja…*, s. 262.

swobody podejmowania decyzji czy rozstrzygania o własnych możliwościach. I. Lipowicz, nie negując możliwości krajowych i międzynarodowych banków danych i systemów informatycznych o charakterze policyjnym czy medycznym, stwierdza, że „jeżeli zakres podobnych systemów informacyjnych staje się dla wygody administracji zbyt szeroki (inwigilacja «na wszelki wypadek» szerszych grup społecznych, jednolite «konto informacyjne» obywatela pozostające w integracji setek danych administracyjnych z różnych dziedzin) lub szczegółowość danych prowadzi to tworzenia «profilów osobowych» (uproszczonej informatycznej charakterystyki jednostki), czy wreszcie dochodzi do ukrytego lub jawnego oznaczenia obywateli za pomocą numerów identyfikacyjnych nie o charakterze porządkowym, lecz znaczącym, mamy do czynienia z przypadkiem wykraczającym poza to, co niezbędne w demokratycznym państwie prawnym”[426].

Realizację prawa do ochrony danych osobowych ma zapewnić jednostce prawo dostępu do dotyczących jej urzędowych dokumentów i zbiorów danych, a ograniczenie tego prawa może określić ustawa[427]. Jak podnosi B. Banaszak, „użyty w art. 51 ust. 3 zwrot urzędowe dokumenty i zbiór danych sugeruje, iż chodzi o wszelkie możliwe źródła informacji znajdujące się w posiadaniu którejkolwiek z trzech władz”[428]. Jest to kluczowa regulacja, na mocy której każdy ma prawo dostępu do informacji znajdującej się w posiadaniu organów państwa i samorządu terytorialnego[429]. Ani dokument urzędowy ani zbiór danych, o których mowa w art. 51 ust. 3, nie muszą mieć charakteru „osobowego” w całości (jak np. rejestr osób) i wystarcza, że dane będą dotyczyć jednej osoby, np. jako właściciela pojazdu lub nieruchomości[430]. Dokument urzędowy dotyczący określonej osoby (ewentualnie zestaw takich dokumentów) nie jest oznaczeniem tożsamym ze zbiorem danych, jednak zbliżonym. Dokumenty urzędowe są przede wszystkim świadectwem odpowiednich działań władz publicznych (np. angaże, zaszeregowania i inne dokumenty znajdujące się w aktach osobowych pracowników), a zbiory danych są zaś zestawami informacji, uzyskanymi przez

---

[426] I. Lipowicz, *Teza nr 3 do art. 51 Konstytucji RP*, [w:] *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, red. J. Boć, Wrocław 1998, s. 99.

[427] Prawo to nie ma już tak bezwzględnego charakteru jak poprzednio omawiana zasada, jednak jest niezwykle ważne. Zakres podmiotowy prawa gwarantowanego w art. 51 ust. 3 jest taki sam jak w art. 51 ust. 1.

[428] B. Banaszak, *Konstytucja…*, s. 263.

[429] Stanowi też jakby dodatkowe wzmocnienie, ustanowionego w art. 61 Konstytucji RP, ogólnie sformułowanego prawa do uzyskiwania informacji o działalności organów władzy publicznej czy jeszcze szerzej ujętego prawa do pozyskiwania i rozpowszechniania informacji- wynikającego z art. 54 ust. 1 Konstytucji RP (*„Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji”)* Zob. *Ibidem*, s. 263.

[430] J. Boć, *Konstytucje…..,* s. 100.

dany czynnik władzy publicznej[431]. Można więc domagać się dostępu do pojedynczych zapisów niebędących częścią większego zbioru, a także do wszelkich zbiorów, gdyż nie zostały wyłączone z możliwości dostępu żadne zbiory informacji i dokumentów (np. będących w posiadaniu policji)[432]. Nie można jednak domagać się dostępu do dokumentów i zbiorów „nieurzędowych", tj. prywatnych, nawet jeśli będą one w całości nastawione na gromadzenie informacji dotyczących danej osoby (możliwe jest jednak ograniczenie dostępu do nich, o ile zostaną one wprowadzone w drodze ustawy wydanej zgodnie z art. 31 ust. 3 Konstytucji) [433].

Żaden organ państwowy nie może przetwarzać informacji o obywatelach, nie licząc się z możliwością kontroli z ich strony. Konstytucja wskazuje prawne wytyczne, które precyzuje ustawa o ochronie danych osobowych. Zbiory danych czy dokumenty zakwalifikowane nawet jako tajne, np. z uwagi na bezpieczeństwo państw, mogą zostać poddane weryfikacji na wniosek osoby, której dotyczą (zapewne kontrola ta nie przybierze w tym wypadku formy bezpośredniego dostępu zainteresowanego do tych danych, jednak dzięki możliwości odwołania się np. do Generalnego Inspektora Ochrony Danych osobowych, a następnie do NSA wyczerpana zostanie droga krajowa). Ponadto prawo, o którym mowa, może być ograniczone tylko normami rangi ustawowej. Ustawodawca miał na myśli ustawę nie jako jeden konkretny akt, lecz jako akt określonego typu[434].

Polski system prawny opiera się na zasadzie samodzielnego decydowania o informacjach na temat własnej osoby[435]. Zasada ta dotyczy wszystkich osób i powiązana jest z możliwością nadzorowania posługiwania się takimi informacjami, poprzez możliwość edycji własnych danych osobowych[436]. Konstytucja RP formułując w art. 51 ust. 4 prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą, „mówi o szczególnym uprawnieniu wynikającym z ogólnej zasady art. 47 Konstytucji, obejmującej prawo do przedstawiania/ kształtowania swego

---

[431] Ponieważ dla jednostki i dla jej prawa do prywatności obydwa zestawy mają analogiczne znaczenie, stąd też jednolite ich potraktowanie w komentowanym artykule. Zob. P. Sarnecki, *Art. 51…*, s. 5.
[432] Możliwe jest ograniczenie dostępu do nich o ile zostaną one wprowadzone w drodze ustawy wydanej zgodnie z art. 31 ust. 3 Konstytucji RP.
[433] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 95.
[434] Zob. ustawa o ochronie danych osobowych, która określa zasady i tryb gromadzenia oraz udostępniania informacji, jednak i pewne zagadnienia szczegółowe regulują inne ustawy.
[435] Użyte stwierdzenie „informacje dotyczące osoby" może być uznane za synonim pojęcia danych osobowych. Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 95. Konstytucja używając formuły „informacji dotyczących osoby", wskazuje, że informacja zachowuje swój osobowy charakter do momentu, dopóki możliwe jest ustalenie na jej podstawie tożsamości konkretnej osoby, której dotyczy. Zob. B. Banaszak, *Konstytucja…*, s. 259.
[436] Zob. M. Polok, *Bezpieczeństwo danych osobowych*, Warszawa 2008, s. 79.

publicznego obrazu, rysującego się na tle danych zebranych przez władzę”[437]. Trzeba zaznaczyć, iż prawo to dotyczy całokształtu informacji będących w dyspozycji władz publicznych, przy czym art. 51 ust. 4 „nie odnosi się do rodzaju i zakresu informacji gromadzonych o osobie, ale jedynie do kwestii ich prawdziwości”[438]. Możność weryfikowania, prostowania lub usuwania danych osobowych jest urzeczywistnieniem prawa do kontroli. Uprawnienia uzyskane na mocy tego artykułu zapewniają jednostce chociażby realizację ustawowego prawa do kontroli przetwarzania danych osobowych na mocy art. 32 ust. 1 pkt 6 u.o.d.o. I. Lipowicz wskazuje, iż „rozwój informatyki sprawia, że uprawnienia informacyjne stają się coraz istotniejsze. Mylna lub fałszywa informacja osobowa może być pozbawić obywatela prawa do pracy, do pomocy społecznej czy do zasiłku dla bezrobotnych. W miarę automatyzacji procesu decyzyjnego, rozdziału różnorodnych świadczeń i ulg dane osobowe nabierają nowego znaczenia. Prawo do żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych lub zebranych sprzecznie z ustawa nie może podlegać - odmiennie niż prawo dostępu - ograniczeniu. […]. Pozostawienie w obrębie administracji fałszywych informacji o danym człowieku nie pozwala na racjonalne podejmowanie decyzji i jej zgodne z prawem działanie. Realizacja tego prawa głównie przez obywateli służy również sprawnemu i sprawiedliwemu wykonywaniu władzy publicznej”[439].

Chociaż w Konstytucji RP jest mowa o „prawie do żądania” sprostowana i usunięcia, to jednak według J. Barty, P. Fajgielskiego i R. Markiewicza „nie powinno to stanowić argumentu na rzecz osłabienia prawa i uznania, że jego respektowanie (przez dysponenta informacji) ma w jakiejś mierze uznaniowy charakter[440]. Ponadto autorzy ci stoją na stanowisku, iż „z żądaniem poprawienia, uzupełnienia lub usunięcia informacji nie można wystąpić przeciw każdemu (stosując wykładnię bardziej celową, racjonalną i uwzględniającą kontekst całej regulacji), ale tylko wówczas, gdy chodzi o informacje będące w gestii urzędów, znajdujące się w urzędowych dokumentach lub zbiorach. Wątpliwe byłoby formułowanie prawa do sprostowania tam, gdzie nie istnieje w ogóle prawo dostępu do zbioru informacji”[441].

Każdy, kto stwierdzi, że jego dane osobowe są niepełne, błędne i niewłaściwe może żądać ich sprostowania, a także może żądać usunięcia danych zebranych sprzecznie z u.o.d.o. Dysponentem tych danych jest więc tylko osoba, której dane dotyczą. W razie wątpliwości w

---

[437] Wyrok TK z dnia 12 grudnia 2005 r., K 32/04, OTK-A 2005, Nr 11, poz. 132.
[438] Wyrok TK z dnia 3 marca 2003 r., K 7/01, OTK-A 2003, Nr 3, poz. 19.
[439] Zob. I. Lipowicz, *Administracyjnoprawne zagadnienia informatyki*, Katowice 1984, s. 11.
[440] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 96.
[441] *Ibidem*, s. 96.

ustaleniu podmiotu władnego rozporządzać danymi, organem właściwym do rozstrzygnięcia przedmiotowego sporu, a tym samym zapewnienia skutecznej ochrony, jest sąd.

W ramach szeroko pojętego zagadnienia zakresu ochrony danych osobowych na gruncie Konstytucji RP istotne są również inne niż dotychczas przedstawione konstytucyjne regulacje, pośrednio odnoszące się do ochrony danych osobowych, jednak mające znaczący wpływ na ochronę przetwarzania danych osobowych w Polsce.

Gwarantowana na mocy art. 49 Konstytucji wolność i ochrona tajemnicy komunikowania się odnosi się chociażby do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych. J. Barta, P. Fajgielski i R. Markiewicz stoją na stanowisku, iż przepływ informacji w tych systemach korzysta z ochrony danych osobowych, w odniesieniu do otwartych sieci komputerowych, w stosunku zaś do zamkniętych systemów znajduje się poza zakresem konstytucyjnych gwarancji tajemnicy komunikowania się[442].

Kolejnym prawem zawartym w Konstytucji RP w obrębie ochrony danych osobowych jest prawo do informacji, gwarantowane w art. 54 i art. 61. Mamy tu do czynienia z pewnego rodzaju konfliktem konstytucyjnie chronionych praw, gdyż z jednej strony jednostka ma prawo chronić swoje dane osobowe, zaś z drugiej strony może domagać się uzyskania informacji o innych osobach. Szczegółowe regulacje w tym zakresie znajdują się w ustawie o dostępie do informacji publicznej[443].

Na koniec należałoby jeszcze wskazać na przyjętą w Konstytucji „swobodę działalności gospodarczej" wyrażoną w art. 22. Ograniczenie wolności działalności gospodarczej jest dopuszczalne tylko w drodze ustawy i tylko ze względu na ważny interes publiczny. Nie ma powodów, aby nie przyjąć, iż w określonych przypadkach elementem działalności lub wręcz samą tego rodzaju działalnością może być przetwarzanie danych osobowych. Sygnalizowane w Konstytucji ograniczenia w tej mierze znajdują podstawę właśnie w komentowanej ustawie o ochronie danych osobowych; równocześnie wskazywać można, co najmniej w większości przypadków, na przemawiający za tymi ograniczeniami ważny interes publiczny[444].

Kluczową jednak przesłanką dla faktycznej realizacji konstytucyjnego statusu prawnego jednostki jest istnienie w danym państwie środków ochrony wolności i praw człowieka oraz obywatela, o których mowa w Konstytucji w art. 77 – art. 80. Te konstytucyjne gwarancje to zespół wszystkich obowiązujących w systemie prawnym danego

---

[442] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 98.
[443] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, z późn. zm.).
[444] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 98.

państwa rozwiązań i instytucji, zapewniających lub umożliwiających praktyczną i skuteczną realizację wolności i praw człowieka oraz obywatela na jego terytorium[445]. Na tej podstawie zatem wyrażone w Konstytucji m. in. prawo osobiste obywatela RP do pozyskiwania i gromadzenia informacji o człowieku jedynie takich, które są niezbędnie konieczne w demokratycznym państwie prawnym, jest zapewnione właśnie dzięki istnieniu formalnych gwarancji oraz funkcjonowaniu organu stojącego na straży przestrzegania praw jednostki. Powołanie i działalność Generalnego Inspektora Ochrony Danych jest zatem instytucjonalno-prawną gwarancją urzeczywistnienia ochrony praw i wolności człowieka w RP.

W art. 51 ust. 5 Konstytucji zawarta została zapowiedź uchwalenia ustawy regulującej zasady i tryb gromadzenia oraz udostępniania informacji. Na charakter art. 51 ust. 5 zwrócił uwagę Trybunał Konstytucyjny, który w wyroku z 19 lutego 2002 r. wskazał, że zasada wyłączności ustawy obejmuje zasady i tryb gromadzenia i udostępniania informacji. Przepis ten TK odnosi do gromadzenia i udostępniania informacji przez podmioty prywatne. W ocenie TK „niezależnie od możliwych wątpliwości co do zakresu art. 51 ust. 5 Konstytucji, na gruncie obowiązującej Konstytucji nie podlega dyskusji, że sprawy związane z przetwarzaniem danych osobowych należą do zakresu wyłączności ustawy. TK zwrócił uwagę w komentowanym artykule, że to ustawa w sposób zupełny i wyczerpujący regulować powinna wszystkie sprawy o istotnym znaczeniu dla urzeczywistnienia wolności i praw człowieka i obywatela zagwarantowanych w Konstytucji. Zasada wyłączności ustawy nie wyklucza przekazywania do unormowania w drodze rozporządzeń określonych spraw szczegółowych, dotyczących statusu jednostki, ale niemających istotnego znaczenia z punktu widzenia realizacji wolności i praw człowieka i obywatela zagwarantowanych w Konstytucji. Zasada wyłączności ustawy wymaga jednak, aby upoważnienie do wydania rozporządzenia spełniało wymagania określone w art. 92 Konstytucji”[446]. Odnosząc ustalenia TK do sfery przetwarzania danych osobowych Trybunał zwrócił uwagę, że sprawy istotne, które muszą zostać uregulowane w ustawie, obejmują w szczególności warunki dopuszczalności przetwarzania danych osobowych. Ustawa powinna określać w sposób szczególnie precyzyjny warunki przetwarzania danych dotyczących sfery intymności jednostki, a ustawodawca może natomiast przekazać do unormowania w drodze rozporządzenia niektóre sprawy szczegółowe i techniczne związane z przetwarzaniem danych osobowych[447]. Jak

---

[445] J. Matwiejuk, *Konstytucyjne wolności, prawa i obowiązki człowieka i obywatela*, [w:] *Prawo konstytucyjne*, red. M. Grzybowski, Białystok 2009, s. 102.
[446] Wyrok TK z dnia 19 lutego 2002 r., U 3/01.
[447] M. Zubik, *Konstytucja…*, s. 471.

powszechnie przyjmuje się w doktrynie, wykonaniem zapowiedzi z art. 51 ust. 5 stało się uchwalenie ustawy o ochronie danych osobowych (dalej: u.o.d.o.)[448].

3. Ochrona danych osobowych w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

a) uwagi ogólne

Podniesienie prywatności do rangi wartości konstytucyjnej wiązało się z koniecznością wprowadzenia szeregu zmian na poziomie ustawodawstwa zwykłego. Ustawa zasadnicza artykułuje jedynie potrzebę ochrony prawa obywateli do zachowania w tajemnicy danych o charakterze informacji osobowych, nakładając jednocześnie na ustawodawcę obowiązek stworzenia warunków koniecznych do jej zapewnienia w przypadku, gdy dochodzi do jej naruszeń[449]. Koniecznym elementem systemu ich ochrony jest więc rozwijająca postanowienia konstytucyjne ustawa, która konkretyzuje obowiązki wszystkich podmiotów przetwarzających dane osobowe. Szczególne znaczenie w tym zakresie odegrało uchwalenie wskazanej wyżej ustawy o ochronie danych osobowych[450]. Ustawa ta nie tylko zrealizowała konstytucyjny wymóg ochrony danych osobowych, ale także dostosowała polskie regulacje prawne w tym zakresie do międzynarodowych i europejskich standardów praw człowieka.

Prace nad ustawą trwały ponad 6 lat. Podstawowym wzorcem prawnym przy opracowywaniu projektu tej regulacji była Konwencja Nr 108 Rady Europy oraz postanowienia zawarte w dyrektywie 96/46/WE, a wpływ na uchwalenie tej ustawy miały przesłanki zarówno o wewnętrznym, jak i zewnętrznym charakterze[451].

Główne przyczyny wewnętrzne, które warunkowały stworzenie ustawy o ochronie danych osobowych w Polsce, miały związek z niezwykle szybkim rozwojem nowych technologii. W latach 90. nastąpił gwałtowny postęp informatyzacji, a także postęp technologiczny ułatwiających proces transmisji i przetwarzania danych. Te zjawiska stworzyły poważną ilość zagrożeń w stosunku do gromadzonych i przetwarzanych

---

[448] Tak np. B. Kurzępa, *Przestępstwa z ustawy o ochronie danych osobowych*, „Prokuratura i Prawo" 1999, Nr 6, s. 45.

[449] K. Wygoda, *Ochrona danych osobowych i prawo do informacji o charakterze osobowym,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002, s. 407.

[450] Ustawa o ochronie danych osobowych weszła w życie 30 kwietnia 1998 r., z wyjątkiem art. 8 - art. 11, art. 13 i art. 45, które weszły w życie po upływie dwóch miesięcy od dnia ogłoszenia oraz art. 55 - art. 59, obowiązujących po upływie 14 dni od dnia ogłoszenia.

[451] Por. *Prawna ochrona danych osobowych. Uzasadnienie projektu ustawy przyjętego przez Radę Ministrów 13 sierpnia 1996 r.,* „Przegląd Rządowy" 1996, nr 10, s. 88.

informacji, dlatego niezbędne stało się stworzenie prawnych szczegółowych regulacji, które wprowadziłyby skuteczny system ochrony i procedur w zakresie bezpiecznego i legalnego przetwarzania danych osobowych. Co więcej, na rozwój ochrony informacji osobowych wpłynęły także zmiany ustrojowe w państwie, które to dały prymat jednostce i jej prawom i wymusiły tym samym rewizję regulacji prawnych kształtujących jej status w państwie[452]. Czynniki uniemożliwiające wprowadzenie przez polskiego ustawodawcę do tej pory regulacji w tym zakresie, wypływały z okresu PRL, gdy ochrona danych osobowych odgrywała znacznie mniejszą rolę niż w tym czasie w krajach rozwiniętych[453].

Zewnętrznymi przesłankami powstania ustawy o ochronie danych osobowych okazały się istniejące standardy międzynarodowe, wśród nich Unii Europejskiej. Uchwalenie 29 sierpnia 1997 r. pierwszej w Polsce ustawy o ochronie danych osobowych było przejawem postępującej demokratyzacji życia publicznego i troski o ochronę prywatności każdego jej obywatela, a także uwzględniało doświadczenia zagraniczne. U.o.d.o. została przyjęta jako wyraz wykonania przez Polskę zobowiązania zapewnienia zgodności jej przyszłego ustawodawstwa z ustawodawstwem wspólnotowym, stosownie do treści art. 68 Układu Europejskiego z dnia 16 grudnia 1991 r. [454].

W brzmieniu, jakie ustawa otrzymała w chwili uchwalenia, nie można było jednak mówić o jej zgodności w dyrektywą 95/46/WE. U.o.d.o. w pierwotnej wersji nie mogła zostać uznana za implementację dyrektywy i z tego względu konieczne były jej istotne dwie nowelizacje w 2001 i 2004 r. Polska ustawa o ochronie danych osobowych, inaczej niż niektóre ustawy z zakresu ochrony danych państw członkowskich Unii Europejskiej, nie recypowała modelu regulacji zawartego w dyrektywie, a więc nie formułowała *explicite* podstawowych zasad przetwarzania danych osobowych[455]. Zamiast tego w przepisach u.o.d.o. zostały unormowane: zasady i tryb postępowania przy przetwarzaniu danych osobowych, prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych oraz sposób wykonywania tych uprawnień, a także zakres działania oraz zasady

---

[452] G. Koksanowicz, *Ochrona danych osobowych w świetle Konstytucji oraz Ustawy o ochronie danych osobowych*, [w:] *Konstytucyjny ustrój państwa*, red. T. Bojarski, E. Gdulewicz, J. Szreniawski, Lublin 2000, s. 90.

[453] B. Banaszak, K. Wygoda, *Regulacja prawna ochrony danych osobowych w Polsce w świetle ustawy z 29 sierpnia 1997 r. i standardów europejskich*, [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 49.

[454] Dz. U. z 1994 r., Nr 11, poz. 38 z późn. zm.; Układ Europejski ustanawiał stowarzyszenie między Rzeczpospolitą Polską z jednej strony a Wspólnotami Europejskimi i ich państwami członkowskimi z drugiej strony.

[455] Jak wskazuje P. Litwiński, *op. cit*., s. 22., w nauce prawa przyjmuje się, że art. 26 u.o.d.o „odpowiada" art. 6 dyrektywy 95/46/WE. Por. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit*., s. 548.

organizacji i funkcjonowania organu do spraw ochrony danych osobowych, jakim jest Generalny Inspektor Ochrony Danych Osobowych.

Biorąc pod uwagę założenie, iż prawo uznaje się za skuteczne, „jeżeli jego normy w sposób bezpośredni lub pośrednio, poprzez akty stosowania prawa i wykonywanie tych aktów, wywołują skutki zgodne w dostatecznie wysokim stopniu z założonym przez prawodawcę lub inne podmioty celem”[456], publicznoprawna ochrona danych osobowych od samego początku była niepełna, a to z uwagi na nieskuteczność regulacji na skutek przebiegu procesów legislacyjnych[457]. Niestabilność ochrony danych osobowych spowodowana była faktem, iż ustawę wielokrotnie nowelizowano. Oczywiście, nie bez znaczenia był też fakt dalszego rozwoju technologicznego, a także procesy integracji europejskiej, w których Polska brała czynny udział, co niosło za sobą konieczność uaktualniania i uszczegóławiania materii w zakresie przetwarzania informacji osobowych. Badając literaturę przedmiotu z trudem można napotkać na kompleksową analizę wszystkich nowelizacji przedmiotowej ustawy. Najwięcej, bo aż 5 nowelizacji uchwalono w 2001 r., 3 nowelizacje dokonano w 2004 r., a kolejne miały miejsce w 2010 r.

Pięć pierwszych ustaw zmieniających dotyczyło tylko art. 43 ust. 1 u.o.d.o. i wiązało się z utworzeniem nowych jednostek w ramach reformy samorządowej[458], utworzeniem Krajowego Rejestru Karnego[459], powołaniem Generalnego Inspektora Informacji Finansowej[460] nową ustawą z dnia 11 kwietnia 2001 r. o rzecznikach patentowych[461] oraz przetwarzaniem danych przez doradcę podatkowego i biegłego rewidenta[462].

---

[456] Z. Kmieciak, *Skuteczność regulacji administracyjnoprawnej*, Łódź 1994, s. 27-28.
[457] G. Szpor, *Uwarunkowania…,* s. 30.
[458] Art. 47 ustawy z dnia 21 stycznia 2000 r. o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej (Dz. U. Nr 12, poz. 136), dotyczył zmiany w treści art. 43 ust. 1 pkt 6 u.o.d.o.: po wyrazach „rad gmin*”* dodano wyrazy „rad powiatów” i „sejmików województw” (od dnia 23 lutego 2000 r.).
[459] Art. 29 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. nr 50, poz. 580), dotyczył zmian w treści art. 43 ust. 1 pkt 2, który otrzymał brzmienie: „2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym” (od dnia 22 czerwca 2001 r.).
[460] Art. 47 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł (Dz. U. Nr 116, poz. 1216), dodał do art. 43 ust. 1 u.o.d.o., po pkt 2, pkt 2a, w brzmieniu: „2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej” (od dnia 23 czerwca 2001 r.)
[461] Dz. U. Nr 42, poz. 509.; Art. 71 dotyczył art. 43 ust. 1 pkt 5 u.o.d.o., w którym po wyrazach „radcy prawnego” dodaje się wyrazy „rzecznika patentowego” (od dnia 11 czerwca 2001 r.).
[462] Art. 11 ustawy z dnia 11 kwietnia 2001 r. o zmianie ustawy o doradztwie podatkowym oraz niektórych innych ustaw (Dz.U. Nr 49, poz. 474), dotyczy art. 43 ust. 1 pkt 5, otrzymał brzmienie: „5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego lub biegłego rewidenta” (od dnia 22 sierpnia 2001 r.).

Ustawą z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych[463]. zostało znowelizowanych 19 artykułów[464], co wprowadziło istotne zmiany do istniejącego dotychczas porządku prawnego. W uzasadnieniu projektu podkreślono, że proponowane zmiany wynikały z konieczności dostosowania polskiej ustawy do postanowień dyrektywy 95/46/WE. Nowelizacja ta zredukowała istotne wątpliwości terminologiczne i zniosła zbędne bariery przetwarzania danych osobowych, które ujawniły się w trakcie stosowania ustawy, rozbudowała uprawnienia osoby, której dane są przetwarzane w systemach teleinformatycznych, a także spełniła postulaty przedsiębiorców, poszerzając przesłanki dopuszczalności przetwarzania i redukując obowiązki informacyjne[465]. Konsekwencją tej nowelizacji była także zmiana rozporządzenia wykonawczego MSWiA[466]. Nowelizacja z 2001 r., o której mowa, w sposób istotny zmieniła zasady publicznoprawnej ochrony informacji dotyczących osób fizycznych. Głównym celem zmian postawionych przez prawodawcę było pełne dostosowanie krajowej ustawy o ochronie danych osobowych do wymogów dyrektywy 95/46/WE; chodziło przede wszystkim o definicję danych osobowych i zasadę automatyzacji rozstrzygnięć indywidualnych. Niejako przy okazji nowela wprowadziła znaczące modyfikacje w zakresie definicji legalnych przesłanek dopuszczalności przetwarzania danych osobowych, uprawnień Generalnego Inspektora oraz obowiązków administratorów danych w tym dotyczących rejestracji zbiorów danych[467].

Kolejna nowelizacja, dokonana ustawą z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[468], ograniczyła na mocy art. 43 ust. 2 u.o.d.o uprawnienia kontrolne GIODO. Po tej nowelizacji ukazał się tekst jednolity ustawy o ochronie danych osobowych, a wkrótce potem w związku z reformą sądownictwa administracyjnego, dokonano terminologicznej zmiany art. 21 ust. 2 u.o.d.o.[469].

---

[463] Dz. U. Nr 100, poz. 1087.

[464] Nowelizacja ta dotyczyła: art. 6; art. 7 pkt 2a, 2b; art. 14 pkt 1; art. 15; art. 18 ust. 2a; art. 23 ust. 1 pkt 3 i 5; art. 23 ust. 4; art. 24 ust. 2; art. 25 ust. 2 pkt 4,5,6; art. 26a; art. 27 ust. 1, art. 27 ust. 2 pkt 8,9,10; art. 28, art. 32 ust. 1 pkt 8,9; art. 32 ust. 2,3,3a; art. 35 ust. 3; art. 36, art. 41 ust. 1 pkt 4a,7; art. 43 ust. 1 pkt 1a; art. 43 ust. 2

[465] G. Szpor, *Uwarunkowania…,* s. 34.

[466] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 1 października 2001 r. zmieniające rozporządzenie w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 121, poz. 1306).

[467] G. Sibiga, *Nowelizacja ustawy o ochronie danych osobowych*, „Monitor Prawniczy" 2001, nr 23, s. 1153.

[468] Dz. U. Nr 74, poz. 676.

[469] Ustawa z dnia 30 sierpnia 2002 r. (Dz. U. Nr 101, poz. 926.). Przepisy wprowadzające ustawę - Prawo o ustroju sądów administracyjnych i ustawę - Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1271), w art. 21 ust. 2 wyrazy „Naczelnego Sądu Administracyjnego" zastępuje się wyrazami „sądu administracyjnego" (od dnia 1 stycznia 2004 r.)

Także istotna zmiana nastąpiła w 2004 r. na mocy ustawy z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych [470] i była to największa z dotychczasowych nowelizacji u.o.d.o. Dotyczyła 34 artykułów[471], w tym również tych, które były znowelizowane niespełna trzy lata wcześniej, powołując się na te same uzasadnienie dotyczące integracji europejskiej i potrzebę zgodności z dyrektywą 95/46/WE[472]. Uchwalenie przedmiotowej ustawy stanowiło realizację dwóch zasadniczych celów: dalszego dostosowywania niektórych przepisów ustawy do wymogów dyrektywy 95/46/WE oraz wprowadzenia zmian podyktowanych doświadczeniami zebranymi przez Generalnego Inspektora Ochrony Danych Osobowych w procesie stosowania u.o.d.o.[473]. Wprowadzone zmiany nie ograniczały się do samej ustawy. Dotychczasowe rozporządzenia wykonawcze przestały obowiązywać 1 maja 2004 r., a w ich miejsce wprowadzono rozporządzenie Prezydenta RP z 29 maja 1998 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych[474].

Kolejne nowelizacje ustawy o ochronie danych osobowych podyktowane były różnymi zmianami wprowadzanymi w innych ustawach, co niosło za sobą konieczność dostosowania i ujednolicenie pojęć oraz instytucji także w samej u.o.d.o.

Ustawą z dnia 23 stycznia 2004 r. Ordynacja wyborcza do Parlamentu Europejskiego[475] zostały znowelizowane m. in. art. 18 ust. 2 u.o.d.o oraz 43 ust. 1 pkt 6 u.o.d.o.

Ustawą z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym[476] wprowadzono zmiany w treści art. 43 ust. 2 u.o.d.o., a odnosiły się do wyłączenia uprawnień GIODO w zakresie rejestracji zbiorów danych przetwarzanych przez Agencję

---

[470] Dz. U. Nr 33, poz. 285; zmiana ustawy o ochronie danych osobowych weszła w życie 1 maja 2004 r.

[471] Nowelizacja ta dotyczyła: art. 2 ust. 2; art. 3; art. 3a; art. 7 pkt 4,5,6,7; art. 12a; art. 13 ust. 2; art. 14, art. 15 ust.1, art. 18 ust. 1; art. 22 a; art. 23 ust. 1 pkt 2,3,5; art. 24 ust. 1 pkt 3; art. 25 ust. 1 pkt 4, ust. 2 pkt 2,4,5; art. 29 ust. 1; art. 30 pkt 2; art. 31ust. 3,5; art. 31 a; art. 32 ust. 1 pkt 5a, art. 33 ust. 1, rozdział 5: art. 36,37,38,39,39a; art. 41 ust. 1 pkt 2,3,3a,6,7, ust. 2; art. 42 ust. 1,3,4; art. 43 ust. 1 pkt 3,4; art. 44 ust. 1 pkt 3, ust. 2,3; art. 44a; art. 45; art. 46; art. 46a; rozdział 7: tytuł; art. 47 ust. 1, 3; art. 48.

[472] Projektowano zmiany 14 artykułów, w tym: art. 2 ust. 2, art. 3, dodanie do art. 7 pkt 6 i 7, zmiany art. 23 ust. 1, art. 24 pkt 3 i art. 25 pkt 4, art. 30 pkt 2 i dodanie do art. 32 pkt 5a oraz zmiany art. 48.Zmiany w art. 41-44 dotyczące rejestracji zbiorów danych osobowych, określono jako porządkujące i uzupełniające obowiązujące przepisy w celu zapewnienia pełnej zgodności ustawy z dyrektywą. Zob. X. Konarski, G. Sibiga, *Zmiany w ustawie o ochronie danych osobowych w świetle Dyrektywy 95/46/WE*, „Monitor Prawniczy" 2004, nr 12, s. 548-555.

[473] Uzasadnienie projektu ustawy o zmianie ustawy o ochronie danych osobowych wraz z projektem podstawowego aktu wykonawczego z 16.10.2003 r., druk nr 2120/IV, s. 12.

[474] Dz. U. Nr 73, poz.464 z późn. zm. Po wejściu w życie nowelizacji z 2004 r. obowiązywało tylko jedno z 3 dotychczasowych rozporządzeń wykonawczych.

[475] Dz. U. Nr 25, poz. 219.

[476] Dz. U. Nr 104, poz. 708.

Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Centralne Biuro Abtykorupcyjne oraz Wojskowe Służby Informacyjne.

Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej i ustawy o ochronie danych osobowych[477] wprowadziła nowe brzmienie art. 43 w ust.1 pkt 2b u.o.d.o.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[478] także spowodowała zmiany w u.o.d.o., m. in. w: art. 30 pkt 1, art. 32 ust. 1 pkt 4 oraz art. 43 ust. 1 pkt 1 u.o.d.o.

W 2010 r. miała miejsce trzecia co do wielkości nowelizacja u.o.d.o., dokonana ustawą z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych[479]. W wyniku tych zmian wprowadzono do u.o.d.o. 8 nowych przepisów (art. 13 ust. 1a, art. 15 ust. 3, art. 15 ust. 4, art. 16 ust. 1a, art. 41 ust. 3, art. 41 ust. 4, art. 54a u.o.d.o.), zmieniono też dotychczasowe brzmienie 8 przepisów (art. 7 pkt 5, art. 12, art. 13 ust. 3, art. 33 ust. 1, art. 34, art. 41 ust. 1 pkt 2, art. 41 ust. 2, art. 44 ust. 1 pkt 2 u.o.d.o.) oraz uchylono 3 przepisy (art. 29, art. 30 i art. 50 u.o.d.o.)[480]. Ustawa zmieniająca u.o.d.o. wprowadziła sześć zasadniczych obszarów zmian. Niewątpliwie najwięcej zmian odniosło się do uprawnień, organizacji biura, procedur kontrolnych Generalnego Inspektora oraz prawnokarnej ochrony inspektorów GIODO. Najważniejszą jednak ze wskazanych zmian było wyposażenie GIODO w uprawnienia egzekucyjne. Kolejne zmiany w u.o.d.o. dotyczyły: uchylenia przepisów dotyczących udostępniania danych (art. 29 i art. 30 u.o.d.o.), wprowadzenia przepisu wyraźnie przewidującego możliwość odwołania zgody, zmian w zakresie rejestracji zbiorów danych osobowych[481] oraz zmian dotyczących odpowiedzialności karnej[482].

Oprócz zmian z samej ustawie o ochronie danych osobowych, omawiana nowelizacja wprowadziła zmiany jeszcze w trzech innych regulacjach ustawowych związanych z zagadnieniami z zakresu ochrony danych osobowych. Pierwszą ze znowelizowanych ustaw szczególnych była ustawa z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w

---

[477] Dz. U. Nr 41, poz. 233.
[478] Dz. U. Nr 182, poz. 1228.
[479] Dz. U. Nr 229, poz. 1497.
[480] P. Fajgielski, *Nowelizacja ustawy o ochronie danych osobowych - zakładane cele i przewidywane skutki*, „Ochrona danych osobowych. Dodatek do Monitora Prawniczego" 2011, nr 3, s. 2.
[481] Pierwsza zmiana dotyczyła sprecyzowania i poszerzenia zakresu danych zawartych w zgłoszeniu rejestracyjnym - art. 41 ust. 1 pkt 2 u.o.d.o.), druga zmiana dotyczyła zgłoszenia rozszerzenia zakresu danych przetwarzanych w zbiorze o dane sensytywne (art. 41 ust. 4 u.o.d.o.), trzecia zmiana obejmowała zmodyfikowanie jednej z przesłanek odmowy rejestracji zbioru (art. 44 ust. 1 pkt 2 u.o.d.o.).
[482] Uchylono art. 50 u.o.d.o. dotyczący odpowiedzialności karnej za przechowywanie danych w zbiorze niezgodnie z celem utworzenia zbioru oraz wprowadzono nowy art. 54a u.o.d.o. przewidujący odpowiedzialność karną za udaremnianie lub utrudnianie inspektorom wykonania czynności kontrolnych.

administracji[483], a zmiany dotyczyły rozszerzenia zakresu egzekucji administracyjnej o obowiązki nakładane w drodze decyzji przez Generalnego Inspektora. Drugą zmienioną ustawą była ustawa z 24 maja 2000 r. o Krajowym Rejestrze Karnym[484]., w której przepisach dopuszczono możliwość przetwarzania danych zawartych w Krajowym Rejestrze karnym do celów statystycznych i badań naukowych, a dane o karalności zaliczono do danych sensytywnych, stąd podstawa przetwarzania takiej kategorii danych powinna być ustawa Trzecią ustawą zmienioną na skutek nowelizacji była ustawa z 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych[485], w której wskazano przepisy u.o.d.o. mające zastosowanie w zakresie gromadzenia, przetwarzania i udostępniania informacji kryminalnych.

Istotna nowelizacja ustawy o ochronie danych osobowych miała również miejsce 31 grudnia 2011 r., a dotyczyła ona danych przedsiębiorcy. Wtedy to stracił moc art. 7a ust. 2 ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej[486], który stanowił, że „ewidencja działalności gospodarczej jest jawna i dane osobowe w niej zawarte nie podlegają przepisom ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych". Uwzględniając obowiązujący wówczas stan prawny, NSA słusznie stwierdził w swym wyroku z 15 marca 2010 r., że „ustawie o ochronie danych osobowych nie podlegają tylko dane wpisane do ewidencji działalności gospodarczej. Pozostałe zaś informacje o osobie fizycznej prowadzącej działalność gospodarczą takim wyłączeniom już nie podlegają (…) Po wyrejestrowaniu działalności gospodarczej przedsiębiorca staje się obiektywnie osobą nieprowadzącą działalności gospodarczej. Jego dane osobowe z dniem wykreślenia działalności z ewidencji działalności gospodarczej podlegają zatem pełnej ochronie zagwarantowanej ustawą o ochronie danych osobowych[487]. Od 1 stycznia 2012 r. dane osobowe przedsiębiorców, informacje identyfikujące przedsiębiorców w obrocie gospodarczym (o ile – dla konkretnego stanu faktycznego – będą stanowiły dane osobowe w rozumieniu art. 6 u.o.d.o.) zostały zatem włączone pod ochronę ustawy o ochronie danych osobowych. Konsekwencją tej nowelizacji jest obowiązek rejestracji zbiorów danych osobowych przez administratorów danych

[483] Dz. U. Nr 24, poz. 151 z późn. zm.
[484] Dz. U. Nr 50, poz. 580 z późn. zm.; P. Fajgielski, *Nowelizacja…*, s. 5.
[485] Dz. U. Nr 110, poz. 1189 z późn. zm.; Taka konstrukcja prawna oznacza wyłączenie w stosowaniu pozostałych przepisów u.o.d.o. w stosunku do działalności będącej przedmiotem regulacji zmienionej w ten sposób ustawy. Zob. P. Fajgielski, *Nowelizacja…*, s. 5.
[486] Dz. U. Nr 101, poz. 1178 z późn. zm.
[487] Wyrok NSA z dnia 15 marca 2010 r., I OSK 756/09; wyrok dostępny pod adresem: http://orzeczenia.nsa.gov.pl/doc/B0AA.

osobowych dotyczących przedsiębiorców, w których są dane przedsiębiorców, jeżeli zbiór nie podlega przesłankom do zwolnienia z takiej rejestracji na podstawie art. 43 ust. 1 u.o.d.o[488].

Od 1 stycznia 2015 r. na mocy art. 9 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[489], obowiązują zmiany przepisów w u.o.d.o. dotyczące m.in. funkcjonowania administratora bezpieczeństwa informacji (o czym szerzej w rozdziale V pracy). Zgodnie z treścią art. 46b u.o.d.o. administrator danych jest obowiązany zgłosić do rejestracji GIODO także powołanie i odwołanie administratora bezpieczeństwa informacji (ABI). Omawiane zmiany w przepisach przewidują także zwolnienie z obowiązku rejestracji u Generalnego Inspektora tych zbiorów danych, które nie są prowadzone z wykorzystaniem systemów informatycznych (zbiory danych prowadzone wyłącznie w formie papierowej), z wyjątkiem gdy w zbiorze przetwarzane są tzw. dane szczególnie chronione, o których mowa w art. 27 ust. 1 ustawy (art. 43 ust.1 pkt 12 u.o.d.o.).

Ostatnia jak dotąd nowelizacja u.o.d.o. miała miejsce 1 kwietnia 2016 r., kiedy weszła w życie ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci[490]. Na mocy art. 38 pkt 1 tej ustawy wprowadzono istotne zmiany w przepisach ustawy o ochronie danych osobowych dotyczące administratora danych oraz instytucji powierzenia przetwarzania danych.

Wprowadzane nowelizacje, czy to związane ze zmianami ustrojowymi w Polsce czy dokonywane w związku z integracją europejską, powodowały znaczne trudności z recepcją kolejnych nowych norm przez ich adresatów i obniżały „skuteczność komunikacyjną prawa"[491]. Z punktu widzenia ustawodawcy pozwoliły na chociażby częściowe osiągnięcie zakładanego przez projektodawców celu w postaci poprawy skuteczności przepisów o ochronie danych osobowych. Wszystkie nowelizacje miały jednak na celu wyeliminowanie nieprawidłowych i wadliwie działających konstrukcji prawnych, tak by doprecyzować działania mechanizmów ochronnych i ułatwić w praktyce stosowanie przepisów ustawy. Należy także pamiętać, że uchwalona w 1997 r. u.o.d.o. była pierwszą i wręcz eksperymentalną tego typu ustawą w polskim systemie prawa. Nie powinny zatem dziwić wprowadzane zmiany, czy to w kontekście dostosowania polskiej regulacji do wymogów unijnych, czy to korekty ustawodawcy w zakresie obowiązywania ustawy. Wszelkie

---

[488] Zob. E. Kuczma, *Ochrona danych osobowych przez przedsiębiorcę*, [w:] *Przedsiębiorca w społecznej gospodarce rynkowej*, red. T. Kocowski, J. Gola, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", Wrocław 2014, nr 372, s. 210 i n.
[489] Dz. U. poz. 1662.
[490] Dz. U. poz. 195.
[491] G. Szpor, *Uwarunkowania…,* s. 36.

nowelizacje należałoby przyjąć jako naturalny proces adaptacyjny tego zakresu regulacji w ramach polskiego porządku prawnego.

b) zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych

Wpływ przedstawianych czynników zaowocował finalnie wprowadzeniem do polskiego porządku prawnego pierwszego aktu prawnego szczegółowo regulującego materię informacji o charakterze osobowym. Prawo do ochrony informacji osobowych zostało przyznane każdemu, przy czym prawem tym objęte są tylko osoby fizyczne. Ustawa nałożyła określone obowiązki na administratorów danych wynikające z przetwarzania danych osobowych, konkretyzując szereg niedookreślonych dotąd pojęć i zjawisk związanych z szerokim zagadnieniem ochrony danych osobowych. Ideą przyświecającą twórcom tejże ustawy było także, aby każdy administrator tych danych wdrożył w swojej organizacji system ich ochrony zapewniający legalne i bezpieczne przetwarzanie danych.

Wprowadzone na mocy tej ustawy normy prawne mają za zadanie ochronę prawa do prywatności jednostki, przy jednoczesnym zapewnieniu zainteresowanym jednostkom dostępu do informacji, jakie na ich temat posiadają podmioty zajmujące się przetwarzaniem danych osobowych[492]. Ustawa stanowi zamkniętą całość i zapoczątkowała późniejsze procesy wdrażania i przestrzegania ustanowionych standardów, jakie narzuciła wszystkim podmiotom, objętym swoim zasięgiem. Od chwili jej wejścia w życie zostały ujednolicone zasady w zakresie przetwarzania i ochrony danych osobowych w Polsce.

U.o.d.o. normuje następujące rodzaje spraw: zasady i tryb postępowania przy przetwarzaniu danych osobowych (materia proceduralna), prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych (prawo materialne), a także zakres działania oraz zasady organizacji i funkcjonowania organu do ochrony danych osobowych (materia ustrojowa), gdyż ustawodawca stworzył instytucjonalne gwarancje mające zapewnić ich przestrzeganie w postaci powołania odrębnego organu Generalnego Inspektora Ochrony Danych Osobowych. Ponadto, w stosunku do osób, które dopuszczą się naruszenia przepisów ustawy o ochronie danych osobowych (m. in. administratorzy danych), w ustawie przewidziano odpowiedzialność cywilną za szkody wynikłe z ich zachowania lub zaniechania, a odpowiedzialność ta dodatkowo została wsparta przepisami karnymi, także zawartymi w samej ustawie (art. 49 - art. 54 u.o.d.o.). Wszystkie czyny naruszające przepisy

[492] B. Banaszak, K. Wygoda, *op. cit.,* s. 53.

ustawy zostały uznane za przestępstwo i podlegają ściganiu z urzędu. Z zakresu obowiązywania ustawy wyłączone są jednak niektóre zagadnienia, dlatego u.o.d.o. nie reguluje problematyki ochrony danych osobowych kompleksowo.

Ustawa o ochronie danych osobowych realizując wymagania stawiane przez Wspólnotę Europejską, skonkretyzowała konstytucyjnie zagwarantowane prawo do decydowania o tym komu, w jakim zakresie i w jakim celu przekazywane są dane, dając ustawowe gwarancje przestrzegania tego prawa, poprzez wyposażenie tych osób, których dane dotyczą w środki służące realizacji tego prawa, a odpowiednie organy i służby w środki prawne, gwarantujące jego przestrzeganie. Choć niejednokrotnie jednostka nie ma żadnego wpływu na to, czy i jakie dane jej dotyczące są przetwarzane, to może jednak czuwać nad tym, by zbierane przez organ władzy publicznej dane były merytorycznie poprawne i adekwatne do celu, dla którego zostały zebrane[493]. Każda jednostka zatem na mocy ustawy posiada prawo do ochrony dotyczących jej danych.

Ustawa daje obywatelom możliwość skorzystania z prawa do formalnej kontroli przetwarzania dotyczących ich danych, które ustanowione zostało w rozdziale 4 ustawy. Mogą oni domagać się również: uzyskania informacji czy zbiór danych istnieje, ustalenia administratora danych, adresu jego siedziby, uzyskania informacji o celu, zakresie i sposobie przetwarzania danych oraz informacji o źródle, z którego pochodzą, żądania uzupełnienia, uaktualnienia, sprostowania, a nawet czasowego lub stałego wstrzymania przetwarzania danych, jeżeli są one nieaktualne, niekompletne, nieprawdziwe lub zostały zebrane z naruszeniem prawa albo są już zbędne do realizacji celu, dla którego były zebrane[494]. U.o.d.o przyznaje obywatelom także prawo do sprzeciwu, gdy administrator przetwarza dane w celach innych niż te, dla których były zbierane lub przekazuje je innemu administratorowi danych. W takiej sytuacji przysługuje im prawo żądania od administratora danych odpowiedniego zachowania się w przypadku nieprzestrzegania ustawy, a także prawo występowania do Generalnego Inspektora Ochrony Danych Osobowych, organów ścigania oraz wymiaru sprawiedliwości w sprawach naruszenia przepisów o ochronie danych osobowych[495].

Osoby, których dane dotyczą, zostały wyposażone w instrumenty kontroli procesu przetwarzania ich danych osobowych, zaś na administratorów nałożono konkretne obowiązki. Z jednej strony chodziło o zapewnienie prawa do prywatności, zaś z drugiej strony

---

[493] *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 1999*, s. 12.
[494] *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2011*, s. 13.
[495] *Ibidem*, s. 13.

wyposażono podmioty w prawo do informacji o osobie, której dane dotyczą. Taka regulacja wprowadziła swoiste balansowanie interesów, co zaowocowało na przestrzeni czasu rozbieżnością stanowisk w doktrynie oraz niejednolitość orzecznictwa sądowo-administracyjnego w sprawach z zakresu ochrony danych osobowych[496].

Opisywany akt prawny reguluje ponadto podstawowe zasady dotyczące przetwarzania danych osobowych (art. 2), jednak nie jest to określenie wyczerpujące. Poza zasadami postępowania przy przetwarzaniu danych osobowych i prawami osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych, u.o.d.o. reguluje status organu ochrony danych osobowych. Zwrot „zasady postępowania przy przetwarzaniu danych osobowych"[497] oznacza przede wszystkim obowiązki administratora danych i innych podmiotów związanych z przetwarzaniem, ale również i inne obowiązki niż tylko wskazane w rozdziale 3 ustawy o ochronie danych osobowych zatytułowanym „Zasady przetwarzana danych osobowych"[498].

Ustawa ma charakter subsydiarny, gdyż jej przepisów nie stosuje się, jeżeli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej (art. 4 u.o.d.o). Należy to rozumieć, że przepisów ustawy nie stosuje się w zakresie, w jakim konwencja międzynarodowa, wiążąca RP, zawiera postanowienia odmienne; nie ma przy tym znaczenia, czy są to postanowienia surowsze, czy bardziej liberalne od postanowień ustawy[499].

Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idąca ochronę niż wynika to z przepisów omawianej ustawy, to stosuje się przepisy tych ustaw (art. 5 u.o.d.o). Jak słusznie zauważył A. Drozd, „art. 5 jest przykładem normy kolizyjnej i artykuł ten może być rozumiany przynajmniej dwojako. Jego zakresem zastosowania mogą być objęte wszystkie przepisy przewidujące dalej idącą ochronę danych osobowych niż wynikającą z ustawy lub tylko przepisy przewidujące dalej idącą ochronę danych osobowych, które odnoszą się do ich przetwarzania"[500]. Właściwa jest druga interpretacja, gdyż potrzeba zastosowania omawianej normy kolizyjnej występuje tylko wtedy, gdy dochodzi do kolizji przepisów prawnych wprowadzających odmienne unormowania[501].

---

[496] G. Szpor, *Uwarunkowania…*, s. 36.
[497] Zasad tych nie można utożsamiać z zasadami prawa w znaczeniu wskazanym w teorii prawa. Por. S. Wronkowska, M. Zieliński, Z. Ziembiński, *Zasady prawa. Zagadnienia podstawowe*, Warszawa 1974, s. 74 i n.
[498] A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2008, s. 18.
[499] *Ibidem*, s. 21.
[500] A. Drozd, *Ustawa…*, s. 36-37.
[501] J. Nowacki, Z. Tabor, *Wstęp do prawoznawstwa*, Kraków 2002, s. 179 i 183.

J. Barta i R. Markiewicz poddali gruntownej ocenie i analizie prawo do ochrony danych osobowych. Na mocy oceny jego treści, przedmiotu i charakteru za autorami można zatem wyróżnić dwa aspekty prawa do ochrony danych osobowych: prywatnoprawny i publicznoprawny.

Aspekt prywatnoprawny to emocjonalny, osobisty stosunek występujący między osobą fizyczną a dotyczącymi jej danymi. Może być on traktowany jako dobro osobiste w postaci autonomii informacyjnej człowieka (każde więc posłużenie się danymi przez osobę trzecią bez zgody zainteresowanego narusza ten stosunek lub powoduje „zakłócanie spokoju psychicznego"), w kategoriach własnościowych (człowiek jest właścicielem informacji, które go dotyczą) lub w ujęciu złagodzonym (osoba sprawuje władztwo nad dotyczącymi jej danymi)[502]. Ta konstrukcja komponuje się z cywilnym prawem do ochrony danych, będącym swoistym dobrem niematerialnym, ściśle związanym z osobą, na którym wsparta może zostać konstrukcja roszczeń w przypadku wystąpienia zdarzenia o charakterze deliktowym[503]. Właściciel danych dysponuje więc prawem dostępu do swoich danych (art. 24 ust. 1 pkt 3 u.o.d.o), posiada prawo modyfikacji danych wraz z prawem usunięcia ich ze zbioru (art. 35 u.o.d.o) czy zaprzestania przetwarzania ze względu na szczególne okoliczności (art. 32 ust. 1 pkt 7-8 u.o.d.o), a także ma prawo sprawowania kontroli nad przestrzeganiem swoich danych osobowych poprzez spełnienie obowiązku informacyjnego[504].

Aspekt publicznoprawny wyraża się w poddaniu przetwarzania danych osobowych publicznoprawnej ocenie i regulacji[505]. Wynika z tego także obowiązek właściwego zabezpieczenia tego prawa, a realizację zapewnia się poprzez zagrożenie sankcjami karnymi[506].

Prawo ochrony danych osobowych może być ponadto rozumiane w znaczeniu podmiotowym i przedmiotowym.

Przepisy regulujące zakres podmiotowy mają szczególne znaczenie dla stosowania każdego aktu normatywnego, gdyż wyznaczają krąg podmiotów, do których odnoszą się uprawnienia i obowiązki wynikające z tego aktu[507]. Art. 1 ust. 1 u.o.d.o wskazuje, iż „każdy

---

[502] J. Barta, M. Markiewicz, *op. cit.,* s. 245-246.
[503] M. Polok, *op. cit.*, s. 157.
[504] *Ibidem*, s. 157.
[505] J. Barta, M. Markiewicz, *op. cit.*, s. 245-246.
[506] M. Polok, *op. cit.*, s. 158.
[507] Zob. A. Krasuski, Zakres *podmiotowy ustawy o ochronie danych osobowych - uwagi de lege lata i de lege ferenda*, [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008, s. 37.

ma prawo do ochrony dotyczących go danych osobowych". Tak zatem prawo do ochrony danych osobowych wynikające z art. 1 u.o.d.o. jest immanentnym prawem każdej osoby[508]. Przepis ten w ust. 1 wyraża jedną z naczelnych zasad leżących u podstaw ustawy o ochronie danych osobowych i przyznaje prawo do ochrony każdemu. Tak szeroko określony zakres ochrony skonkretyzowany został w rozdziale 4 ustawy („Prawa osoby, której dane dotyczą"), z którego wynika prawo dostępu do zbiorów danych i prawo to przyjmuje konkretny kształt w postaci odpowiednich uprawnień lub żądań.

Treść art. 1 w powiązaniu z innymi przepisami przedmiotowej ustawy, a zwłaszcza z art. 6, pojęcie „każdy" nakazuje interpretować jako „każda osoba fizyczna"[509]. Co prawda, nie zostało to w sposób dostateczny sprecyzowane, jednak chodzi tu o każdą jednostkę fizyczną, a nie jakikolwiek podmiot prawa[510]. Wobec tego prawo do ochrony danych osobowych ma charakter powszechny[511]. Takie ujęcie zapewnia m. in. roszczenia wobec podmiotów przetwarzających jego dane osobowe, aby przetwarzanie odbywało się w zgodzie z obowiązującymi prawnymi wymogami przetwarzania danych z poszanowaniem prawa do prywatności tej osoby[512].

Zakres zastosowania art. 1 ust. 1 obejmuje nie tylko relacje jednostka - władza publiczna, lecz również stosunki prywatnoprawne[513]. Interpretacji tego artykuły nie sposób dokonać bez uwzględnienia treści art. 6 u.o.d.o. Skoro pojęcie danych osobowych obejmuje tylko informacje o osobach fizycznych, to prawo do ochrony danych osobowych przyznane zostało nie każdemu podmiotowi prawa, lecz tylko każdej osobie fizycznej[514]. Takie ujęcie zakresu podmiotowego prawa do ochrony danych osobowych jest zgodne z Konstytucją RP, a występujące w art. 51 ust. 1 i 3 zwroty: „informacji dotyczących jego osoby", czy „dotyczących go dokumentów i zbiorów danych" rozumiane są jako odnoszące się jedynie do osób fizycznych[515]. Jest to uzasadnione ze względu na ścisły związek prawa do ochrony danych osobowych z gwarantowanym w art. 47 Konstytucji RP prawem do prywatności, które przysługuje wyłącznie jednostce a nie innym podmiotom prawa[516].

---

[508] R. Szałowski, *Ochrona danych osobowych. Komentarz do ustawy z 29.08.1997*, Zielona Góra 2000, s. 12.
[509] A. Szewc, *Z problematyki*…, cz. I, „Radca Prawny" 1999, nr 4, s. 27.
[510] Por. wyrok NSA w Warszawie z dnia 28 listopada 2002 r., II SA 3389/01, LEX nr 241604.
[511] A. Szewc, *Z problematyki*…, cz. I, „Radca Prawny" 1999, nr 4, s. 27.
[512] M. Polok, *op. cit.*, s. 157.
[513] A. Drozd, *Ustawa…*, s. 14.
[514] M. Jabłoński, K. Wygoda, *Zasady ochrony danych osobowych*, [w:] *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, red. J. Kołaczyński, Warszawa 2003, s. 129.
[515] I. Lipowicz, *Teza…*, s. 100.
[516] Stanowisko to jest uzasadnione także brzmieniem pkt 24 preambuły dyrektywy 95/46/WE.

W ustawie o ochronie danych osobowych zakres podmiotowy określony został również w art. 3 i w art. 3a ust. 1. Zgodnie z treścią art. 3 u.o.d.o, zakres podmiotowy ustawy obejmuje organy państwowe, samorządu terytorialnego, państwowe i komunalne jednostki organizacyjne oraz podmioty niepaństwowe, jeżeli realizują zadania publiczne. Oprócz tego zakresem podmiotowym obowiązywania ustawy zostały objęte osoby prawne, jednostki organizacyjne niemające osobowości prawnej, osoby fizyczne, o ile wykonują na danych osobowych operacje inne niż w celach domowych i prywatnych (art. 3a u.o.d.o.), operujące na danych osobowych w związku z realizacją celów statutowych, działalnością zarobkową czy zawodową. Przedstawione podmioty, o ile decydują o celach i środkach przetwarzania danych osobowych, zgodnie z art. 7 pkt 4 ustawy spełniają kryteria administratora danych.

W pierwszej kolejności zostały wymienione organy państwowe, jednak ustawa nie zawęża tego pojęcia. Stosuje się ją zatem względem wszelkich organów państwowych, zarówno centralnych, jak i lokalnych. Drugą kategoria podmiotów są wszystkie organy samorządu terytorialnego, ponieważ w u.o.d.o. brak jest wyłączeń podmiotowych w tym zakresie.

Zakres podmiotowy ustawy obejmuje więc podmioty publiczne: organy państwowe, organy samorządu terytorialnego i państwowe i komunalne jednostki organizacyjne (np. miejskie zakłady oczyszczania, miejskie zakłady komunikacji).

Ponadto stosowanie u.o.d.o. obejmuje także podmioty prywatne, tj. podmioty wymienione w art. 3 ust. 2 pkt 1 i 2 - osoby fizyczne (bez względu na narodowość, obywatelstwo, wiek i zdolność do czynności prawnych) i osoby prawne (np. spółdzielnie, fundacje, stowarzyszenia) oraz jednostki organizacyjne niemające osobowości prawnej (np. nieposiadające osobowości prawnej spółki prawa handlowego), które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych, przy czym, aby podlegać ustawie wystarczy, by podmioty te miały siedzibę lub miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej albo w państwie trzecim[517], ewentualnie (jeśliby nie spełniały tego warunku) przetwarzały dane wykorzystując środki techniczne znajdujące się na obszarze RP. Ustawę stosuje się przy spełnieniu łącznie dwóch wskazanych powyżej przesłanek oraz wyłącznie względem podmiotów prywatnych

[517]Art. 7 u.o.d.o definiuje „państwo trzecie" jako państwo nienależące do Europejskiego Obszaru Gospodarczego (EOG). W konsekwencji art. 3 ust. 2 nie obejmuje podmiotów mających siedzibę (miejsce zamieszkania) na terytorium państw innych niż Polska i nienależących do EOG, dlatego u.o.d.o stosuje się do podmiotów prywatnych mających siedzibę (miejsce zamieszkania) na terytorium państwa należącego do EOG, gdyż należy je traktować tak jak podmioty mające siedzibę (miejsce zamieszkania) na terytorium Polski. Zob. A. Drozd, *Ustawa…*s. 27.

(podmiotów niepublicznych realizujących zadania publiczne). Określona przesłanka posiadania siedziby (miejsca zamieszkania[518]) na terytorium Polski dotyczy pomiotu będącego administratorem danych, a nie innego podmiotu, do którego stosuje się ustawę o.d.o. (wniosek ten jest uzasadniony brzmieniem art. 7 pkt 4, który wiąże status administratora wyłącznie z podmiotami wskazanymi w art. 3 u.o.d.o.)[519]. W piśmiennictwie wskazuje się ponadto, że nawet wtedy gdy siedziba (miejsce zamieszkania) administratora danych znajduje się na terytorium Polski, a faktycznie nie przetwarza on danych osobowych na tym terytorium (w tym za pośrednictwem innych podmiotów), to u.o.d.o. nie znajduje zastosowania[520]. Powyższe stanowisko jest zgodne z art. 3 ust. 2 i Dyrektywy 95/46/WE[521]. Co więcej, na skutek przyjęcia kryterium prawa siedziby czy miejsca zamieszkania (*lex sitae; lex domicili*) na określenie zastosowania ustawy, w świetle literalnego brzmienia art. 3, ustawa znajdzie zastosowanie także do administratorów danych mających miejsce zamieszkania lub siedzibę w Polsce lub w państwie trzecim, tj. poza Europejskim Obszarem Gospodarczym (EOG), a tym samym poza obszarem Unii Europejskiej.

Biorąc pod uwagę podmioty przetwarzające dane osobowe należy wyprowadzić wniosek, iż ustawowe regulacje dotyczące zawartych w niej praw i obowiązków stosuje się, zgodnie z treścią art. 3 u.o.d.o., do organów państwowych oraz samorządu terytorialnego, a także do innych państwowych i komunalnych jednostek organizacyjnych oraz podmiotów niepaństwowych realizujących zadania publiczne. Zatem art. 3 ust. 1 dotyczy podmiotów o charakterze publicznym, zaś art. 3 ust. 2 podmiotów o charakterze niepublicznym. Wskazane rozróżnienie ma w zasadzie charakter techniczny, gdyż u.o.d.o. nie nakłada rozbieżnych zasad czy obowiązków w zależności od charakteru ustrojowego administratora danych[522]. Takie szerokie określenie kręgów podmiotów podlegających ustawie pozwala na objęcie jej przepisami w zasadzie wszystkich zainteresowanych, którzy mogą mieć styczność z procesem przetwarzania danych osobowych od strony administrowania tymi zbiorami, z uwzględnieniem ustawowych wyjątków (art. 43 u.o.d.o). Można by także wyprowadzić wniosek, iż *a contrario* podmioty nie wymienione w treści art. 3 u.o.d.o nie mają obowiązku stosowania się do przepisów omawianej ustawy.

---

[518] Pojęcie siedziba i miejsce zamieszkania jest właściwe prawu cywilnemu, dlatego ich znaczenie na gruncie u.o.d.o trzeba ustalić na postawie przepisów Kodeksu cywilnego.
[519] A. Drozd, *Ustawa…*, s. 27.
[520] X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 156.
[521] A. Drozd, *Ustawa…*, s. 28.
[522] Jedynym wyjątkiem jest art. 25 ust. 2 pkt 5 u.o.d.o. Jest to przepis, który rozróżniając sektory, w których działają określone w nim podmioty stanowi nawiązanie do art. 2 pkt d Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady.

Pewnym rodzajem wyjątku od ogólnych zasad wymienionych w art. 3 u.o.d.o. jest art. 3a ust. 1 u.o.d.o, który wyłącza możliwość stosowania zasad przetwarzania danych osobowych regulowanych tą ustawą do określonego kręgu podmiotów, a podstawy wyłączenia mają przy tym odmienne od siebie *ratio legis*[523].

Ustawa nie ma zastosowania, zgodnie z treścią art. 3a ust. 1 u.o.d.o., w przypadku osób nieżyjących - ze względu na ochronę powszechnych dóbr osobistych (kult pamięci osoby zmarłej) [524], osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych[525], podmiotów mających siedzibę albo miejsca zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych (art. 3a ust. 1 pkt 2 u.o.d.o.) oraz do administratorów danych z siedzibą w Unii Europejskiej, nawet wówczas, gdy podmioty te będą przetwarzać dane przy użyciu środków technicznych znajdujących się w Polsce (w tym przypadku prawem właściwym będzie prawo obowiązujące w państwie członkowskim, w którym siedzibę ma administrator danych)[526] oraz osób fizycznych, które wykorzystują dane wyłącznie w celach osobistych lub domowych[527] (art. 3a ust. 1 pkt 1 u.o.d.o.).

Art. 3a ust. 2 u.o.d.o wprowadza kolejny rodzaj wyłączenia z zakresu stosowania u.o.d.o. i dotyczy on trzech obszarów działalności, tj. prasowej działalności dziennikarskiej[528]. (w rozumieniu prawa prasowego), działalności literackiej i działalności artystycznej[529]. Wyłączenie nie ma charakteru bezwzględnego, gdyż doznaje ograniczenia w obliczu istotnego naruszenia praw i wolności osoby, której dane dotyczą i nie będzie miało także zastosowania do czynności Generalnego Inspektora Ochrony Danych Osobowych

---

[523] I. Zgoliński, I. Zduński, *op. cit.,* s. 30.

[524] Generalny Inspektor Ochrony Danych Osobowych, *ABC wybranych zagadnień z ustawy o ochronie danych osobowych*, Warszawa 2007, s. 10-11.

[525] Także przetwarzanie danych osobowych w związku z działalnością zarobkową niebędącą jednak działalnością gospodarczą może zostać objęte zakresem zastosowania art. 3a ust. 1 pkt 1. Przykładowo przetwarzanie danych osobowych w związku z uczestnictwem w aukcjach elektronicznych, które jest często działalnością zarobkową, należy uznać za przetwarzanie tylko w celach osobistych, jeżeli osoba fizyczna nie uczestniczy w nich w związku z prowadzeniem działalności gospodarczej. Zob. A. Drozd, *Ustawa*…, s. 29.

[526] A. Krasuski, *op. cit*, s. 39.

[527] Należy przez to rozumieć przetwarzanie danych osobowych w ramach wspólnot rodzinnych.

[528] Wyłączenia przewidziane w art. 3a ust. 2 u.o.d.o. dotyczą jedynie celów dziennikarskich, czyli pracy nad publikacją tzw. materiału prasowego. Klauzula prasowa nie obejmuje więc przetwarzania danych osobowych, które jedynie towarzyszy prasowej działalności dziennikarskiej, literackiej lub artystycznej. Zob. A. Młynarska-Sobaczewska, M. Sakowska. *„Klauzula prasowa" z ustawy o ochronie danych osobowych jako gwarancja wolności wypowiedzi*, „Państwo i Prawo" 2005, nr 1, s. 68.

[529] Przez działalność artystyczną lub literacką należy rozumieć w szczególności działalność twórczą będącą przedmiotem prawa autorskiego - Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz. 83 z późn. zm.). Działalność tego typu jest prowadzona też na podstawie ustawy z dnia 30 czerwca 2005 r. o kinematografii (Dz. U. Nr 132, poz. 1111 z późn. zm.), a także w pewnym sensie na podstawie ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz. U. Nr 114, poz. 493 z późn. zm.).

wykonywanych na mocy art. 15 – art. 19 u.o.d.o[530]. Co istotne, do podmiotów prowadzących omawiane rodzaje działalności nie stosuje się przepisów odnoszących się do zabezpieczenia danych osobowych, w tym prowadzenia dokumentacji opisującej sposób przetwarzania danych, wyznaczenia administratora bezpieczeństwa informacji, czy też prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych. Nie znajdują względem nich zastosowania także przepisy definiujące podstawowe pojęcia, w tym administratora danych osobowych. Podmiotom prowadzącym działalność dziennikarską, literacką lub artystyczną nie przysługuje status administratora danych[531].

U.o.d.o, odmiennie niż art. 3 pkt 2 Dyrektywy 95/46/WE, nie wyłącza z zakresu zastosowania przetwarzania danych osobowych związanych z bezpieczeństwem publicznym, obronnością kraju i bezpieczeństwem państwa (w tym także gospodarczym). Wprawdzie ograniczone zostały na mocy ustawy (art. 15 ust. 2, art. 18 ust. 2a i art. 43 ust. 2) uprawnienia Generalnego Inspektora w zakresie kontroli i nadzoru co do administratorów danych działających w dziedzinach związanych z bezpieczeństwem publicznym, obronnością kraju i bezpieczeństwem państwa, lecz ustawa nie przewiduje wyłączenia stosowania wszystkich jej przepisów. Nie oznacza to także, iż do omawianych działań należy stosować wszystkie przepisy u.o.d.o., ponieważ zwykle przepisy ustaw stosowanych względem podmiotów związanych z bezpieczeństwem publicznym, obronnością kraju i bezpieczeństwem państwa stanowią *leges speciales* i wyłączają obowiązywanie przepisów ustawy o ochronie danych osobowych (art. 5 u.o.d.o).

Przepisów ustawy o ochronie danych osobowych nie stosuje się również, jeżeli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej (art. 4 u.o.d.o.)[532]. Komentowany przepis stanowi wyraz prymatu prawa międzynarodowego nad prawem krajowym i jest to jedną z ważniejszych zasad prawnych. U.o.d.o. nie znajduje zatem zastosowania na terytorium Polski w sytuacji, gdy odmienne regulacje przewidziane są w jakiejkolwiek umowie międzynarodowej, której Rzeczpospolita Polska jest stroną. Pomimo iż

---

[530] I. Zgoliński, I. Zduński, *op. cit,* s. 32.
[531] Wyrok SN z dnia 2 października 2006 r., V KK 243/06, OSNKW 2006, nr 12, poz.113.
[532] Kwestię, czy każda umowa międzynarodowa, której strona jest Polska, może wyłączać stosowanie przepisów u.o.d.o., rozstrzyga art. 87 ust. 1 Konstytucji. Należy zatem przyjąć, iż tylko umowy międzynarodowe ratyfikowane za uprzednią zgoda wyrażoną w ustawie są umowami międzynarodowymi w rozumieniu art. 4 u.o.d.o. i mogą wyłączać stosowanie przepisów niniejszej ustawy. Pozostałe ratyfikowane umowy międzynarodowe nie mogą wyłączać stosowania przepisów u.o.d.o, gdyż zgodnie z unormowaniami Konstytucji wyłączenie takie musi nastąpić na podstawie umowy międzynarodowej ratyfikowanej niesamodzielnie przez Prezydenta, lecz za uprzednią zgodą wyrażoną w ustawie. Zob. R. Kwiecień, *Miejsce umów międzynarodowych w porządku prawnym państwa polskiego*, Warszawa 2000, s. 173.

ustawa spełnia standardy europejskie i jest dostosowana do wymogów międzynarodowych, nie oznacza to pełnej harmonizacji i dlatego stosowny przepis umieszczono w jej treści.

Kolejne wyłączenie dotyczy stosowania ustawy w sytuacji, gdy przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ochronę niż wynika to z ustawy o ochronie danych osobowych. Art. 5 u.o.d.o. odnosi się do sytuacji zbiegu przepisów, w przypadku gdy dochodzi do kolizji przepisów prawnych wyłącznie w ramach relacji między u.o.d.o a przepisami zawartymi w innych aktach normatywnych o randze ustawy[533]. Zastosowanie w tym przypadku ma reguła *lex specialis derogat legi generali*. Celem art. 5 jest zapewnienie możliwie najpełniejszej ochrony procesów przetwarzania danych w momencie, gdy inny akt prawny odnosi się do materii ochrony danych osobowych i zawiera sformułowania gwarantujące dalej idącą ochronę niż przewiduje to ustawa o ochronie danych osobowych. Powinno nastąpić więc wyłączenie stosowania u.o.d.o., gdy ustawa ta przewiduje mniejszy zakres ochrony[534].

Zakres przedmiotowy ustawy o ochronie danych osobowych został określony w rozdziale pierwszym ustawy. Regulacje te mają wielopłaszczyznowy charakter, gdyż ustawodawca określił cel wprowadzanych przepisów, relacje zachodzące z innymi aktami prawnymi podejmującymi tę problematykę (w tym z regulacjami prawno-międzynarodowymi) oraz zakres stosowania ustawy[535].

Ustawę stosuje się do przetwarzania danych osobowych w zbiorach prowadzonych w systemie papierowym (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne), w systemach informatycznych, także w przypadku przetwarzania danych osobowych poza zbiorem (art. 2 ust. 2 pkt 1 i 2 u.o.d.o). Ustawa nie ma zatem zastosowania (art. 2 ust. 3 u.o.d.o.) np. w przypadkach przetwarzania danych osobowych w zbiorach doraźnych, tj. tworzonych wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji - wyjątkiem są przepisy dotyczące zabezpieczenia takich zbiorów przez okres ich funkcjonowania (przepisy rozdziału 5 u.o.d.o.).

---

[533] A. Drozd, *Ustawa*…, s. 37.

[534] Zob. wyrok NSA z dnia 26 stycznia 2009 r., I OSK 174/08, LEX nr 478301. Odrębną grupą przepisów, których zakres zastosowania koliduje z zakresem zastosowania u.o.d.o., są m.in. przepisy ustanawiające tajemnice zawodowe i tajemnice prawnie chronione; art. 11 ust. 1 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.); art. 161 ust. 1 i 2, art. 159 ust. 2 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 zpóźn. zm.).; art. 134 ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach (Dz. U. z 2006 r. Nr 234, poz. 1694 z późn. zm.) oraz art. 105 a ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 1997 r. Nr 140, poz. 938. z późn. zm.).

[535] M. Polok, *op. cit.*, s. 156.

Dane osobowe korzystają z ochrony przewidzianej niniejsza ustawą już wówczas, jeżeli tylko mogą znaleźć się w zbiorze danych osobowych, bez względu na to, czy się w nim ostatecznie znalazły, a ustawa w odniesieniu do różnych etapów i rodzajów przetwarzania danych, określa dodatkowe uprawnienia osób, których dane te dotyczą (w rozdziale 4 u.o.d)[536]. Każdy zatem ma prawo do ochrony dotyczących go danych, a nie jedynie ten, czyje dane znalazły się w zbiorze[537].

Treść przetwarzanych danych osobowych jest bez znaczenia i dlatego błahe dane osobowe są również chronione na podstawie tej ustawy[538]. Oczywiście ochrona nie przysługuje osobom fizycznym, gdy przetwarzane informacje nie mają w ogóle charakteru danych osobowych. Kwestia pojedynczych danych, jak i danych występujących „w oderwaniu" nie znajduje natomiast swojego miejsca na gruncie regulacji u.o.d.o. Wyjątkiem jest jedynie regulacja art. 2 ust. 2 pkt 2 u.o.d.o., na podstawie którego ustawę o ochronie danych osobowych stosuje się do przetwarzania danych osobowych w systemach informatycznych także w przypadku przetwarzania danych poza zbiorem danych.

Kluczowe znaczenie dla wskazania przedmiotowego zakresu zastosowania u.o.d.o. posiada również rozstrzygnięcie, czy każda informacja o charakterze osobowym, czy tylko ta, która jest w zbiorze danych, objęta została publicznoprawną ochroną. W doktrynie istnieją dwa zasadniczo skrajne względem siebie stanowiska dotyczące zapewnienia ochrony danych osobowych osoby fizycznej, co znacznie utrudnia bezsprzeczne ustalenie zakresu obowiązywania ustawy o ochronie danych osobowych[539]. Według pierwszego ochrona danych powinna być zapewniona tylko wówczas, gdy dane osobowe są przetwarzane w zbiorach (zbiorach ewidencyjnych, zbiorach danych czy też są zbierane w celu utworzenia jednego z tych zbiorów), a zatem stosowanie u.o.d.o. ograniczone zostaje tylko do sytuacji przetwarzania danych w zbiorach danych[540]. Zgodnie z drugim stanowiskiem, na gruncie ustawy nie rozróżnia się ochrony na dane znajdujące się w specjalnych zbiorach danych oraz dane poza zbiorami, dlatego też u.o.d.o. można stosować w razie przetwarzania danych osobowych w innych postaciach[541]. Na gruncie tego założenia przedmiotem regulacji u.o.d.o.

---

[536] I. Kamińska, *Ochrona danych osobowych. Orzecznictwo sądów administracyjnych*, Warszawa 2007, s. 13.
[537] Postanowienie SN z dnia 11 grudnia 2000 r., II KKN 438/00, OSNKW 2001, nr 3-4, poz. 33.
[538] A. Drozd, *Ustawa…*, s. 15.
[539] M. Sakowska, *Pojęcie „zbiór danych" na gruncie ustawy o ochronie danych osobowych*, „Radca Prawny" 2005, nr 2, s. 62.
[540] Takie stanowisko reprezentują m. in.: B. Banaszak,. K. Wygoda, *Regulacja…*, s. 53; K. Wygoda, *Ochrona…*, s. 407; A. Szewc, *Z problematyki…*, cz. I, „Radca Prawny" 1999, Nr 3, s. 21; A. Mednis, *Ustawa…*, s. 15; Stanowisko to podziela także Generalny Inspektor Ochrony Danych Osobowych.
[541] Różni autorzy różnie jednak określają poszczególne postaci przetwarzania. Zob. A. Drozd, *Zakres zakazu przetwarzania danych osobowych*, „Państwo i Prawo" 2003, nr 2, s. 43-46; I. Zgoliński, I. Zduński, *op. cit.*, s.

jest każde przetwarzanie danych, a nie tylko tych, które znajdują się w zbiorze. Wniosek taki wyprowadzić można z gramatycznej analizy treści art. 2 ust. 1 wskazując, iż ustawodawca określa w nim zasady postępowania przy przetwarzaniu danych osobowych, a nie przetwarzaniu danych osobowych w zbiorze danych. Co więcej, szersze ujmowanie zakresu stosowania przedmiotowej ustawy jest możliwe z uwagi na konstrukcję art. 1 ust. 1, który stanowi, iż każdy ma prawo do ochrony dotyczących go danych osobowych, a art. 1 ust. 2 przewiduje, że ich przetwarzanie może mieć miejsce w ustawowo określonym trybie, ze względu na dobra wskazane w tym przepisie. Na przykład A. Drozd twierdzi, iż ochrona należy się wszystkim danym osobowym, a nie tylko danym występującym w zbiorach. Jego zdaniem u.o.d.o zajmuje się przetwarzaniem danych osobowych w ogóle, a więc również poza zbiorami danych w rozumieniu art. 7 pkt 1 u.o.d.o.[542]. Pogląd ten podziela również D. Fleszer, wskazując, iż ustawodawca definiując zakres stosowania zwrotu „przetwarzanie danych osobowych" nie odniósł się wyłącznie do wykonywania czynności na danych osobowych w zbiorze danych, zatem nieuzasadnione jest według autorki zawężenie stosowania przepisów ustawy o ochronie danych osobowych tylko do przetwarzania danych w zbiorze danych[543]. D. Fleszer zauważa ponadto, że stawianej tezie odpowiada także podejście ustawodawcy w przepisach szczególnych, wskazując jako przykład art. 16 ust. 2 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[544]: „dane osobowe podlegają ochronie […] w zakresie ich przetwarzania niezależnie od tego, czy jest ono dokonywane w zbiorach danych"[545]. Takie stanowisko prezentuje również judykatura. W postanowieniu z 11 grudnia 2000 r. Sąd Najwyższy stwierdził, iż ujęcie danych w zbiorze nie jest warunkiem *sine qua non* ich ochrony[546].

Podzielam tezy przytoczone na poparcie drugiego stanowiska, zgodnie z którym ochrona danych osobowych powinna być zapewniona wszelkim danym osobowym. Moim zdaniem warunek ich przetwarzania w zbiorze dodatkowo tylko powinien wzmacniać konieczność ich ochrony. Ustawodawca w treści art. 2 ust. 1 wskazał, iż „ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych". Użyte

---

17; W. Zimny, *Trudności z terminem „zbiór danych" w ustawie o ochronie danych osobowych*, „Rzeczpospolita" z 6 września 2000 r., nr 208; G. Szpor, *Publicznoprawna…,* s. 11-12; A. Bierć, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce - aspekty cywilnoprawne,* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 114.

[542] A. Drozd, *Zakres…*, s. 43.

[543] D. Fleszer, *op. cit.*, s. 49.

[544] Dz. U. Nr 144, poz. 1204 z późn. zm.

[545] D. Fleszer, *op. cit.*, s. 49.

[546] Postanowienie SN z dnia 11 grudnia 2000 r., II KKN 438/00, OSNKW 2001/3-4/33.

stwierdzenie „mogą być" jednoznacznie wskazuje, iż chodzi o zapewnienie ochrony także tym danym osobowym, które aktualnie nie są, lecz potencjalnie i w przyszłości mogłyby się znaleźć w zbiorze danych. Stosowany zakres ochrony i zasady ich przetwarzania powinny być identyczne względem wszystkich danych osobowych bez względu na fakt ich rzeczywistej obecności w zbiorze danych.

c) pojęcie danych osobowych i ich rodzaje

O obowiązku ochrony danych osobowych możemy mówić w razie łącznego spełnienia określonych warunków. Co najważniejsze, przedmiotowa informacja musi mieć status danych osobowych, a dane osobowe muszą być przetwarzane w odpowiedniej formie. Dane przetwarza jeden z podmiotów zaliczonych do zakresu podmiotowego u.o.d.o., oraz gdy nie zachodzi jedna z przesłanek ograniczenia lub wyłączenia stosowania przedmiotowej ustawy, a także zastosowania ustawy nie wyłączają normy kolizyjne[547]. W przypadku gdy chociażby jeden ze wskazanych warunków nie zostanie spełniony, to podmiot przetwarzający dane osobowe zwolniony jest z obowiązku respektowania publicznoprawnych warunków ochrony danych osobowych.

Pojęcie „danych osobowych" jest kluczowym pojęciem w zakresie prawnej ochrony danych osobowych, nie tylko w odniesieniu do krajowej ustawy o ochronie danych osobowych, ale także w stosunku do wszystkich innych aktów prawnych o zasięgu ponadnarodowym, a także mechanizmów czy instytucji z zakresu ochrony danych osobowych. Punktem wyjścia jest ustalenie, czy charakter informacji, którymi się dysponuje spełnia przesłanki danych osobowych i czy niesie za sobą konieczność stosowania przepisów o ochronie danych osobowych.

W prawie międzynarodowym i w prawie wewnętrznym wielu państw już w latach osiemdziesiątych zdefiniowano pojęcie „dane osobowe". W polskim systemie prawnym pojęcie to pojawiło się po raz pierwszy w rozdziale 8 ustawy z dnia 29 września 1994 r. o rachunkowości[548], gdzie pojęcie „dane" obejmuje także inne informacje niż te, określane mianem „dane osobowe" w rozumieniu u.o.d.o. W art. 5 ustawy z 29 czerwca 1995 r. o statystyce publicznej[549] dane osobowe zdefiniowano jako dane statystyczne od i o osobach fizycznych dotyczące ich życia i sytuacji oraz „dane osobowe wraz z danymi indywidualnymi

[547] T. Szewc, *Publicznoprawna ochrona informacji*, Warszawa 2007, s. 3.
[548] Dz. U. z 1994 r., Nr 121, poz. 591.
[549] Dz. U. z 1995 r. Nr 88, poz. 439.

tzn. dającymi się powiązać z podmiotem gospodarczym albo inną osobą prawną bądź jednostką organizacyjną niemającą osobowości prawnej, tworzą kategorię danych jednostkowych”[550]. Legalna definicja danych osobowych została zawarta jednak dopiero w art. 6 u.o.d.o.

Artykuł 6 wspomnianej ustawy w pierwotnym brzmieniu stanowił, że za dane osobowe uważa się „każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby”[551]. W ramach takiego ujęcia definicji danych osobowych za dane osobowe uznawało się tylko tzw. dane identyfikacyjne[552]. Było to jednak zbyt wąskie określenie, wielokrotnie krytykowane w doktrynie, gdyż przede wszystkim nie było zgodne z prawem wspólnotowym i wytycznymi dyrektywy 95/46/WE[553]. Wskazywano, iż za dane osobowe powinny zostać uznane wszelkie informacje, „jeżeli tylko możliwe jest ich odniesienie do konkretnej osoby”[554]. Postulowano szerokie rozumienie tego określenia, w sposób obejmujący wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

W tym miejscu warto zauważyć, iż według projektu ustawy o ochronie danych osobowych z 13 sierpnia 1996 r.[555] termin „dane osobowe” był inaczej zdefiniowany. W myśl art. 5 projektu, „dane osobowe” to każda informacja dotycząca osoby fizycznej, której tożsamość jest określona lub można ją ustalić na podstawie tej informacji. W odniesieniu do pierwotnej definicji danych osobowych w literaturze przedmiotu pojawiło się wiele słów krytyki. Jak trafnie podnosił A. Mednis, pojęcie danych (informacji) o charakterze osobowym jest centralnym sformułowaniem ustawy, lecz obecna definicja ustawowa, zawarta w art. 6 u.o.d.o., jest błędna[556]. Autor ten zwracał uwagę, że definicja postulowana w projekcie z 1996 r. z nie do końca jasnych powodów została w finalnej fazie prac zmieniona, a zmiana ta spowodowała, zgodnie z literalną interpretacją tekstu, że większość dotyczących człowieka informacji została wyłączona spod ochrony ustawy o ochronie danych osobowych. Ponadto A. Mednis zauważył , że definicja zawarta w niniejszym projekcie nie stawiała wymogu, by z

---

[550] G. Szpor, *Publicznoprawna…,* s. 6.
[551] Treść art. 6 u.o.d.o sprzed nowelizacji w 2001 r. tj. przed wejściem w życie ustawy z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 100, poz. 1087).
[552] W oparciu o pierwotne brzmienie pojęcia dane osobowe Naczelny Sąd Administracyjny w wyroku z dnia 17 listopada 2000 r., II SA 1860/00, uznał, że przedmiotem ochrony ustawy „nie są wszystkie dane o osobach fizycznych, lecz jedynie tzw. dane identyfikujące, a więc imię, nazwisko, adres, PESEL, NIP itp.”.
[553] P. Litwiński, *Ochrona…*, s. 69.
[554] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…,* s. 383- 384.
[555] Uzasadnienie projektu z dnia 13 sierpnia 1996 r. ustawy o ochronie danych osobowych, „Przegląd Rządowy” 1996, Nr 10, s. 85.
[556] Por. A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 21 i n.

danych informacji wynikała tożsamość osoby, ale przede wszystkim kładła nacisk na to, że informacja - aby miała charakter osobowy - powinna dotyczyć osoby, która już znamy na podstawie innych danych.

Nowelizacją u.o.d.o. w 2001 r.[557] ustalono już aktualne brzmienie art. 6 u.o.d.o. Na mocy ustawy przedmiotem ochrony są dane osobowe. Pojęcie danych zdefiniowano w art. 6 u.o.d.o., zgodnie z którym za dane takie uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Obowiązująca definicja danych osobowych jest już w pełni zgodna z wytycznymi prawa europejskiego i nawiązuje do definicji tego pojęcia zawartej w art. 2 pkt. a dyrektywy 95/46/WE, zgodnie z którą za dane osobowe należy uznać wszelkie informacje odnoszące się do oznaczonej lub możliwej do oznaczenia osoby fizycznej (tak w art. 6 ust. 1 u.o.d.o). Za dane w świetle tej definicji uznaje się więc wszelkie informacje, które prowadzą do identyfikacji osoby, której jej dotyczą, i nie są to wyłącznie dane identyfikacyjne[558]. Dane osobopoznawcze także korzystają z ochrony przewidzianej w u.o.d.o.[559]. Tak szerokie rozumienie ustawy pozwala na przyjęcie, iż za dane osobowe uznaje się także wszelkie informacje, które mogą być powiązane z osobą fizyczną, także dane utrwalone jako obraz lub dźwięk, odciski palców, informacje o kodzie genetycznym[560]. Poza tradycyjnym zapisem literalnym, za dane mogą być więc uznane: wizerunek czy głos utrwalone na zdjęciach, kasetach audio i wideo czy urządzeniach dokonujących cyfrowego zapisu.

Aby mówić o danej osobowej, spełnione powinny zostać zatem następujące kryteria: musi dotyczyć osoby fizycznej i być informacją (każdą), a osoba fizyczna musi być zidentyfikowana lub jej tożsamość powinna dać się zidentyfikować w sposób pośredni (art. 6 ust. 1 u.o.d.o). Bez znaczenia będzie sposób przekazania informacji, ważne jest, aby informacja była zrozumiała i mogła zostać zrozumiana przez osoby trzecie. Dane osobowe, jako informacje o osobie mogą być danymi już opublikowanymi lub rozpowszechnionymi (w Internecie, prasie itp.), jak również znajdującymi się w tajnych zbiorach i rejestrach[561].

Co więcej, wątpliwości istnieją także względem danych aktualnych, danych z przeszłości oraz planów na przyszłość osoby fizycznej jako danych osobowych. Ustawa nie

---

[557] Ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 100, poz. 1087).
[558] A. Mednis, *Postulowane zmiany w ustawie o ochronie danych osobowych*, „Ochrona Danych Osobowych. Biuletyn ABI" 2000, nr 3, s. 13.
[559] A. Drozd, *Ochrona…*, s. 43.
[560] Przez dłuższy czas akty prawne wyznaczające standardy z zakresu ochrony danych osobowych nie rozstrzygały tego problemu jednoznacznie, a dopiero dyrektywa 95/46/WE wprowadziła jasność interpretacyjną, że inne typy informacji, jak np. odciski palców czy próbki krwi również stanowią dane osobowe.
[561] Por. M. Brzozowska, *op. cit.*, s. 29.

rozróżnia kategorii informacji na podstawie kryterium ich aktualności. W orzecznictwie wskazuje się, że na tożsamość w rozumieniu u.o.d.o składa się nie tylko to, kim jest obecnie osoba fizyczna (dane aktualne), ale także kim była (dane z przeszłości) oraz nawet co zamierza na przyszłość (dane przyszłe).Wszystko to powoduje, że dana osoba różni się od innej[562].

Objęcie pojęciem „dane osobowe" wszelkich informacji dotyczących zidentyfikowanej lub możliwej do identyfikacji osoby fizycznej wymaga wyjaśnienia znaczenia zwrotu „dane" oraz „informacje".

Pierwszy element zwrotu „dane" nie jest zdefiniowany w aktach prawnych poświęconych ochronie danych osobowych, nie jest też przedmiotem pogłębionych rozważań nauki o ochronie danych osobowych. Termin ten na potrzeby ochrony danych osobowych został zapożyczony z nauk informatycznych, gdzie określenia „dane" używa się do wszelkiego typu jednostkowych znaków, symboli, wzorców czy cech[563] . Na gruncie u.o.d.o. jest on zauważalny głównie w relacji pomiędzy określeniem „dane" i „informacje", kiedy to dwa te terminy w zasadzie stosuje się zamiennie[564]. Pojęcie danych i informacji należy do trudno definiowalnych terminów z uwagi na swój pierwotny charakter.

„Informacja" również nie doczekała się powszechnie akceptowanej i jednoznacznej w nauce definicji[565]. W definicjach słownikowych znajdują się różnorodne ujęcia tego terminu, jak np. „powiadomienie o czymś, zakomunikowanie czegoś, wiadomość, wskazówka, pouczenie"[566] lub też „każdy czynnik, dzięki któremu ludzie lub urządzenia automatyczne mogą bardziej sprawnie, celowo działać"[567]. W literaturze prawniczej pojęcie „informacja" zdefiniowane jest szeroko, z uwzględnieniem potocznego znaczenia tego słowa, a także z uwzględnieniem dodatkowych elementów, jak użytkownik czy cel informacji[568]. Podkreślić należy także deskryptywną funkcję informacji: za informację uznaje się bowiem takie dane,

---

[562] Wyrok WSA w Warszawie z dnia 3 marca 2009 r., sygn. akt II SA/Wa 1495/08, LEX nr 530464.
[563] M. Jagielski, *Prawo…*, s. 41.
[564] Pomimo świadomości pewnej różnicy między nimi, która w praktyce ochrony danych osobowych jest jednak mało znacząca.
[565] Zob. S. Kurek-Kokocińska, *Zagadnienia teoretyczne i uwarunkowania prawne działalności informacyjnej*, Łódź 2004, s. 11.; K. Tarnacka, *Prawo do informacji w polskim prawie konstytucyjnym*, Warszawa 2009, s. 76 i n.
[566] Zob. *Słownik języka polskiego*, M. Szymczak red., tom I, Warszawa 1978, s. 788.
[567] A. Drozd, *Ustawa*…, s. 44.
[568] Zob. W Kilian, [w:] *Prawnicze i ekonomiczne aspekty komunikacji elektronicznej*, red. J. Gołaczyński, Warszawa 2003, s. 14.

które dotyczą pewnego modelu stanowiącego wybrany wycinek świata i jednocześnie model ten opisują[569].

W definicji danych osobowych informacja występuje w tzw. ujęciu datologicznym, polegającym na odwzorowaniu pewnego wycinka rzeczywistości, niezależnie od tego, czy jej odbiorca jest w stanie z niej skorzystać[570]. Jest to przeciwieństwo ujęcia indologicznego uznającego przekaz za informację tylko wtedy, gdy jest ona przydatna odbiorcy, ponieważ nie była mu ona wcześniej znana[571] (śladów tej koncepcji można doszukiwać się w art. 27 ust. 2 pkt 8 u.o.d.o., który zezwala na przetwarzanie danych podanych do publicznej wiadomości osobie, której dane dotyczą)[572]. Dowolność formy sygnału, czyli sposobu przeniesienia informacji, wskazuje, że informacja może mieć charakter językowy (słowny), jak i pozajęzykowy (symboliczny). Istotne dla uznania przekazu za informację jest, by była ona zrozumiała, czyli możliwa do odkodowania.

Informacją w rozumieniu u.o.d.o. są w pierwszej kolejności znaki językowe, gdyż najczęściej ustawa jest stosowana do przetwarzania danych osobowych w formie językowej. Język jest bowiem najbardziej i najlepiej rozwiniętym systemem komunikowania się między ludźmi. Ponadto informacjami w rozumieniu ustawy są także inne okoliczności towarzyszące znakom językowym lub tylko informacje pozajęzykowe[573], które decydują o zakwalifikowaniu informacji językowych do kategorii danych osobowych, a nawet przesądzają o kwalifikowaniu danych osobowych do kategorii danych sensytywnych z art. 27 u.o.d.o.

Forma wyrażania danych osobowych może być różna. Z reguły dane wyrażane są w sposób zwerbalizowany (słownie), ale mogą być wyrażone w inny sposób: wizualny (np. fotografia), audialny (np. nagranie głosu osoby) czy mieszany (audiowizualny jak np. utrwalenie wizerunku i głosu osoby)[574]. Mogą to być też komunikaty wyrażone i zapisane w jakikolwiek sposób, niezależnie od sposobu, zakresu i swobody ich udostępniania, jak i niezależnie od sposobu ich pozyskania[575], pod warunkiem spełnienia dalszych wymogów zawartych w definicji z art. 6 u.o.d.o.

---

[569] Zob. R. Cisek, [w:] R. Cisek, J, Jezioro, A. Wiebe red., *Dobra i usługi informacyjne w obrocie gospodarczym*, Warszawa 2005, s. 19.
[570] T. Szewc, *op. cit.,* s. 4.
[571] Zob. B. Stefanowicz, *Informacja*, Warszawa 2004, s. 13.
[572] Zob. T. Szewc, *op. cit.,* s. 4.
[573] Zob. A. Drozd, *Ustawa*…, s. 45.
[574] A. Szewc, *Z problematyki…*, „Radca Prawny" 1999, nr 4, s. 25.
[575] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona*…., s. 370.

Pozajęzykowe dane osobowe i ich ochrona w popularnym obecnie automatycznym sposobie przetwarzania danych osobowych odgrywają bardzo istotną rolę. Np. tzw. dane biometryczne obejmujące indywidualne biologiczne cechy poszczególnych osób (jak głos, linie papilarne, źrenice, cechy twarzy czy geometria ręki) są wykorzystywane do identyfikacji określonych osób w różnym celu, począwszy ze względów zagrożenia terroryzmem, skończywszy na stosowaniu takiej identyfikacji biometrycznej w życiu codziennym przez pracodawców do identyfikacji czasu pracy pracowników (co zostało uznane przez Generalnego Inspektora Ochrony Danych osobowych uznane za niedopuszczalną praktykę[576]).

Mając powyższe na uwadze można przyjąć, że na potrzeby legalnej definicji z u.o.d.o informacją jest każda okoliczność mająca znaczenie w świetle przyjmowanych w społeczeństwie reguł kulturowych[577]. Także każda informacja, niezależnie od sposobu i formy jej wyrażenia, podlegać może ocenie z punktu widzenia pojęcia danych osobowych i każda informacja - potencjalnie, w zależności od relacji przedmiotowo-podmiotowej, a więc tego, do jakiego modelu, wycinka rzeczywistości się odnosi, oraz tego, kto tę informację przetwarza[578]- może zostać uznana za informację o charakterze osobowym.

Konkretna informacja nie musi być powszechnie zrozumiała, gdyż charakter prawny tej informacji będzie oceniany indywidualnie dla każdego jej dysponenta[579]. Nie musi być również prawdziwa, tzn. może dotyczyć okoliczności w sposób obiektywny nieistniejących, pod warunkiem jednak, iż może być przypisana do konkretnej, identyfikowalnej osoby fizycznej[580].

Jednocześnie w art. 6 ust. 2 i ust. 3 wskazane jest, jakie osoby można uznać za możliwe do zidentyfikowania, a także jaka informacja nie jest umożliwiającą określenie tożsamości osoby.

Ustalając, czy dane informacje wyczerpują znamiona danych osobowych, niewątpliwie należy odnosić się indywidualnie do okoliczności konkretnego przypadku i kontekstu przetwarzania. Treść informacji ustala się z uwzględnieniem tzw. reguł znaczeniowych języka, wskazań wiedzy naukowej czy też rozmaitych reguł kulturowych, a

---

[576] Zob. *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych w roku 1999,* s. 94; *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych w roku 2007*, s. 92; wyrok NSA z dnia 6 września 2011 r., sygn. akt I OSK 1476/10, w którym NSA uznał, że wykorzystanie danych biometrycznych (linii papilarnych) pracowników do kontroli czasu pracy jest nieproporcjonalne do zamierzonego celu ich przetwarzania.
[577] Por. A. Drozd, *Ustawa*…, s. 45.
[578] Zob. R. Cisek, J, Jezioro, A. Wiebe red., *Dobra i usługi informatyczne w obrocie gospodarczym,* Warszawa 2005, s. 19-20.
[579] Zob. P. Litwiński, *op. cit.,* s. 70.
[580] P. Litwiński, *op. cit.,* s. 71.

wskazanie relacji zachodzącej między informacją a osobą fizyczną jest kwalifikacją ze względu na określony stan faktyczny.

Informacja dotyczy osoby fizycznej wtedy, gdy przekazuje jakąś wiedzę na jej temat, a z uwagi na użycie przez ustawodawcę zwrotu „wszelkie informacje" obojętne jest, jakiej sfery życia one dotyczą. A zatem, mogą nimi być: okoliczności niezależne (jak imię i nazwisko, wiek, płeć, adres), cechy nabyte (jak np. wykształcenie, znajomość języków), a ponadto sytuacja majątkowa rozumiana jako aktywa i pasywa, a także dane osobowe innych osób (jak imiona i nazwiska osób spokrewnionych, przyjaciół)[581]. Status danych osobowych może zostać potencjalnie przyznany wszelkim informacjom odnoszącym się do osoby fizycznej, by możliwa była jej identyfikacja, w tym danych o charakterze ekonomicznym, umysłowym czy odnoszącym się do życia zawodowego.

Duża część informacji wykorzystywana w stosunkach społecznych (jak np. ogólny komunikat „dziecko Kowalskiego") może dotyczyć więcej niż jednej osoby fizycznej, co rodzi to w praktyce problem przyporządkowania takich informacji jednej tylko osobie fizycznej. Jest to ściśle związane z jedną z cech informacji, jaką są nieograniczone możliwości łączenia. Mimo iż określona informacja może zostać powiązana z więcej niż jedną osobą fizyczna, to w danych okolicznościach należy ją uznać za dane osobowe tylko jednej osoby fizycznej. Ustalając powiązanie informacji z konkretną osobą fizyczną należy kierować się metodą typologiczną, wedle której informacje słabiej lub silniej mogą być związane z określoną osobą. W konkretnej sytuacji zatem należy uznać za dane osobowe informacje należące do tej osoby fizycznej, z którą są one związane w najwyższym stopniu w świetle reguł znaczeniowych języka, wskazań wynikających z wiedzy naukowej oraz innych rozmaitych reguł kulturowych kształtujących się w świadomości społecznej[582]. Podobnie należy postępować przy rozstrzyganiu wątpliwości, czy określona informacja dotyczy osoby fizycznej czy innego podmiotu niż osoba fizyczna.

W stronie podmiotowej ochrony danych osobowych z założenia mamy do czynienia z danymi, które pozwalają zidentyfikować konkretną, ale pojedynczą osobę. Wyklucza to zatem z zakresu pojęcia dane osobowe podmiotu zbiorowego, jak np. grupa ludzi. Tak restrykcyjne sformułowanie warunkujące kryterium indywidualizacji w konkretnych przypadkach może być jednak sprzeczne z celem ochrony danych osobowych[583]. Nie budzi wątpliwości, że

---

[581] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona*…., s. 382.
[582] Zob. A. Drozd, *Ustawa*…, s. 48.
[583] W ustawodawstwach innych państw obowiązuje większa niż w Polsce elastyczność w określeniu wprost różnych zbiorowych podmiotów ochrony danych osobowych. Dla przykładu w Finlandii ochroną objęte są dane

wszyscy ludzie objęci są ochroną z zakresu danych osobowych, dlatego nie można czynić wyjątków z powołaniem się np. na kryterium obywatelstwa (w szczególności ochrona przysługuje także względem informacji o osobach niebędących obywatelami państwa).

Osoba, której dane dotyczą, nie musi być wskazywana wprost przez podanie jej imienia i nazwiska. Okoliczności pociągających za sobą identyfikację osoby fizycznej może być wiele. Wystarczające jest zapewnienie jej identyfikowalności (tzn. musi być możliwa do zidentyfikowania), a ma to miejsce wówczas, gdy jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 1 i 2 u.o.d.o). Samo wyliczenie zamieszczone w ustawie, a przedstawione powyżej, ma charakter przykładowy, o czym świadczy użycie w art. 6 u.o.d.o sformułowania „w szczególności". Podanie imienia i nazwiska nie zawsze doprowadzą do zidentyfikowania osoby fizycznej, gdyż w przypadku popularnych imion i nazwisk konieczne są wręcz informacje dodatkowe precyzujące tożsamość osoby i uznania dotyczących jej informacji za dane osobowe[584]. W niektórych jednak sytuacjach, jak uznał NSA w wyroku dotyczącym Instytutu Pamięci Narodowej, nawet dane dotyczące imienia i nazwiska mogą stanowić identyfikację osoby fizycznej, o ile w sposób nawet pośredni istnieje możliwość ustalenia jej tożsamości[585]. W takich okolicznościach imię i nazwisko będą uznane za dane osobowe.

Powołanie się na czynniki charakteryzujące osobę fizyczną może identyfikować ją w jej środowisku, ale nie pociągać za sobą takiego skutku na forum publicznym. Na przykład gdy mówimy o „kierowniku produkcji" i gdy chodzi o pracownika niewielkiej firmy, ma miejsce identyfikacja środowiskowa tej osoby. Gdy jednak stosujemy już określenie „małżonka prezydenta", to mamy do czynienia z identyfikacją powszechną. W pierwszym przypadku informacje dotyczące tej osoby nie spełniają miana danych osobowych. W celu zapobieżenia tak daleko idącej relatywizacji pojęcia „dane osobowe" przyjmuje się, iż o tym, czy określoną informację uznaje się za dane identyfikujące, rozstrzyga się biorąc pod uwagę zasób wiadomości przeciętnego człowieka[586].

---

odnoszące się wprost do „rodziny" czy „gospodarstwa domowego". Istnieją jednak i państwa, gdzie restrykcja jest daleko posunięta, jak np. w Szwecji, gdzie już w 1975 r., a potem w 1997 r., zapadły rozstrzygnięcia uznające, że numer telefonu nie ma charakteru informacji osobowej, ponieważ telefon nie może być używany przez więcej niż jedną osobą. Podaję za: M. Jagielski, *Prawo*…, s. 51.

[584] A. Szewc, *Z problematyki…,* „Radca Prawny" 1999, nr 4, s. 24.

[585] Wyrok NSA w Warszawie z dnia 28 stycznia 2008 r., I OSK 1365/06, LEX nr 453453.

[586] Zob. wyrok Sądu Apelacyjnego w Krakowie z dnia 19 grudnia 2000 r., I ACa 794/00.

Uznanie informacji za umożliwiające identyfikację określonej osoby fizycznej ulega modyfikacji ze względu na tzw. klauzulę nadmierności[587]. Przykładem jej zastosowania przez ustawodawcę jest art. 6 ust. 3 u.o.d.o. Klauzula ta opiera się na założeniu, że w niektórych sytuacjach życiowych określenie tożsamości osoby (zwłaszcza pośrednie) może być możliwe na skutek podjęcia działań wymagających dodatkowych nakładów, czy poniesienia nadmiernych kosztów. Konieczność taka może pociągnąć za sobą pozbawienie informacji miana danych osobowych. Kwalifikowanie określonego typu informacji jako uniemożliwiających określenie tożsamości osoby fizycznej wymaga oceny i uwzględnienia możliwości technicznych w czasie przetwarzania danych osobowych, gdyż to, co dziś wymaga nadmiernych kosztów, w ciągu krótkiego czasu może stać się łatwe do zrealizowania. Informacjami uniemożliwiającymi określenie tożsamości osoby nie są informacje, które można uzyskać w zwykłej i dozwolonej drodze[588]. Pojęcie nadmiernych kosztów, działań czy czasu rozpatrywać należy w odniesieniu do konkretnych podmiotów przetwarzających dane osobowe i ich możliwości, którymi dysponują w danym stanie faktycznym. Decydujące jest tutaj zachowanie pewnej proporcji między poniesionymi nakładami a rezultatem w postaci ustalenia tożsamości osoby fizycznej, gdyż charakter „nadmierności" w odniesieniu do kosztów, czasu i działań ma niewątpliwie charakter względny[589].

Zaliczenie określonej informacji do kategorii danych osobowych uzależnione jest wyłącznie od posiadania statusu osoby fizycznej, który przysługuje każdemu człowiekowi i jest niezależny np. od posiadania obywatelstwa czy ukończenia określonego wieku. Informacja może zostać uznana za mającą charakter danych osobowych tylko wtedy, gdy dotyczy „osoby fizycznej" (jednostki ludzkiej). Interpretacja tego fragmentu definicji nie nastręcza co do zasady szczególnych trudności. Ustawodawca formułując definicję danych osobowych posłużył się pojęciem „osoby fizycznej", które występuje w prawie cywilnym. Ponieważ kodeks cywilny nie definiuje pojęcia osoby fizycznej, dlatego ustalając jego znaczenie posłużyć się należy określeniem sformułowanym w nauce prawa cywilnego[590].

W praktyce pojawiają się wątpliwości w zakresie stosowania u.o.d.o. względem: informacji odnoszących się do płodów (w odniesieniu do procesów przetwarzania danych

---

[587] T. Szewc, *op. cit.*, s. 7.
[588] Wyrok SN z dnia 5 września 2001 r., sygn. akt I CKN 1159/00, OSNC 2002 nr 5, poz. 67.
[589] T. A. J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych*, Wrocław 2013, s. 16.
[590] Osoba fizyczna czyli jednostka ludzka. Zob. A. Wolter, J. Ignatowicz, K. Stefaniuk, *Prawo cywilne. Zarys części ogólnej*, Warszawa 2001, s. 157.

osobowych w zbiorach informacji medycznej), osób zmarłych lub uznanych za takie, a także osób prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej.

W nauce sporne jest, czy zdolność prawna, stanowiąca normatywną cechę każdej osoby fizycznej, przysługuje dziecku poczętemu, lecz nienarodzonemu (*nasciturus*). Według pierwszej teorii dziecko poczęte ma zdolność prawną (przysługuje mu zdolność prawna pod warunkiem rozwiązującym w postaci urodzenia martwego)[591]. Według drugiej teorii przyjmuje się, iż dziecko poczęte nie ma zdolności prawnej, ponieważ uzyskuje ją dopiero z chwilą urodzenia[592]. Wedle zaś trzeciej teorii, która jest najwłaściwsza do zaadoptowania na gruncie ustawy u.o.d.o., dziecku poczętemu przysługuje tzw. warunkowa zdolność prawna pod warunkiem zawieszającym, że urodzi się ono żywe[593], gdyż z uprawnień wynikających z ustawy o ochronie danych osobowych może korzystać człowiek tylko od chwili urodzenia. Jak wskazuje A. Drozd, „ochrona danych osobowych w każdej fazie rozwoju człowieka stanowi konstytucyjnie chronioną wartość. Nie znaczy to jednak, że intensywność tej ochrony w każdej fazie życia człowieka i w każdych okolicznościach ma być taka sama"[594]. Ochrona danych osobowych powinna być jednak wystarczająca do skutecznej ochrony konstytucyjnie gwarantowanej wartości[595].

Informacje dotyczące *nasciturusa* będą podlegać ochronie prawnej przewidzianej ustawą o.d.o. do momentu urodzenia jako dane osobowe jego matki, a niekiedy i to raczej wyjątkowo, w zależności od kontekstu ich przetwarzania, jako dane jego ojca lub innych osób[596]. Najwcześniej, bo wraz z urodzeniem się żywego dziecka, można mówić o danych osobowych dziecka, które obejmują także informacje z okresu prenatalnego.

Na uwagę zasługuje jeszcze relacja zachodząca pomiędzy pojęciem danych osobowych i osoby fizycznej, gdyż w art. 6 u.o.d.o. pojawia się sformułowanie o informacjach jej „dotyczących". Powiązanie między informacjami a osobą przedstawione zostało w opinii Grupy Roboczej Art. 29[597], która dotyczy pojęcia danych osobowych[598]. W

---

[591] A. Stelmachowski, *Zarys teorii prawa cywilnego*, Warszawa 1998, s. 157-159.
[592] A. Wolter, J. Ignatowicz, K. Stefaniuk, *op. cit.*, s. 159.
[593] Z. Radwański, *Prawo…*, s. 155.; A. Szpunar, *Szkoda wyrządzona przed urodzeniem dziecka*, „Studia cywilistyczne" 1969, t. XIII-XIV, s. 379.
[594] A. Drozd, *Ustawa…*, s. 49.
[595] Zob. orzeczenie Trybunału Konstytucyjnego z dnia 28 maja 1997 r., sygn. K 26/96, OTK ZU 1997, nr 2, poz. 19, LexPolonica nr 320490. W orzeczeniu tym Trybunał odniósł się wprawdzie do prawa do życia, lecz myśl leżąca u podstaw stanowiska Trybunału zajętego w sprawie ma szerszy zakres i może być odniesiona do ochrony danych osobowych.
[596] A. Drozd, *Ustawa…*, s. 49-50.
[597] Grupa Robocza Art. 29 jest to zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych. To niezależny podmiot o charakterze doradczym, powołany na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie

opinii podniesiono m.in., iż problematyczna może okazać się sytuacja, w której informacje dotyczą danej osoby pośrednio, a „dane przekazują przede wszystkim informacje o przedmiotach, a nie o osobach. Przedmioty te należą zazwyczaj do kogoś, podlegają wpływowi działania pewnych osób lub wywierają na nie pewien wpływ, lub też pozostają w pewnego rodzaju sąsiedztwie fizycznym lub geograficznym w stosunku do osób lub należących do nich przedmiotów". Żaden z aktów prawnych nie odnosi się do osoby fizycznej tylko bezpośrednio, a to z uwagi na fakt, iż uznanie za dane osobowe tylko i wyłącznie takich informacji musiałoby mieć swoje odbicie w aktach prawa wspólnotowego, a następnie w treści art. 6 rodzimej u.o.d.o. Konieczne jest zatem wskazanie czynników, których wystąpienie będzie skutkowało uznaniem, że dane osoby fizycznej „dotyczą"[599]. Jak wynika z konkluzji zawartej w Opinii Grupy Roboczej art. 29, dane nie muszą koncentrować się wokół osoby fizycznej, by stanowiły jej dane osobowe, przy czym konieczne jest tutaj istnienie jednego z trzech wymienionych elementów: celu[600], treści[601] lub skutku[602].

Z uwagi na charakter u.o.d.o., która w art. 2 ust. 1 „ określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych", w kategoriach danych osobowych nie traktuje się informacji o osobach zmarłych. Panuje powszechne przekonanie, że ochronie przewidzianej przez ustawę o ochronie danych osobowych nie podlegają informacje o osobie zmarłej[603]; stanowisko takie zajmuje NSA[604] oraz Generalny Inspektor Ochrony Danych

---

przetwarzania danych osobowych i swobodnego przepływu tych danych. (ang. *Working Party on the Protection of Indyviduals with regard to the Processing of Personal Data*). Zespół roboczy tworzą przedstawiciele organów nadzorczych w zakresie ochrony danych osobowych powołanych przez państwa Unii Europejskiej oraz ustanowionych dla instytucji i organów wspólnoty i z przedstawiciela Wspólnoty. Celem Zespołu roboczego jest przyczynianie się do jednolitego stosowania dyrektywy we wszystkich krajach członkowskich, opiniowanie projektów wspólnotowych aktów normatywnych z zakresu ochrony prywatności, wydawanie opinii w sprawie istniejącego poziomu ochrony danych osobowych w krajach wspólnoty jak i poza Unią. Przedstawicielem Polski w zespole roboczym jest Generalny Inspektor Ochrony Danych Osobowych.Więcej informacji dostępnych jest na stronie GIODO: http://www.giodo.gov.pl/261/j/pl/.

[598] Opinia 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych. Treść opinii dostępna jest pod adresem: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf.

[599] T. A. J. Banyś, J. Łuczak, *op. cit.,* s. 21.

[600] «Cel» występuje, jeżeli dane osobowe są lub mogą być wykorzystywane w celu oceny osoby, jej traktowania w określony sposób lub też wpływania na jej status lub zachowanie. Opinia 4/2007 w sprawie pojęcia danych osobowych, s. 10-11.

[601] «Treść»: informacja dotyczy osoby jeżeli jest „na temat" tej osoby, co musi zostać ocenione w świetle wszystkich okoliczności sprawy. Opinia 4/2007 w sprawie pojęcia danych osobowych, s. 10-11.

[602] «Skutek»- mimo iż nie występuje element „treść" ani „cel", dane osobowe można uznać za „dotyczące" osoby, ponieważ ich użycie będzie prawdopodobnie mieć wpływ na jej prawa i interesy, przy uwzględnieniu wszystkich okoliczności sprawy. Potencjalny skutek nie musi polegać na znacznym wpływie, a wystarczy, że pewna osoba może być traktowana odmiennie od innych osób na skutek przetwarzania takich danych. Opinia 4/2007 w sprawie pojęcia danych osobowych, s. 10-11.

[603] Stanowisko takie zajmują m. in.: A. Drozd, *Ustawa*…, s. 46.; A. Mednis, *Ustawa*…, s. 24-25.; J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 376-377.; R. Szałowski, *op. cit.,* s. 30.

Osobowych[605]. Analizując ten przypadek należy także odnieść się do zakresu pojęcia „osoba fizyczna".

Atrybutem każdej osoby fizycznej jest jej zdolność prawna, wyrażająca się tym, iż może ona być podmiotem praw i obowiązków[606]. Kodeks cywilny w art. 8 reguluje kwestię chwili powstania zdolności prawnej człowieka, jednak nie zawiera wyraźnego stwierdzenia, że zdolność ta wygasa z chwilą śmierci. W nauce prawa przyjmuje się jednak powszechnie, że zmarły nie może mieć ani zdolności prawnej, ani zdolności do czynności prawnych[607]. Konsekwencją takiego stanowiska jest przyjęcie w doktrynie (gdyż u.o.d.o. nie rozstrzyga tego problemu wprost[608]), że przepisy niniejszej ustawy mają zastosowanie wyłącznie do osób żyjących.

Chwila śmierci wyznacza kres bytu osoby fizycznej i od tej chwili można już mówić o osobie fizycznej jako osobie zmarłej. Śmierć osoby fizycznej wywołuje skutek na przyszłość (*ex nunc*) w tym sensie, że to zdarzenie prawne nie przekreśla istnienia osoby fizycznej przed jego zajściem i w konsekwencji usprawiedliwione jest stanowisko, że np. informacje opisujące osobę przed jej śmiercią dotyczą osoby fizycznej[609].

W przypadku ochrony danych o osobach zmarłych chodzi przeważnie o informacje, których ujawnienie mogłoby poniżyć zmarłego w pamięci potomnych, jak np. informacje o jego dewiacjach seksualnych czy nałogach. W tym przypadku należy jak najbardziej zawężająco traktować przepisy ustawy. Jeśli chodzi o osoby zmarłe, ochronie ich czci i pamięci służą przepisy prawa cywilnego w zakresie ochrony dóbr osobistych (art. 23 – art. 25 kodeksu cywilnego).

Ponadto w praktyce szereg problemów dotyczy aktualizacji danych osobowych. Administratorzy danych nie zawsze z należytą starannością przetwarzają dane osobowe, czasami korzystając z danych osobowych osób zmarłych (np. gdy pod adresy mailowe osób zmarłych wysyłane są informacje reklamowe[610]). Jak słusznie zauważył P. Litwiński, ustawodawca przyjął w przepisach u.o.d.o konstrukcję aktywnej realizacji praw związanych z ochroną danych osobowych przez osobę, której dane dotyczą[611]. Skoro więc uprawnienia te z

---

[604] Wyrok NSA z dnia 17 listopada 2000 r., sygn. akt II SA 1860/00, niepublikowany.
[605] *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych za rok 2002*, s. 22.
[606] Z. Radwański, *Prawo…*, s. 143.
[607] S. Dmowski, [w:] S. Dmowski, S. Rudnicki, *Komentarz do kodeksu cywilnego. Ks.1. Część ogólna*, Warszawa 1999, s. 56.
[608] Np. szwedzka ustawa o ochronie danych osobowych z dnia 29 kwietnia 1998 r. w art. 3 stwierdza wprost, iż zakresem stosowania jej przepisów objęte są wyłącznie osoby fizyczne.
[609] A. Drozd, *Ustawa*…, s. 50.
[610] *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych w roku 2002*, s. 235.
[611] Zob. P. Litwiński, *op. cit.*, s. 72.

natury rzeczy mogą przysługiwać wyłącznie osobom żyjącym, to informacje o osobach zmarłych powinny pozostać poza zakresem zastosowania przedmiotowej ustawy.

Na potrzeby przetwarzania danych w ramach stosunków pracy często pojawia się problem wykorzystywania danych osobowych pracowników przez pracodawców. Na tym tle wyodrębniła się kategoria danych osobowych zwanych danymi osobowymi służbowymi. Informacje o pracowniku, takie jak np. jego imię i nazwisko, służbowy adres *e-mail*, numer telefonu czy stanowisko pracy, są ściśle związane z życiem zawodowym pracownika i z wykonywaniem przez niego obowiązków służbowych. Dane te mogą być wykorzystywane, w tym udostępniane przez pracodawcę, nawet bez zgody pracownika, którego one dotyczą. Wskazuje na to również stanowisko Sądu Najwyższego zawarte w wyroku z dnia 19 listopada 2003 r., w którym zostało stwierdzone, iż „nazwisko i imię jest skierowanym na zewnątrz znakiem rozpoznawczym osoby fizycznej i ujawnienie go w celu jej identyfikacji nie może być zasadniczo uznane za bezprawne, o ile nie łączy się z naruszeniem innego dobra osobistego, np. czci, prywatności lub godności osobistej. Ujawnienie przez pracodawcę nazwiska (imienia) pracownika bez jego zgody nie stanowi bezprawnego naruszenia dobra osobistego, jeżeli jest usprawiedliwione zadaniami i obowiązkami pracodawcy związanymi z prowadzeniem zakładu, jest niezbędne i nie narusza praw oraz wolności pracownika”[612]. SN zwrócił też uwagę, że „najistotniejszym składnikiem zakładu pracy (przedsiębiorstwa) są ludzie, a funkcjonowanie zakładu wiąże się nierozłącznie z kontaktami zewnętrznymi – kontrahentami, klientami [...]. Dlatego pracodawca nie może być pozbawiony możliwości ujawniania nazwisk pracowników, zajmujących określone stanowiska w ramach instytucji. Przeciwne stanowisko prowadziłoby do sparaliżowania lub poważnego ograniczenia możliwości działania pracodawcy, bez żadnego rozsądnego uzasadnienia w ochronie interesów i praw pracownika [...]. Imiona i nazwiska pracowników widnieją na drzwiach w zakładach pracy, umieszcza się je na pieczątkach imiennych, pismach sporządzanych w związku z pracą, prezentuje w informatorach o instytucjach i przedsiębiorstwach, co oznacza, że zgodnie powszechną praktyką są one zasadniczo jawne”. Kwestia służbowego udostępnienia informacji o pracowniku, w związku z pełnionymi funkcjami służbowymi (służbowych danych osobowych), nie może być uznana za naruszenie obowiązujących zasad ochrony danych osobowych zawartych w u.o.d.o[613].

---

[612] Wyrok SN z dnia 19 listopada 2003 r., sygn. I PK 590/02.

[613] Tego typu kwestie powinny jednak być zawarte w regulaminie wprowadzonym przez pracodawców na podstawie art. 104 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1974 r., Nr 24, poz. 141).

Analiza różnorodnych kryteriów informacji, które mogą wyczerpać znamiona danych osobowych wskazuje, iż koncepcja prawodawcy, aby stworzyć jednolity przedmiot ochrony, nie powiodła się. Podziały zaproponowane w doktrynie mają na celu systematyzację i uporządkowanie informacji, którym może przysługiwać status danych osobowych, podziały zaś wynikające z ustawy o ochronie danych osobowych mają charakter normatywny i przejawiają się w odmiennym ukształtowaniu obowiązków związanych z procesem przetwarzania danych osobowych należących do różnych kategorii (art. 23 i art. 27 u.o.d.o.)[614].

Ustawa definiując pojęcie danych osobowych odnosi się do informacji osobowych określających tożsamość człowieka, ale także i do takich, które funkcji identyfikacyjnej bezpośrednio nie spełniają; co więcej, to właśnie znajomość tożsamości osoby jest warunkiem ustalenia tych danych. W związku z taką możliwą konstrukcją danych osobowych pojęcie danych osobowych należy ujmować dualistycznie[615]. Do zakresu desygnatów tych danych należy zarówno informacja identyfikacyjna - umożliwiająca ustalenie tożsamości konkretnego człowieka, jak i informacja osobopoznawcza - pozwalająca na dokładniejsze poznanie jego szczegółowych przymiotów, takich jak: cechy fizyczne, psychiczne, fizjologiczne, kulturowe, społeczne itp.[616] Zważywszy na przedstawione cechy klaruje się podział (chociaż nienazwany i nie wprost wskazany w ustawie, a jedynie wynikający z przepisów) na dane osobowe zwykłe (pospolite, standardowe, neutralne) i dane wrażliwe (sensytywne, z ang. *sensitive data*)[617].

Jest to podział przeprowadzony w oparciu o przesłanki dopuszczalności przetwarzania danych osobowych, które zostały odmiennie ukształtowane. Informacje osobopoznawcze w dużej części zawarte są w danych wrażliwych, co do których proces przetwarzania objęty jest daleko idącymi restrykcjami prawnymi (art. 27 u.o.d.o.)[618]. Dane wrażliwe są wymienione w formie katalogu zamkniętego. Zostały wyeksponowane na tle pozostałych danych osobowych

---

[614] P. Litwiński, *Ochrona…*, s. 82.
[615] A. Szewc, *Z problematyki*…, „Radca Prawny" 1999, nr 4, s. 25.
[616] Zob. J. Żermen, *Ochrona danych osobowych*, „Gazeta Prawna" 1996, nr 60.
[617] W nauce prawa spotkać można także inne koncepcje dotyczące klasyfikacji danych osobowych. Wyodrębnić można np. trzy kategorie danych osobowych: dane identyfikujące konkretną osobę (nazwisko, imiona, miejsce zamieszkania, data urodzenia, imiona rodziców), dane adresowe oraz dane osobiste, przekazujące informacje o stosunkach majątkowych i niemajątkowych danej osoby. Podział ten nie obejmuje jednak wszystkich kategorii informacji, które mogą zostać uznane za dane osobowe, stąd jego doniosłość w nauce prawa jest znikoma. Zob. G. Sibiga*, Postępowanie…,* s. 39. G. Szpor proponuje natomiast, aby obok danych osobowych, dających się powiązać z osobą fizyczną, wyróżnić także tzw. dane indywidualne, dające się powiązać z przedsiębiorcą lub jednostką organizacyjną niemającą osobowości prawnej i informacje te łącznie tworzyłyby kategorię danych jednostkowych. Zob. G. Szpor, *Publicznoprawna…,* s. 7 i n.
[618] E. Kulesza, *Zdrowie: zasada i wyjątki*, „Rzeczpospolita" z 4 maja 2000 r.

przyjmując, iż dotyczą bezpośrednio sfer życia należących do prywatności czy nawet intymności osoby fizycznej[619]. Wyróżnienie danych wrażliwych nastąpiło mocą decyzji ustawodawcy, która nie zawsze nawiązuje do teorii sfer jednostki (sfera powszechnej dostępności, sfera prywatności, intymności), gdyż wśród danych osobowych znajdują się tego typu informacje (jak np. informacje dotyczące decyzji administracyjnych), które nie zawsze objęte są sferą życia prywatnego[620].

Pojęcie danych wrażliwych zostało powszechnie przyjęte dla określenia tej specyficznej kategorii danych i występuje zarówno w orzeczeniach sądów administracyjnych[621], jak i w decyzjach GIODO[622]. Ta szczególna kategoria danych osobowych ma charakter zamknięty i obejmuje: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach oraz życiu seksualnym (art. 27 ust. 1 u.o.d.o). Ponadto dane wrażliwe obejmują także informacje dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (art. 27 ust.1 u.o.d.o). Wskazany podział ma uzasadnienie historyczne, gdyż drugi z przedstawionego katalogu danych został dodany nowelizacją 25 sierpnia 2001 r. (wcześniej w tym zakresie obowiązywał przepis odrębny, tj. art. 28 ust. 1 u.o.d.o.)[623]. Ponadto dane osobowe wskazane w pierwszym katalogu traktowane są przez ustawodawcę odmiennie względem danych z katalogu drugiego. W świetle art. 49 u.o.d.o. nieuprawnione przetwarzanie danych z katalogu pierwszego jest zagrożone surowszą odpowiedzialnością karną. W związku z powyższym nasuwa się wniosek, że dane osobowe wymienione w pierwszym katalogu mają charakter szczególnie wrażliwy[624].

Do danych sensytywnych z drugiego katalogu zaliczane są informacje o wszelkich orzeczeniach wydanych przez sądy i organy administracji publicznej, w tym w sprawach

---

[619] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 569
[620] A. Drozd, *Ustawa…,* s. 169.
[621] Zob. postanowienie NSA z dnia 30 maja 2012 r., sygn. I OSK 1109/12. Treść postanowienia dostępna pod adresem: http://orzeczenia.nsa.gov.pl/F151DB7738; wyrok NSA z 30 listopada 2011 r., sygn. akt I OSK 2118/10. Treść wyroku dostępna pod adresem: http://orzeczenia.nsa.gov.pl/doc/6A2A1D2737; wyrok NSA z 18 października 2011 r., sygn. akt I OSK 1742/10. Treść wyroku dostępna pod adresem: http://orzeczenia.nsa.gov.pl/doc/FD6DFF5DD0; wyrok WSA w Warszawie z dnia 20 października 2010 r., sygn. akt II SA/Wa875/10; wyrok NSA z dnia 18 października 2011 r., sygn. akt I OSK 1742/10. Treść wyroku dostępna pod adresem: http://orzeczenia-nsa.pl/wyrok/ii-sa-wa-875-10,182f6e6.html.
[622] Zob. decyzja GIODO dotyczące danych wrażliwych dostępne pod adresem: http://www.giodo.gov.pl/304/j/pl/.
[623] T. A. J. Banyś, J. Łuczak, *op. cit.*, s. 22.
[624] Tak: A. Drozd, *Ustawa…,* s. 170.

cywilnych i administracyjnych. Informacje dotyczące skazań obejmują nie tylko wyroki karne wydane przez sądy powszechne, lecz także orzeczenia sądów koleżeńskich[625].

Na tle danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym mogą pojawić się pewne wątpliwości co do kar dyscyplinarnych nakładanych w ramach odpowiedzialności dyscyplinarnej, a także kar porządkowych nakładanych na pracowników przez pracodawcę na podstawie kodeksu pracy (art. 108 i n. k.p.). Dane osobowe dotyczące orzeczeń o karach dyscyplinarnych należy zaliczyć do kategorii danych wrażliwych, gdyż mieszczą się one w pojęciu innych orzeczeń wydanych w postępowaniu administracyjnym. Podobnie należy traktować dane osobowe dotyczące kar porządkowych stanowiących niższy stopień odpowiedzialności dyscyplinarnej, których nakładanie jest uregulowane w pragmatykach pracowniczych. Natomiast nakładanie kar porządkowych przez pracodawcę na podstawie kodeksu pracy mieści się w ramach zobowiązaniowego stosunku pracy, a kompetencje pracodawcy w tym zakresie różnią się od władztwa administracyjnego[626]. Dlatego też dane dotyczące kar porządkowych, takich jak: kary upomnienia, nagany, kara pieniężna, nie mogą być zaliczone do kategorii danych wrażliwych zamieszczonych w art. 27 ust. 1 u.o.d.o[627].

Katalog danych szczególnie chronionych zawarty w u.o.d.o. jest bogatszy w porównaniu do zakresu danych wskazanych w art. 8 dyrektywy 95/46/WE, gdyż dyrektywa określa tylko minimalne standardy w zakresie ochrony danych wrażliwych. Dyrektywa wiąże te państwa członkowskie, do których jest skierowana, jedynie w zakresie celu, jaki ma być osiągnięty, pozostawiając sposób i zakres regulacji tym państwom do swobodnej wewnętrznej regulacji. Dopuszczalne jest w związku z tym, aby regulacja krajowa zapewniała wyższy i bardziej pełny zakres zabezpieczenia niż nakaz płynący z dyrektywy, np. poprzez zaliczenie do danych wrażliwych kolejnych kategorii informacji[628]. W art. 8 ust. 4 dyrektywy wskazana jest możliwość ustanawiania innych zwolnień od zakazu przetwarzania danych, poza tymi, które zostały określone jako szczególne na mocy prawa krajowego lub decyzji organu nadzorczego, a tym samym rozbudowania katalogu danych wrażliwych z uwagi na ważny interes publiczny, jeśli tylko zostaną wprowadzone odpowiednie gwarancje. Z takiej możliwości skorzystał więc polski ustawodawca umieszczając w grupie danych sensytywnych

---

[625] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 571
[626] Z. Kubot, *Charakter prawny odpowiedzialności porządkowej w kodeksie pracy*, „Państwo i Prawo" 1975, nr 7, s. 94-95.
[627] Tak: A. Drozd, *Ustawa…,* s. 171.
[628] Tak: T. A. J. Banyś, J. Łuczak, *op. cit.,* , s. 23.

dane odnoszące się do przynależności partyjnej, wyznaniowej oraz dane o kodzie genetycznym i nałogach, które w dyrektywie są poza katalogiem wskazanym w art. 8.

Ponadto przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być, na mocy dyrektywy, dokonywane jedynie pod kontrolą oficjalnych władz, lub też, jeżeli zgodnie z prawem krajowym stworzone zostały odpowiednie szczególne zabezpieczenia, z uwzględnieniem wyłączeń, które państwa członkowskie mogą wprowadzić zgodnie z obowiązującymi przepisami krajowymi, zapewniając odpowiednie szczególne zabezpieczenia[629].

W praktyce przetwarzania danych osobowych dane sensytywne wskazane w art. 27 ust. 1 u.o.d.o. odnajdziemy m. in.: w odpowiedzi na zapytanie o udzielenie informacji o osobie[630] (potocznie zwane zaświadczeniem o niekaralności), także jeśli zawiera ona stwierdzenie, że dana osoba nie figuruje w Krajowym Rejestrze Karnym, gdyż daną dotyczącą skazań jest także informacja o braku karalności; w księgach parafialnych Kościoła katolickiego[631]; w dokumentacji medycznej[632], takiej jak karta przebiegu ciąży, skierowanie do szpitala czy karta informacyjna leczenia szpitalnego[633] (zawsze będą one zawierać opisy stanu zdrowia pacjenta lub opis udzielonych mu świadczeń zdrowotnych). Dane wrażliwe znajdują się także we wniosku o nadanie statusu uchodźcy[634] (jego wypełnienie wymaga podania informacji o rasie, pochodzeniu etnicznym, wyznaniu czy o stanie zdrowia wnioskodawcy) czy rejestrze zakażeń szpitalnych i czynników alarmowych[635].

Ze statusem danych sensytywnych wiąże się ponadto odrębny reżim prawny co do całokształtu przetwarzania danych osobowych.

Przesłanki legalnego przetwarzania danych zwykłych zostały określone w art. 23 ust. 1 u.o.d.o, zaś względem danych wrażliwych - w art. 27 ust. 2 u.o.d.o. Istnieje ogólny zakaz

---

[629] M. Polok, *op. cit.*, s. 93.
[630] Informacja udzielana jest na podstawie ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2012 r., poz.654 z późn. zm.).
[631] Prowadzone na podstawie kan. 535 Kodeksu prawa kanonicznego z 1983 r.
[632] Brak jest ustawowej definicji danych medycznych, jednak elementy, które się na nią składają zawarte są w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzecznika Praw Pacjenta (Dz. U. z 2012 r., poz. 159 z późn. zm.).
[633] Rodzaje dokumentacji medycznej wskazuje rozporządzenie Ministra Zdrowia z 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. Nr 252, poz. 1697 z późn.zm.).
[634] Wniosek, o którym mowa w ustawie z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej (Dz. U. z 2006 r. Nr 23, poz.1695 ze późn. zm.); wzór wniosku określa rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 maja 2008 r. w sprawie wzoru formularza wniosku o nadanie statusu uchodźcy (Dz. U. Nr 92, poz. 579 z późn.zm.).
[635] Rejestr prowadzony jest na podstawie przepisów ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. Nr 234, poz. 1570 zpóźn.zm.), a zakres danych przetwarzanych w tym rejestrze określa art. 14 ust. 5 pkt 1-6 ustawy.

przetwarzania danych wrażliwych sformułowany w art. 27 u.o.d.o., chyba że spełniona jest jedna z przesłanek z art. 27 ust. 2 pkt 1-10 u.o.d.o., która jest podyktowana szczególnym charakterem tych informacji i koniecznością zapewnienia każdej osobie fizycznej poszanowania jej prawa do prywatności.

Względem danych sensytywnych istnieją szczególne warunki udostępniania tych danych[636]. W stosunku do danych wrażliwych, zgodnie z art. 46 ust. 2 ustawy, istnieje obowiązek uprzedniego zarejestrowania zbioru danych wrażliwych przed przystąpieniem do przetwarzania danych w zbiorze, chyba że administrator danych osobowych został zwolniony z obowiązku rejestracji zbioru na podstawie art. 43 ust. 1 u.o.d.o. Względem danych zwykłych można przetwarzać dane w zbiorze podlegającym obowiązkowi rejestracji od momentu zgłoszenia wniosku o zarejestrowanie zbioru danych na podstawie art. 46 ust. 1 u.o.d.o. Niezwłocznie po przeprowadzeniu rejestracji Generalny Inspektor Ochrony Danych Osobowych z urzędu wydaje administratorowi danych zaświadczenie o zarejestrowaniu zbioru takich danych (art. 42 ust. 4 ustawy); w stosunku do danych zwykłych zawiadomienie o zarejestrowaniu zbioru danych w GIODO następuje na wniosek administratora danych (art. 42 ust. 3 ustawy). Co więcej, na administratorze danych ustawy ciąży obowiązek zobowiązania do zgłoszenia GIODO rozszerzenia zakresu przetwarzania danych w zbiorze, w wyniku czego będą w nim przetwarzane dane wrażliwe (art. 41 ust. 3).

Względem danych wrażliwych winno się również stosować szczególne środki ochrony i bezpieczeństwa ich przetwarzania, co najmniej na poziomie podwyższonym lub wysokim. Tak restrykcyjnych wymagań nie stawia się w przypadku przetwarzania danych zwykłych, gdyż tu wymaganym poziomem bezpieczeństwa przetwarzania danych są co najmniej środki na podstawowym poziomie bezpieczeństwa.

Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych wrażliwych zagrożone jest karą grzywny, karą ograniczenia wolności oraz podwyższoną górna granicą odpowiedzialności karnej z 2 do 3 lat pozbawienia wolności (art. 49 ust. 1 u.o.d.o.) Względem danych zwykłych jest to kara grzywny, ograniczenia wolności albo kara pozbawienia wolności do 2 lat (art. 49 ust. 2 u.o.d.o).

Rozstrzygnięcie w poszczególnych przypadkach o uznaniu konkretnej danej osobowej za wrażliwą może nastąpić na podstawie kontekstu ich przetwarzania. Posługując się

---

[636] W wyniku nowelizacji ustawy o ochronie danych osobowych z 29 października 2010 r., uchylono art. 30 u.o.d.o., który statuował warunki legalności przetwarzania danych wrażliwych. W obecnym stanie prawnym w celu legalnego udostępniania danych sensytywnych powinna zostać spełniona chociaż jedna z przesłanek zawarta w art. 27 ust. 2 pkt 1-10 u.o.d.o.

przykładem listy osób oczekujących do lekarza należy wyprowadzić wniosek, że jeśli lekarz nie jest specjalistą (np. diabetologiem), do którego zgłasza się pacjent z typową dla tej specjalności chorobą (np. z cukrzycą), wówczas nie można mówić o przetwarzaniu danych wrażliwych dotyczących w tym przypadku stanu zdrowia. Stąd też wywieszenie listy osób oczekujących do lekarza konkretnej specjalności nie prowadzi do ujawnienia informacji dotyczących schorzenia i nie jest przetwarzaniem danych osobowych sensytywnych[637].

Mówiąc o podziale na dane zwykłe i dane wrażliwe, należy mieć na uwadze, że właściwie każdy zbiór danych wrażliwych będzie zawierał dane zwykłe. W przypadku kiedy danym wrażliwym nie będą towarzyszyły jednocześnie dane o zidentyfikowanej osobie fizycznej lub dane wrażliwe nie pozwolą na jej zidentyfikowanie, będziemy mieli w istocie do czynienia z danymi zanonimizowanymi, a tych przecież przepisy ustawy o ochronie danych osobowych nie dotyczą[638].

Przykładem wciąż nastręczającym wątpliwości w praktyce jest kategoryzacja numeru PESEL czy numeru VIN jako danych osobowych. W tym zakresie najważniejszym odniesieniem jest kontekst sytuacyjny, gdyż jednoznaczne przyporządkowanie numeru PESEL do zakresu danych osobowych zależy od tego, czy podmiot dysponujący numerem PESEL może go przyporządkować do określonej osoby fizycznej czy nie. PESEL może być daną osobową dla urzędu, gdyż w rejestrze urzędu do danego numeru PESEL może być przypisane konkretne imię i nazwisko posiadacza tego numeru, adres, miejsce i data jego urodzenia, często konto bankowe itp.[639]. W takiej sytuacji i w powiązaniu z informacjami, które posiada urząd, numer PESEL będzie dana osobową. PESEL może być także daną osobową dla pracodawcy, kiedy w dokumentacji kadrowej będzie wskazywał konkretnego pracownika. Osobie fizycznej, która nie dysponuje jednak żadnymi dodatkowymi informacjami, jakie do doidentyfikowania posiada (np. czy urząd czy pracodawca), sam numer PESEL nie będzie określał tożsamości osoby, która ten numer używa.

Co do zasady sam numer VIN nie stanowi informacji, na podstawie której można zidentyfikować konkretną osobę, zatem nie można uznać go za dane osobowe[640]. Przy ustalaniu czy numer VIN należy do kategorii danych osobowych, należy jednak wziąć pod uwagę zarówno przepisy ustawy o ochronie danych osobowych, jak i unormowania ustawy

---

[637] T. Szewc, *op. cit.,* s. 10.
[638] T. A. J. Banyś, J. Łuczak, *op. cit.,* s. 26.
[639] M. Brzozowska, *op. cit.,* s. 28.
[640] http://www.giodo.gov.pl/317/id_art/2836/j/pl.

z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym[641]. Ta druga regulacja stanowi, iż każdy pojazd uczestniczący w ruchu powinien posiadać nadane przez producenta cechy identyfikacyjne, jak numer VIN albo numer nadwozia, podwozia lub ramy (art. 66 ust. 3a Prawa o ruchu drogowym). Trudno więc uznać, że sam numer VIN stanowi dane osobowe. Na jego podstawie nie można bowiem zidentyfikować konkretnej osoby ani bezpośrednio, ani pośrednio bez nadmiernego kosztu, czasu i działań. Jednak dla niektórych podmiotów mających dostęp do informacji zgromadzonych w centralnej ewidencji kierowców posiadanie samego nr VIN stanowi informację, na podstawie której są one w stanie, bez nadmiernego kosztu, czasu i działań, zidentyfikować konkretną osobę. Zgodnie bowiem z art. 80a ust. 2 Prawa o ruchu drogowym w centralnej ewidencji pojazdów gromadzi się dane i informacje o pojazdach zarejestrowanych oraz o ich właścicielach lub o niektórych posiadaczach. Ustawa o ruchu drogowym wskazuje ponadto zamknięty katalog podmiotów, które mają dostęp do informacji zgromadzonych w centralnej ewidencji pojazdów. Są to m.in. policja, prokuratura, sądy, komornicy sądowi, ZUS, straże gminne (miejskie), organy właściwe w sprawach kontroli skarbowej, organy właściwe w sprawach rejestracji pojazdów, organy podatkowe. Dla wskazanych podmiotów, jak również dla administratora danych, jakim w tym przypadku jest minister właściwy do spraw administracji publicznej, powiązanie numeru VIN z innymi informacjami identyfikującymi właściciela pojazdu, nie stanowi problemu[642]. Umożliwia więc bez nadmiernego kosztu, czasu i działań, zidentyfikować konkretną osobę. Dla nich numer VIN będzie stanowił dane osobowe.

Przedstawione przykłady wskazują, iż różne informacje w różnych okolicznościach można poczytywać za dane osobowe. Jedne podmioty bez większego nakładu sił, kosztów i czasu mogą precyzyjnie ustalić tożsamość osoby fizycznej, dla innych podmiotów z kolei będzie się to wiązało z nieproporcjonalnym nakładem różnych środków. Należy wskazać, że ustawa o ochronie danych osobowych nie precyzuje konkretnie zakresu czy katalogu informacji, które zawsze i w każdych okolicznościach będą uważane za dane osobowe[643].

Wątpliwości w zakresie uznawania pewnych informacji za dane osobowe dotyczą także informacji przesłaniających, tzw. pseudonimów. Bywają one często stosowane jako identyfikatory np. w systemach informatycznych lub teleinformatycznych. W zależności od konkretnych okoliczności mogą być uznane za dane osobowe, jeżeli określenie na ich podstawie tożsamości osoby fizycznej nie pociąga za sobą nadmiernych kosztów, działań czy

---

[641] Dz. U., Nr 98, poz. 602.
[642] http://www.giodo.gov.pl/317/id_art/2836/j/pl.
[643] M. Brzozowska, *op. cit.*, s. 28.

czasu. Danymi osobowymi nie są także informacje fikcyjne, czyli takie, które nie dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[644].

Informacje dotyczące zidentyfikowanej lub możliwej do identyfikacji osoby fizycznej są danymi osobowymi niezależnie od tego, czy są prawdziwe, czy też częściowo odpowiadają prawdzie bądź są z nią niezgodne[645]. Jeżeli dane osobowe są niezgodne z prawdą, nieaktualne albo niekompletne, to na podstawie art. 32 ust. 1 pkt 6 u.o.d.o. osoba zainteresowana może wystąpić do administratora danych z żądaniem uzupełnienia, uaktualnienia, sprostowania danych osobowych albo czasowego wstrzymania ich przetwarzania lub ich usunięcia.

Danymi osobowymi zawartymi w zbiorach danych nie są jedynie informacje prawdziwe czy aktualne, nie mogą to być jednak informacje anonimowe, gdyż z założenia uniemożliwiają jakąkolwiek identyfikację osoby fizycznej[646]. Podobnie rzecz się ma w odniesieniu do danych statystycznych, których, z uwagi na sposób ich opracowania, nie można połączyć z określoną już osobą fizyczną i które czynią niemożliwym zidentyfikowanie nieznanej osoby fizycznej.

Rozwój technologii, a zwłaszcza Internetu, tworzy nowe i znacznie większe niż dotychczas możliwości w zakresie przetwarzania danych osobowych[647]. W życie społeczne człowieka wkraczają sieci komputerowe i coraz łatwiej i szybciej można zweryfikować tożsamość drugiego człowieka i dotrzeć do konkretnych informacji o sobie lub o innych osobach fizycznych, zarówno to na potrzeby stosunku pracy, celów handlowych, medycznych, jak i marketingowych[648]. W związku z upowszechnieniem i rozwojem nowych technologii prężnie kształtuje się obok „tradycyjnych" danych osobowych nowa kategoria danych, tj. danych elektronicznych, zwanych też cyfrowymi danymi osobowymi lub danymi

---

[644] A. Drozd, *Ustawa…,* s. 55.
[645] *Ibidem*, s. 54-55.
[646] Na mocy art. 32 ust. 1 pkt 6 u.o.d.o każdej osobie przyznano prawo do żądania od administratora danych uzupełnienia, uaktualnienia czy sprostowania dotyczących go danych osobowych.
[647] Internet jest największą siecią komputerową na świecie. Jest rozległą siecią rozproszoną, gdyż łączy ze sobą wiele często znajdujących się w znacznej odległości od siebie systemów komputerowych (łączy około 30 mln serwerów znajdujących się w różnych punktach na kuli ziemskiej) i nie można w niej wyróżnić komputera centralnego czy też ośrodka zarządzającego. Internet jest siecią, która może działać nawet w sytuacji odłączenia od niej znacznej części serwerów, a każdy jej fragment jest zdolny do samodzielnego działania. Jest to globalne i ponadkrajowe medium komunikowania się i przekazu informacji, umożliwiające kontakt za pośrednictwem poczty elektronicznej, grup dyskusyjnych, forów i dające możliwość kopiowania programów, prowadzenia reklamy, dokonywania zakupów czy transakcji bankowych. Zob. J. Petzel, *Informatyka prawnicza. Zagadnienia teorii i praktyki*, Warszawa 1999, s. 291- 295.
[648] Przy pomocy specjalnych programów tzw. *packet sniffers* wyszukiwane mogą być przepływające w sieci dane określonego rodzaju, np. wybierane według słów kluczowych lub według danych o karcie kredytowej, a tak uzyskane informacje można wykorzystywać w dowolnym celu prywatnym, dla dalszych ingerencji czy też nawet przestępstw gospodarczych.

„swoistymi”[649]. Z pewnością z nowo wyodrębniającymi się danymi wiąże się sporo wątpliwości co do uznania ich za dane osobowe (jak ich proces przetwarzania, gromadzenia czy rejestracji zbiorów zawierających ten rodzaj danych), ale i co do prawnego wykorzystywania tych danych w Internecie. Komplikacje powoduje również brak jednolitego aktu prawnego (obecnie istnieje szereg ustaw, które wprowadzają różny poziom ochrony i nie zawsze są adekwatne w czasie co do aktualnej rzeczywistości), który kompleksowo regulowałby prawo właściwe dla procesów przetwarzania danych osobowych w sieci Internet. Warto jest zatem przedstawić status prawny informacji zbieranych i wykorzystywanych przy okazji korzystania przez użytkowników z sieci Internet, a które to informacje potencjalnie mogą mieć charakter danych osobowych.

Dane osobowe, które są specyficzne dla Internetu, to dane osobowe przetwarzane w obiegu otwartym (Internet), zamkniętym (Internet) oraz w komputerach niepodłączonych do sieci, a także innych urządzeniach elektronicznych przetwarzających dane[650]. W tej kategorii danych mieszczą się dwie kategorie danych: tradycyjne dane przetwarzane cyfrowo oraz dane wirtualne.

Tradycyjne dane przetwarzane cyfrowo to dane elektroniczne, które jednocześnie stanowią dane osobowe i które mają swój odnośnik w rzeczywistości. Jest to np. wszelka elektroniczna dokumentacja, jak: imię i nazwisko, numer telefonu, zdjęcie przetworzone cyfrowo czy cyfrowo przetworzone linie papilarne, o ile prowadzą one do identyfikacji osoby fizycznej. Dane te będą przetwarzane w systemie informatycznym i mogą być przetwarzane zarówno *online* (np. przesyłanie danych w dokumentach czy przesyłanie zdjęć cyfrowych z wizerunkami konkretnych osób), jak i *offline* (np. posiadanie bazy z danymi osobowymi pacjentów, pracowników, klientów itp. w komputerze niepodłączonym do Internetu).

Druga kategoria danych to dane wirtualne, wśród których można wyróżnić dwie grupy.

Do pierwszej z nich zaliczyć należy dane wirtualne, które istnieją jedynie w cyberprzestrzeni, nie mając swojego odbicia w rzeczywistości, ale za ich pomocą jesteśmy w stanie zidentyfikować określoną osobę. Przykładem takich danych są sieciowe adresy IP, adres poczty elektronicznej *e-mail,* pliki *cookies,* adresy domeny internetowej czy adresy sieciowe URL (*Universal Resorce Lokator* czyli jednolity lokalizator zasobów[651]).

---

[649] J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1999, s. 27.
[650] Zob. M. Brzozowska, *op. cit.*, s. 30-31.
[651] Funkcją adresu sieciowego URL jest identyfikowanie w sieci poszczególnych zasobów informacyjnych znajdujących się na serwerach. Zasoby te zwykle są tworzone przez użytkowników Internetu w postaci stron

Druga grupę stanowią cyfrowe dane umieszczane w cyberprzestrzeni, jak np. zdjęcie cyfrowe umieszczane w portalu społecznościowym. Dane cyfrowe to kategoria danych osobowych w rozumieniu u.o.d.o, które są lub mogą być zapisane na nośniku elektronicznym i mogą być uporządkowane w pewnej określonej, wewnętrznej strukturze. Cyfrowe dane osobowe mają swoje odzwierciedlenie w rzeczywistości (np. zbiór danych cyfrowych, cyfrowe dane umieszczane w Internecie) i występują jedynie w sieci internetowej. Dane te mogą być przetwarzane zarówno w Internecie, jak i poza nim w sieciach zamkniętych.

Jeśli dane wirtualne spełniać będą przesłanki z art. 6 u.o.d.o, wówczas stanowić będą dane osobowe. Jest to jednoznaczne z obowiązkiem przestrzegania wszelkich wymogów ustawy, a także zapewnieniem wszelkich środków bezpieczeństwa względem tych danych, o których wspomina ustawa. Informacje należące do kategorii danych wirtualnych nie zawsze jednak będą danymi osobowymi, gdyż każdorazowo na podstawie indywidualnych warunków ocenić należy ilość nakładów (nadmierny czas, działania i koszty) koniecznych do zidentyfikowania określonej osoby na podstawie tych danych. Czasem adres *e-mail,* adres IP czy plik *cookies* w ogóle nie będzie identyfikował ani w sposób bezpośredni, ani pośredni osoby fizycznej, wówczas to takie dane będą tylko danymi technicznymi, a nie będą na pewno stanowiły danych osobowych w rozumieniu ustawy o ochronie danych osobowych.

Warto chociaż pobieżnie przyjrzeć się konstrukcji śladów, które powszechnie pozostawia w sieci przeciętny użytkownik Internetu. Są to: adres sieciowy IP, adres *e- mail* oraz nazwa użytkownika tzw. *nick* lub *login*, czyli informacje, które mogą spełniać kryteria danych osobowych.

Wątpliwości pojawiają się przy klasyfikacji adresu *e-mail* jako danej osobowej. By uzyskać jednoznaczną odpowiedź należy wskazać różne kategorie adresów poczty elektronicznej. Definicja adresu mailowego zawarta jest w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[652] i zgodnie z treścią art. 2 pkt 1 adres elektroniczny jest to oznaczenie systemu teleinformatycznego umożliwiające porozumiewanie się za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Pocztę elektroniczną trzeba więc na gruncie tej ustawy traktować jako środek komunikacji elektronicznej.

WWW, a ich charakter może być różny. Może to być krótka informacja personalna, informacja o firmie mieszcząca się na kilku stronach WWW, czy też olbrzymia baza danych zawierająca informacje o charakterze prawnym. J. Petzel, *op. cit.*, s. 298.

[652] Dz. U. Nr 144, poz. 1204 z późn. zm.

W doktrynie prezentowane są dwa stanowiska w zakresie kwalifikacji adresów *e- mail* jako danych osobowych. Pierwsze stanowisko traktuje każdy adres *e-mail* jako daną osobową, gdyż o kwalifikacji adresu poczty elektronicznej jako informacji o charakterze danych osobowych ma przesądzać obiektywna możliwość identyfikacji osoby, której ten adres dotyczy[653]. Zgodnie z drugim stanowiskiem za dane osobowe można uznać tylko te adresy *e-mail*, które zawierają w sobie jawne dane identyfikujące właściciela[654].

Adres poczty elektronicznej może zostać uznany za daną osobową, jednak im jest on ogólniejszy, tym mniejsza możliwość uznania go za daną osobową. Nie można uznać za daną osobową (lub będzie to znacznie utrudnione) adresu, który nie pozwala na identyfikację osoby[655]. Jeżeli w adresie mailowym stosowany jest identyfikator jak imię i nazwisko albo też podmiot świadczący usługi w zakresie udostępniania skrzynek poczty elektronicznej zebrał przy zawieraniu umowy o świadczenie usług dane osobowe użytkownika, to adres poczty elektronicznej należy do kategorii danych osobowych[656]. Co więcej, w sytuacji, gdy w adresie zawarte są kategorie informacji pozwalających na zidentyfikowanie właściciela adresu, tj. imię i nazwisko w połączeniu z domeną określająca nazwę firmy prawnej i fakt rejestracji domeny w Polsce (jak np. imię_nazwisko@firmaXYZ.pl), adres *e-mail* będzie spełniał kryteria danej osobowej[657]. Trzeba podkreślić, że istotna jest tu możliwość zidentyfikowania osoby. Podanie w adresie ogólnych informacji typu dział i domena firmy, nie daje nam jeszcze możliwości ustalenia tożsamości konkretnej osoby spośród np. pracowników pracujących w danej firmie. Wszelkie niepowtarzalne identyfikatory też mogą być danymi osobowymi, o ile umożliwiają ustalenie tożsamości osoby fizycznej[658]. Istnieje też pewna grupa adresów *e-mail*, które nie są danymi osobowymi. Takim przykładem są adresy przydzielane bezpłatnie, o ile ich treść nie pozwala na identyfikację właściciela (np. użyto pseudonimu), ale i brak jest możliwości ich identyfikacji na podstawie innych posiadanych informacji[659].

Co więcej, w przypadku adresów *e-mail* możliwe jest oprócz prowadzenia korespondencji elektronicznej, także prowadzenie elektronicznego archiwum czy też elektronicznej książki adresowej. Jest to z punktu widzenia ochrony danych osobowych

---

[653] Zob. W. Zimny, *Czy adresy e- mailowe są danymi osobowymi?*, „Biuletyn Ochrona Informacji" 2002, nr 2, s. 8.
[654] Zob. J. Ożegalska-Trybalska, *Adresy e- mailowe a dane osobowe*, „Biuletyn Administratorów Bezpieczeństwa Informacji", grudzień 2001, s. 10-13.
[655] M. Brzozowska, *op. cit.*, s. 36.
[656] X. Konarski, *Komentarz…*, s. 165.
[657] X. Konarski, *Internet i prawo w praktyce*, Warszawa 2002, s. 120.
[658] Zob. A. Drozd, *Ustawa*…, s. 54.
[659] X. Konarski, *Internet…,* s. 120.

proces przetwarzania danych osobowych (np. zbieranie, utrwalanie, przechowywanie, opracowywanie, usuwanie itp.), zatem administrator danych osobowych jest zobowiązany do przestrzegania restrykcji prawnych w zakresie bezpiecznego przetwarzania danych osobowych.

Problematyka adresów IP dopiero od niedawna pojawia się w dyskusjach prawnych. Spowodowane to jest obowiązującym przekonaniem, iż w sieci zapewniona jest anonimowość działań, a wszelkie ruchy w cyberprzestrzeni są niezauważalne. Powstała zatem wątpliwość, czy za pomocą pewnych śladów w sieci można wskazać tożsamość określonej osoby i czy te ślady mogą zostać zakwalifikowane jako dane osobowe. Aby rozwiązać dylemat, czy adres IP należy traktować jako dane osobowe, konieczne jest przedstawienie pokrótce chociaż specyfiki samego adresu sieciowego IP.

Każde urządzenie bezpośrednio podpięte do Internetu posiada własny, unikalny, w danej chwili niepowtarzalny adres, zwany adresem sieciowym IP (*Internet Protocol*), który dla wygody zapisuje się w postaci czterech liczb od 0 do 255, oddzielonych kropkami[660]. Adres IP może być przypisany do jednego, jak i do wielu urządzeń, tworząc wówczas jeden publiczny adres IP, dlatego adres IP wskazuje na obszar, w którym można poszukiwać komputera. Adres IP jest przydzielany posiadaczowi modemu za każdym razem, kiedy chce się on połączyć z Internetem. Zapisuje się on automatycznie i jest automatycznie generowany. W praktyce rozróżnia się IP stałe i zmienne. Adres IP nie musi być przypisany użytkownikowi raz na zawsze, ale np. tylko na czas aktywności danego użytkownika w sieci. Wszelka aktywność danego komputera w sieci będzie więc związana z jego IP, który sprawdza się za pomocą bilingu wskazującego, jaki numer i kiedy łączył się z danym numerem umożliwiającym wejście do Internetu[661].

Stosując się zatem do przesłanek wskazanych w art. 6 u.o.d.o. należy stwierdzić, że adres IP na pewno jest informacją, ale ustalenie czy dotyczy on tylko osoby fizycznej i to takiej, którą można zidentyfikować, jest już problemowe. Identyfikuje on urządzenie typu komputer, telefon mobilny z połączeniem do Internetu itp., za pomocą którego użytkownik loguje się do Internetu. Takie założenie może przesądzić o tym, iż adres IP nie spełnia kryterium klasyfikacji jako dane osobowe. Z drugiej strony jednak poddając analizie przypadki i każdorazowo biorąc pod uwagę możliwości podmiotu, który tym numerem dysponuje, możliwe wydaje się zakwalifikowanie adresu IP jako danej osobowej. Dla

---

[660] J. Petzel, *op. cit.*, s. 296.
[661] M. Brzozowska, *op. cit.*, s. 34.

przedsiębiorcy telekomunikacyjnego, który zawarł z określoną osobą fizyczną (znając jej imię i nazwisko, adres, numer dowodu osobistego itp.) umowę na dostarczenie usług telekomunikacyjnych, bez nadmiernych działań i środków możliwe jest powiązanie określonego numeru z konkretną osobą, której tożsamość jest wówczas w stanie ustalić. W tych okolicznościach adres IP będzie spełniał kryteria z art. 6 u.o.d.o. Dla przeciętnego użytkownika znajomość tylko numeru IP nie warunkuje poznania tożsamości określonej osoby fizycznej, podobnie jak dla moderatora forum, na które może zalogować się dosłownie każdy używając prawdziwych lub fałszywych danych lub też nie podając ich wcale (ta wiedza pozwoli jedynie na przypisanie tego numeru IP konkretnemu dostawcy usług telekomunikacyjnych)[662].

Analizując wytyczne z art. 6 u.o.d.o, można stwierdzić, iż danymi osobowymi są też takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak również na określenie jej tożsamości przy pewnym nakładzie kosztów, czasu lub działań. Opinia Grupy Roboczej ds. Ochrony Danych, powołanej przez Parlament Europejski i Radę Europejską uznała literalnie adres IP za dane dotyczące osoby możliwej do zidentyfikowania, stwierdzając, że: „dostawcy usług internetowych oraz menedżerowie lokalnych sieci mogą, stosując rozsądne środki, zidentyfikować użytkowników Internetu, którym przypisali adresy IP ponieważ systematycznie zapisują w plikach daty, czas trwania oraz dynamiczny adres IP (czyli ulegający zmianie po każdym zalogowaniu) przypisany danej osobie. To samo odnosi się do dostawców usług internetowych, którzy prowadzą rejestr (*logbook*) na serwerze HTTP Nie ma wątpliwości, że w takich przypadkach można mówić o danych osobowych w rozumieniu art. 2 Dyrektywy” [663]. W związku z powyższym jeśli adres IP jest na stałe lub na dłuższy okres przypisany do konkretnego urządzenia, które przypisane jest z kolei konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową[664].

W praktyce możemy się spotkać jednak z sytuacjami, gdy jednoznaczne przypisanie adresu IP do konkretnej, zidentyfikowanej osoby nie jest praktycznie możliwe. Sytuacja taka może wystąpić np. w kawiarenkach internetowych, gdzie komputery udostępniane są klientom bez odnotowywania ich danych identyfikacyjnych. Są to jednak sytuacje wyjątkowe. W wielu przypadkach, nawet przy korzystaniu z komputera w kawiarence internetowej, wykorzystując dane zarejestrowane przez system nadzoru wizyjnego (monitoring)

---

[662] *Ibidem*, s. 35.
[663] Opinia dostępna jest na stronie: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf.
[664] http://www.giodo.gov.pl/319/id_art/2258/j/pl/.

w zestawieniu z innymi danymi (np. dotyczących płatności przy użyciu karty kredytowej), możliwe jest zidentyfikowanie osoby korzystającej w danym czasie z konkretnego komputera.

Z uwagi na okoliczność, że definicja danych osobowych sformułowana w art. 2 dyrektywy 2002/58/WE pokrywa się z definicją podaną w ustawie o ochronie danych osobowych, adresy IP można uznać za dane osobowe. Należy jednak podkreślić, że adres IP będzie uznawany za dane osobowe jedynie wówczas, gdy podmiot przetwarzający adres IP ma jednocześnie dostęp do danych łączących adres IP z innymi danymi identyfikującymi osobę[665]. Do czasu gdy podmiot nie uzyska pewności, że sam nie jest w stanie łączyć adresu IP z innymi danymi identyfikującymi osobę, powinien zabezpieczać adres IP, tak jakby był on daną osobową.

Szczególną uwagę należy przywiązywać do zbiorów obejmujących adresy IP w sytuacji, gdy dochodzi do łączenia podmiotów mogących być administratorami danych osobowych. Może się bowiem okazać, że podmiot dotychczas niemogący łączyć adresu IP z innymi danymi identyfikacyjnymi, uzyskuje taką możliwość po połączeniu podmiotów. W tej sytuacji adresy IP zbierane dotychczas jako dane niemieszczące się w pojęciu danych osobowych, staną się nimi w związku z potencjalną możliwością uzupełnienia ich o dane identyfikacyjne[666].

Podsumowując, można stwierdzić, że sam adres IP komputera nie wyczerpuje definicji danych osobowych, jednak w połączeniu z innymi informacjami umożliwiającymi konkretyzację danej osoby, należy go traktować jako daną osobową, z wszelkimi prawnymi konsekwencjami.

W przypadku „*nicków*" czy nazw użytkowników także powstają wątpliwości, czy należy je uznawać za dane osobowe. Obecnie ani w orzecznictwie, ani w literaturze nie zajęto jednoznacznego stanowiska w tej kwestii. „*Nick*" oznacza skrót (z ang. *nickname* tj. pseudonim), jakim posługuje się dany użytkownik Internetu. Gdy zatem „*nick*" jest pseudonimem kojarzonym z daną osobą, którym posługuje się użytkownik stale (np. na innych portalach, gdzie właściciel „*nicku*" ujawnia swoją tożsamość), wtedy można uznać go za daną osobową. Także w sytuacji gdy osoba użytkująca „*nick*" zdradzi swoją tożsamość i opublikuje swoje dane osobowe pod tym „*nickiem*", wówczas stanie się on daną osobową (dla administratora jest to trudna sytuacja, dlatego też większość z nich postępuje z „*nickami*" tak, jakby były danymi osobowymi)[667]. W większości jednak przypadków „*nick*" nie będzie daną

---

[665] *Ibidem*.
[666] *Ibidem.*
[667] M. Brzozowska, *op. cit.*, s. 37.

osobową, gdyż osoby postronne nie będące ani dostawcami usług, ani administratorami, nie będą miały możliwości poznania tożsamości osoby używającej „*nicku*".

W kontekście nowych kategorii danych osobowych dyskusji poddana jest także klasyfikacja plików *cookies* jako danych osobowych[668]. Pliki te wykorzystywane są do automatycznego rozpoznawania użytkownika w celu wygenerowania odpowiednio spersonalizowanej dla niego strony WWW[669]. „*Cookies"* to małe pliki tekstowe, w których zapisywane są m. in. tzw. sesje, czyli dane pozwalające uwierzytelnić użytkownika na stronach danego serwisu[670] i zależnie od odwiedzanej strony, umieszczane są na komputerze użytkownika, kiedy ten łączy się ze stroną WWW. Pliki *cookies* zawierają informacje wysyłane przez serwer do przeglądarki użytkownika. Zazwyczaj tak gromadzone dane nie są pokazywane przez maszynę użytkownikowi, choć są one zapisywane, śledzone i zatrzymywane na komputerze użytkownika i w jego przeglądarce; pliki te zawierają informacje jednoznacznie identyfikujące komputer użytkownika[671]. Powszechnie pliki te pozwalają tworzyć profile użytkowników i są wykorzystywane w marketingu, a także przy zakupach *online* (dzięki nim strona może identyfikować użytkownika) [672]. Można je wyłączyć, jednak trzeba liczyć się z pewnymi trudnościami przy funkcjonowaniu strony.

Z punktu widzenia ochrony danych osobowych to właśnie ilość i jakość informacji zapisywana w plikach *cookies* pozwalać będzie na ustalenie tożsamości danego użytkownika[673]. Zgodnie z Opinią 1/2008 dotyczącą zagadnień ochrony danych osobowych związanych z wyszukiwarkami[674], pliki typu *cookies* mogą należeć do kategorii danych osobowych, na podstawie których możliwe będzie zidentyfikowanie osoby. Jednak, podobnie jak w przypadku adresów IP, uznanie tych informacji za dane osobowe będzie zależało od charakteru, okoliczności, sposobu i celu, w jakich informacje są zbierane i wykorzystywane.

---

[668] W dyrektywie 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej wskazano, że narzędzia typu *cookies*, jeśli są przeznaczone do prawnie dopuszczalnych celów, takich jak ułatwianie dostarczania usług w społeczeństwie informacyjnym, mogą być wykorzystywane pod warunkiem, że użytkownicy otrzymają dokładną i wyraźną informację, zgodnie z dyrektywą 95/46/WE o celu *cookies*.

[669] X. Konarski, *Internet…,* s. 122.

[670] Przykładem może być poczta e-mail. W sytuacji, gdy użytkownik loguje się na poczcie e-mail, do jego przeglądarki przesyłane są autoryzacyjne pliki *cookies*, zawierające zaszyfrowane dane na temat jego konta. Dzięki temu nie ma potrzeby i konieczności logowania się za każdym razem od początku.

[671] J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 128.

[672] Odmianą plików *cookies* są *pliki flash cookies,* zawarte w banerach wykonanych w technologii flash- występują w większości animacji czy wyskakujących okien. Te pliki od klasycznych *cookies* różnią się m. innym, że nie mogą być przeglądane, blokowane oraz kasowane przez użytkownika za pomocą mechanizmów dostępnych w przeglądarkach internetowych.

[673] M. Brzozowska, *op. cit.,* s. 38.

[674]Opinia Grupy Roboczej Art. 29: 1/2008; dostępna na stronie: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_pl.pdf.

Jeśli zatem pliki *cookies* zawierać będą informacje o charakterze danych osobowych, wówczas posługiwanie się technika *cookies* będzie uznane za przetwarzanie danych. Jeśli pliki *cookies* będą jednak tylko umożliwiały identyfikację danego systemu teleinformatycznego, nie ma wówczas mowy o przetwarzaniu danych osobowych i posługiwaniu się informacjami o charakterze osobowym. Warunkiem stosowania plików *cookies* jest wiedza użytkownika o tym oprogramowaniu. Polski ustawodawca nie uzależnia posługiwania się tego typu oprogramowaniem od uzyskania zgody użytkownika[675].

Mając na uwadze powyższy podział tej nowej kategorii danych osobowych warto pamiętać, iż cyfrowych danych nie można utożsamiać z pojęciem dokumentu elektronicznego. Zgodnie z art. 3 pkt 2 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[676], dokumentem elektronicznym jest stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych. Oznacza to tyle, że jeżeli zapiszemy dane osobowe w pliku tekstowym, w bazie danych na dysku czy katalogu zawierającym pliki dotyczące jednej osoby, będzie to forma przetwarzania danych osobowych. Jeśli te dane będą zapisane i będzie je można traktować jako wyodrębniony zestaw danych, to mamy tu do czynienia z dokumentem elektronicznym. Jeśli natomiast dane nie są w ogóle zapisane na nośniku elektronicznym (np. w przypadku rozmowy na komunikatorze *Skype* czy „Gadu-Gadu" lub dyskusji na czacie czy podczas wypełniania formularza rejestracyjnego na stronach WWW, dopóki formularz nie został zapisany i wysłany), nie ma mowy o istnieniu w tym przypadku dokumentu elektronicznego, ale dane te są danymi cyfrowymi[677]. Nie każdy dokument elektroniczny zatem będzie daną osobową w rozumieniu ustawy o ochronie danych osobowych, a nie każdy dokument elektroniczny będzie zawierał dane osobowe.

Należy zdawać sobie sprawę, że termin dane osobowe zdążył już zakorzenić się w terminologii prawniczej. Dane osobowe stały się słowem kluczowym w obrocie prawnym, jeśli mówimy o ochronie danych osobowych i wszystkich towarzyszących jej procedurach.

Biorąc pod uwagę wszystkie wymagane prawem cechy, które powinny spełniać informacje, by uzyskać miano danych osobowych oraz analizując różnorodne kategorie danych, wyodrębniające się stosunkowo niedawno wraz rozwojem nowoczesnych technologii i coraz częściej funkcjonujące w wirtualnej rzeczywistości, można zaryzykować twierdzenie,

---

[675] M. Brzozowska, *op. cit.*, s. 39.
[676] Dz. U. Nr 64, poz. 565.
[677] M. Brzozowska, *op. cit.*, s. 31.

iż mamy do czynienia z prężnie rozwijającym się nowym rodzajem danych osobowych, które określiłabym mianem cyber-danych. Wykorzystanie różnorodnych systemów sterowania (oddziaływania) w procesach przetwarzania i przekazywania informacji, nierzadko informacji o charakterze osobowym, znacząco wpływa na wyodrębnienie takiej kategorii danych. Współcześnie istniejąca definicja i postrzeganie danych osobowych stanowi podstawę do zrozumienia oraz dalszej analizy ogółu zagadnień ochrony danych osobowych. To jednak, biorąc pod uwagę obecny stan nauki, rozwoju technologii oraz świadomości ludzkiej, jest za mało. Nowoczesne technologie transmisji danych od dłuższego już czasu wymuszają nowe podejście do procesów przetwarzania i myślenia o danych, tak by móc w sposób adekwatny nadążyć za rozwijająca się rzeczywistością. Konieczna jest zatem redefinicja ujęcia danych osobowych oraz uwzględnienie, że w społeczeństwie informatycznym naturalnie kreują się nowe kategorie danych osobowych. Tu istotną rolę pełni organ ochrony danych osobowych, który ma za zadanie odkodować, dookreślić, upowszechnić wiedzę o nich w obrocie prawnym oraz poddać adekwatnej ochronie stosownie do ich specyfiki.

d) przetwarzanie danych osobowych

Wyjaśnienie znaczenia pojęcia przetwarzania danych osobowych i określenie prawnych przesłanek warunkujących jego procesy jest istotne w kontekście różnorodnych działań dokonywanych na danych osobowych oraz ochrony tych danych na gruncie polskiego porządku prawnego.

U.o.d.o wprowadza szczegółowe normy służące realizacji prawa do ochrony danych osobowych. Do tego, aby opisywaną ustawę traktować jako akt kompleksowo regulujący zagadnienia związane z szeroko rozumianą ochroną danych osobowych, przyczynia się niewątpliwie zdefiniowanie przez ustawodawcę pojęcia „przetwarzania danych osobowych”[678]. Na mocy art. 7 pkt 2 u.o.d.o. pojęcie to rozumie się jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych[679].

Z przedstawionego zakresu działań określanych mianem przetwarzania wynika, iż ustawodawca nakazuje przyjęcie wykładni rozszerzającej i uznanie za przetwarzanie

[678] B. Banaszak, K. Wygoda, *op. cit.*, s. 58.
[679] Zob. *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych w roku 2011*, s. 12.

wszelkich operacji dokonywanych na danych osobowych. Nie jest jednak istotne, czy jest to czynność dokonywana w sposób zautomatyzowany, czy też nie. Wskazane znaczenie prawne pojęcia przetwarzania odbiega od potocznego rozumienia tego określenia, zgodnie z którym przez przetwarzanie rozumie się jedynie czynności polegające na dokonywaniu zmian, nadawaniu innego kształtu, formy, przekształcaniu czy przeobrażaniu[680]. Ustawodawca przyjął tak szeroką definicję przetwarzania danych, gdyż nie jest w zasadzie możliwe i jednoznaczne skatalogowanie czynności, które mieściłyby się w pojęciu przetwarzania. Katalog czynności wskazanych w ramach procesu przetwarzania nie jest zamknięty, a jedynie przytoczony przykładowo, na co wskazuje posłużenie się przez ustawodawcę terminem „takie jak".

Jak można sądzić, kolejność operacji wskazana w art. 7 pkt 2 u.o.d.o. nie jest przypadkowa i może być przydatna do określenia ram czasowych danych osobowych, gdyż o przetwarzaniu danych można mówić począwszy od chwili zbierania danych, a skończywszy na ich usunięciu. To przesądza z kolei o zakresie zastosowania ustawy. Ochrona zapewniona jest już z chwilą zbierania danych, aż do czasu ich usunięcia, jak i w trakcie wszelkich czynności dokonywanych na danych osobowych. Zarówno przed zbieraniem, jak i po usunięciu danych nie może być mowy o ich przetwarzaniu i tym samym o zastosowaniu ustawy o ochronie danych osobowych.

Przetwarzanie danych polega na wykonywaniu wszelkich czynności faktycznych na danych osobowych określanych w przypadku podmiotów publicznych jako czynności materialno-techniczne[681]. Nie jest to zatem czynność prawna, a czynność faktyczna, z której wypływają określone konsekwencje prawne[682]. Przetwarzanie może być dokonywane metodami tradycyjnymi (ręcznie) lub w sposób zautomatyzowany (komputerowo, w systemie informatycznym). Przedmiotem zainteresowania prawodawcy są przede wszystkim procesy przetwarzania danych osobowych w zbiorach danych[683] oraz w systemach informatycznych[684], a więc procesy przetwarzania danych w znacznych ilościach, a nie pojedynczych informacji osobowych.

---

[680] *Słownik języka polskiego*, M. Szymczak red., tom II, Warszawa 1978, s. 715.
[681] Por. J. Boć red., *Prawo administracyjne*, Wrocław 2003, s. 353.
[682] Wyrok WSA w Warszawie z dnia 17 listopada 2004 r., II SA/Wa 887/04, LEX nr 164505.
[683] Zbiorem danych w rozumieniu art. 7 pkt 1 u.o.d.o. jest każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Wedle ustawy zatem zbiór powinien wyróżniać się co najmniej trzema cechami; strukturą, posiadaniem danych osobowych oraz dostępnością do nich wedle określonych kryteriów. Zob. I. Zgoliński, I. Zduński, *op. cit.*, s. 43; M. Sakowska, *Pojęcie…,* s. 57-66.
[684] Systemem informatycznym w rozumieniu art. 7 pkt 2a u.o.d.o. jest zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu

Wszystkie wymienione czynności przetwarzania danych osobowych obarczone są obowiązkami wynikającymi z u.o.d.o., jak: obowiązek spełnienia podstaw prawnych dla przetwarzania danych (art. 23 i art. 27), obowiązek informacyjny (art. 24 - art. 25), obowiązek adekwatności, celowości i czasowości przetwarzania danych (art. 26), obowiązki przy udostępnianiu danych (art. 29), obowiązki w razie powierzenia danych (art. 31), obowiązki związane z prawami osób, których dane są przetwarzane (art. 32 - art. 33), obowiązek zabezpieczenia danych (art. 36 – art. 39), obowiązek rejestracji zbioru danych (art. 40), czy obowiązki przy przekazywaniu danych do państwa trzeciego (art. 47 - art. 48)[685].

Rozwijając art. 51 Konstytucji ustawodawca musiał też uregulować podstawowe prawa osób, których dane dotyczą oraz prawa i obowiązki podmiotów-administratorów danych wynikające w faktu przetwarzania przez nie danych osobowych[686]. Do najważniejszym wśród nich należy zaliczyć prawo dostępu do zbiorów danych, urzeczywistniane dzięki możliwości kontroli przetwarzania danych, zwłaszcza poprzez uzyskanie wyczerpujących informacji dotyczących: samego faktu istnienia zbioru, celu, zakresu oraz sposobu przetwarzania znajdujących się w nich danych, a także informacji o jego administratorze, źródle pochodzenia danych, możliwościach ich udostępniania. Ponadto, zgodnie z art. 32 u.o.d.o, dysponentowi danych przysługuje prawo do „żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania bądź ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, do którego zostały zebrane”[687].

Aby prawa owe mogły być realizowane, muszą istnieć odpowiednie sprzężone z nimi obowiązki po stronie administratorów danych[688]. Do najważniejszych spośród nich należą te, które określić można jako związane z informowaniem o przetwarzanych danych, tj.:

- obowiązek zgłoszenia zbioru do rejestracji (art. 40 u.o.d.o.), od wypełnienia którego uzależniona jest w zasadzie możliwość rozpoczęcia przetwarzania danych (art. 46 u.o.d.o);
- obowiązek poinformowania osoby, której dane są zbierane o celu zbierania danych, ich znanych lub przewidzianych odbiorcach, prawie wglądu i poprawiania danych, dobrowolności lub przymusie podania informacji interesujących administratora (oraz o

---

przetwarzania danych. Chodzi tu więc o zautomatyzowane przetwarzanie danych określane też mianem komputerowego przetwarzania danych.

[685] Por. M. Byczkowski, *Zarządzanie procesami przetwarzania danych osobowych*, [w:] *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, red. X.Konarski, G. Sibiga, Warszawa 2007, s. 14.

[686] A. Sakowicz, *Ochrona danych osobowych*, „Jurysta” 2001, nr 10, s. 6.

[687] B. Banaszak, K. Wygoda, *op. cit.*, s. 55.

[688] K. Wygoda, *Ochrona…*, s. 419.

podstawie prawnej tego obowiązku) oraz podania pełnej informacji pozwalającej na identyfikację administratora (art. 24 u.o.d.o.);

- obowiązek odpowiedniego zabezpieczenia zbiorów danych (rozdział 5 u.o.d.o.) wyraźnie nakazujący administratorom zastosowanie takich środków technicznych i organizacyjnych, które zapewniłyby bezpieczeństwo przetwarzania danych w nich zawartych[689]. Powinno się je zabezpieczyć przed udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, uszkodzeniem lub zniszczeniem[690].

Ustawodawca ponadto wprowadził powinność daleko idącej ochrony i restrykcje w zakresie bezpieczeństwa przetwarzania, a także odpowiedzialności, w przypadku naruszenia pewnej kategorii danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, zwanych danymi szczególnie wrażliwymi (sensytywnymi)[691]. Na mocy u.o.d.o. obowiązuje więc generalny zakaz przetwarzania takich danych. Jedynie w art. 27 ust. 2 u.o.d.o. wskazane zostały wyraźnie sytuacje, w których można od tego zakazu odstąpić. Wśród sytuacji umożliwiających przetwarzanie danych wrażliwych znalazły się np. zgoda podmiotu danych (wyrażona tylko na piśmie, której nie można skutecznie wyrazić na przyszłość[692]) oraz inne przesłanki[693], jak np.:

- przepis szczególny[694] innej ustawy[695], który zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;

---

[689] B. Banaszak, K. Wygoda, *op. cit.,* s. 56.

[690] Rozwinięciem tego obowiązku jest wynikający *expressis verbis* z u.o.d.o. a rozszerzony w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z późn. zm.) wniosek, że tylko i wyłącznie osoby na mocy upoważnienia mogą zostać dopuszczone do przetwarzania danych, w tym obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących przetwarzaniu danych.

[691] Katalog danych wrażliwych z art. 27 u.o.d.o częściowo koresponduje z art. 53 ust.7 Konstytucji. Konstytucja przewiduje możliwość ograniczenia uzewnętrzniania religii, ale tylko w drodze ustawy i wyłącznie z ważnych powodów, do których zalicza: konieczność ochrony bezpieczeństwa państwa, ochrony porządku publicznego, ochrony zdrowia i moralności oraz wolności i praw innych osób. Zob. W. Skrzydło, *op. cit.,* s. 56.

[692] A. Drozd, *Ustawa…*, s. 173.

[693] Dyrektywa 95/46/WE w art. 8 ust.4 stanowi, że państwa członkowskie mogą dodatkowo ze względu na ważny interes publiczny, zapewniając odpowiednie gwarancje, ustanowić inne wyjątki od zakazu przetwarzania wrażliwych danych osobowych albo bezpośrednio w prawie krajowym, albo też na podstawie decyzji organu sprawującego nadzór nad ochroną danych osobowych

[694] Do grupy przepisów uchylających zakaz przetwarzania wrażliwych danych osobowych należy zaliczyć chociażby: art. 14 ust. 4 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 30, poz.179 z późn. zm.); art. 22

- przypadki (enumeratywnie wymienione w ustawie), kiedy przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;
- sytuacje, gdy przetwarzanie tej kategorii danych jest niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;
- gdy przetwarzania dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
- gdy przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
- gdy przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
- gdy przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą.

Przesłanki wymienione w art. 27 ust. 2 u.o.d.o. uchylają nie tylko zakaz przetwarzania wrażliwych danych osobowych, lecz również zakaz przetwarzania danych innych niż wrażliwe[696].

Wśród gwarancji dotyczących bezpieczeństwa przetwarzania danych ma swoje miejsce także uregulowana w art. 26 ust. 1 pkt 4 powinność nakazująca administratorom, aby dane były „przechowywane w postaci umożliwiającej identyfikację osób których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania". Ponadto, w celu zażegnania niebezpieczeństwa dyskryminacji oraz zapewnienia jednostkom kontroli treści dotyczących informacji o nich, będących w posiadaniu organów państwa, zabronione jest nadawanie

---

ust.4 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 z późn. zm.; art. 10a ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. Nr 78, poz. 462 z późn. zm.). Zob. A. Drozd, *Ustawa…*, s. 175-176.

[695] Art. 27 ust. 2 pkt 2 u.o.d.o. przesądza o tym, że tylko przepis zawarty w akcie normatywnym o randze ustawy może zezwolić na przetwarzanie wrażliwych danych osobowych. Możliwe jest także powołanie się na przepis zawarty w akcie normatywnym o miejscu wyższym w hierarchii źródeł prawa niż ustawa. Zob. A. Drozd, *Ustawa…*, s. 174.

[696] A. Drozd, *Ustawa…*, s. 172.

ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne, a numery stosowane w ewidencji ludności mogą zawierać tylko oznaczenie płci, daty urodzenia, numer nadania oraz liczbę kontrolną (art. 28 ust. 2 i 3 u.o.d.o). Art. 28 ust. 2 ustanawia zatem szczególny typ danych osobowych i są to numery porządkowe stosowane w ewidencji ludności[697]. Zgodnie z art. 8 ust.7 dyrektywy 95/46/WE państwa członkowskie określą, pod jakimi warunkami może być przetwarzany narodowy numer identyfikacyjny lub inny identyfikator powszechnego stosowania. Stąd art. 28 ust. 2 wprowadza w tym zakresie jedynie zakaz nadawania znaczeń innych niż w nim wskazane, a art. 28 ust. 3 zakaz nadawania znaczeń ukrytych elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne. Powyższe nie przeczy jednak zgodności tego przepisu z dyrektywą 95/46/WE, gdyż ustawodawca wskazał w tym zakresie warunki przetwarzania, tj. zakaz wykonywania na tym typie danych osobowych operacji nadawania im innych znaczeń niż określone w art. 28 ust. 2 i ust. 3[698].

W u.o.d.o. pojawiają się obowiązki mające na celu wypełnienie i uściślenie zapisów ogólniejszych (chociażby tych, które wynikają z art. 23 u.o.d.o., a dotyczące ogólnych warunków dopuszczalności przetwarzania danych). Aby spełnić ustawowe wymogi dotyczące bezpiecznego przetwarzania danych osobowych, należy przestrzegać głównych zasad postępowania przy przetwarzaniu danych osobowych wyznaczonych w art. 26 ust. 1 u.o.d.o., ujmującym je w formę podstawowych obowiązków administratora danych[699]. Z jego treści wynika, że administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie, ma on przestrzegać określonych zasad.

Zasada legalności oznacza, że dane mogą być przetwarzane tylko zgodnie z prawem[700]. Przesłanka celowości nakazuje, aby dane były zbierane tylko dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, jeśli jest to niezgodne z

---

[697] Do kategorii numerów porządkowych stosowanych w ewidencji ludności należy zaliczyć numer nadawany na podstawie przepisów zawartych w rozdziale 7 a ustawy z 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. Nr 14, poz. 85 z późn. zm.); jest to numer powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL).

[698] Zob. A. Drozd, *Ustawa…*, s. 189.

[699] Zgodnie z treścią art. 7 pkt 4 u.o.d.o administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych. Między innymi może to być organ państwowy, organ samorządu terytorialnego lub państwowa albo komunalna jednostka organizacyjna.

[700] Zwrot „przetwarzanie zgodnie z prawem" został użyty wystarczająco szeroko, by objąć nim wszystkie normy prawne obowiązujące zgodnie z przyjętą w Konstytucji RP koncepcją źródeł prawa. Dotyczy zgodności przetwarzania danych osobowych z szeroko pojętym porządkiem prawnym, którego częścią są zasady współżycia społecznego. Zob. A. Drozd, *Ustawa…*, s. 157.

tymi celami[701]. Zasada merytorycznej poprawności określa, że dane powinny być merytorycznie poprawne[702] a zasada adekwatności wskazuje, by dane były adekwatne w stosunku do celów, w jakich są przetwarzane[703]. Zasada ograniczenia czasowego określa, że dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie mogą być przetwarzane dłużej niż jest to niezbędne do osiągnięcia celu, dla którego zostały zebrane[704].

Wart przypomnienia jest także fakt, iż pierwotnie w ustawie uregulowane były także kwestie udostępniania i odmowy udostępniania danych osobowych w trybie art. 29 i art. 30 u.o.d.o.[705]. Na mocy tych przepisów osoba starająca się o udostępnienie jej danych musiała bądź wskazać na przepisy, które upoważniają ją do uzyskania danych, bądź uzasadnić w sposób wiarygodny potrzebę posiadania danych, przy zastrzeżeniu, że ich udostępnianie nie naruszy praw i wolności osób, których dane dotyczą[706]. Nie oznacza to jednak zasadniczego ograniczenia udostępniania danych, ale jedynie konieczność dokonywania oceny dopuszczalności udostępniania danych na podstawie przesłanek dopuszczalności przetwarzania danych, określonych przepisami art. 23 i art. 27 u.o.d.o.

---

[701] Związany jest z tym np. obowiązek zbierania tylko takich danych, które są niezbędne do realizacji celu, dla którego podejmowane jest ich zbieranie (art. 35 ust.1 u.o.d.o. w związku z art. 51 ust. 2 Konstytucji). Cele muszą być oczywiście oznaczone i zgodne z prawem, a dalsze przetwarzanie owych danych nie powinno być niezgodne z tymi celami. Dane musza być merytorycznie poprawne i adekwatne do tych celów (art. 26 ust. 1 pkt 2 i 3 u.o.d.o.) .

[702] Administrator danych jest obowiązany również zapewnić poprawność danych osobowych. Obowiązek ten obejmuje m. in. aktualizowanie danych osobowych, odnotowywanie poszczególnych zmian danych osobowych. Jego naruszeniem jest natomiast zbieranie danych ze źródeł niewiadomego pochodzenia, które nie gwarantują poprawności danych osobowych. Zob. A. Drozd, *Ustawa…s*, s. 162.

[703] Zakres danych osobowych adekwatnych do celu przetwarzania oceniać trzeba każdorazowo uwzględnieniem konkretnego stosunku, w związku z którym administrator danych przetwarza dane osobowe. Zob. wyrok NSA z dnia 27 listopada 2003 r., II SA 209/03, dostępny na: www.giodo.gov.pl.

[704] *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych w roku 2011,* s. 12.

[705] Przepisy dotyczące udostępniania danych tj. art. 29 i 30 u.o.d.o. zostały uchylone na mocy nowelizacji u.o.d.o. ustawą z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych.

[706] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*,s. 104.

ROZDZIAŁ IV
POZYCJA USTROJOWA
GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

1. GIODO jako organ państwowy

a) uwagi ogólne

Ponadnarodowe regulacje poświęcone prywatności i danym osobowym wyznaczały merytoryczne standardy ich ochrony, jednak szczegółowe mechanizmy i narzędzia ochrony stanowiły już indywidualną sprawę każdego państwa. W latach 90. XX w. nastąpił przełom w międzynarodowej ochronie prywatności i ochronie danych osobowych, zakładający konieczność powołania specjalnego organu ds. ochrony danych osobowych na szczeblu krajowym. Najważniejszym wyznacznikiem pozycji tego organu miała być jego niezależność. Organ ten powinien gwarantować bezstronność, być niezależnym w stosunku do osób i urzędów odpowiedzialnych za tworzenie i przetwarzanie danych, a także posiadać odpowiednie możliwości techniczne do działania. Ważnym czynnikiem prawnej pozycji takiego organu jest także sposób jego funkcjonowania oraz przyznane mu kompetencje.

Konsekwencją realizacji międzynarodowych wytycznych w zakresie powołania niezależnego organu ochrony i nadzoru w zakresie ochrony prywatności, w tym ochrony danych osobowych, stało się wprowadzenie do polskiego porządku prawnego na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych organu Generalnego Inspektora Ochrony Danych Osobowych. W ten sposób został zrealizowany przez ustawodawcę cel utworzenia instytucjonalnych gwarancji przestrzegania i realizowania praw oraz obowiązków wynikających z u.o.d.o[707].

Od początku obowiązywania ustawy pojawiały się rozbieżności co do konkretnego określenia pozycji ustrojowej GIODO, w tym określenia jego miejsca w systemie organów państwowych. Przedstawienie trafnej klasyfikacji tego organu, jakim jest GIODO, na tle innych organów w Polsce nie jest łatwym zadaniem, jednak jest to dodatkowa motywacja do

[707] Zob. S. Sagan, *Generalny Inspektor Ochrony Danych Osobowych w Polsce,* Warszawa 2011, s. 120.

zgłębienia tej problematyki. Podejmując więc próbę umiejscowienia GIODO pośród tych organów, za punkt wyjścia przyjmę przedstawienie klasyfikacji organów w Polsce.

b) definicja organu państwowego

Ogół organów państwowych oraz wszelkie siły polityczne i społeczne związane z funkcjonowaniem organizacji państwowej (w tym także partie polityczne, grupy nacisku, związki zawodowe, organizacje pozarządowe, samorządy zawodowe i gospodarcze) tworzą mechanizm państwowy[708]. Aby możliwa była realizacja władzy w państwie, potrzebny jest odpowiednio zorganizowany i wyposażony aparat, zwany aparatem państwowym. Pod tym pojęciem rozumie się zespół ludzi powołanych do wypełniania zadań państwa w trybie określonym przez prawo i w tym celu wyposażony w specyficzne środki prawne, włącznie z prawem stosowania przymusu państwowego[709]. Aparat państwowy współczesnego państwa jest obszerną i zróżnicowaną wewnętrznie strukturą, której podstawowym elementem są organy państwowe, za pomocą których państwo spełnia swoje różne funkcje[710]. Organ państwowy można określić zatem jako część składową aparatu państwowego.

Dokonując konstytucyjnoprawnej analizy pojęcia „organ państwowy" należy także sprecyzować pojęcia „grupa organów państwowych" i „system organów państwowych". Aby zostały urzeczywistnione funkcje państwa, z reguły nie jest wystarczające działanie tylko jednego organu, muszą zostać powołane ich grupy. Grupą organów państwowych jest określany ogół organów państwowych wykonujących tę samą funkcję państwa, podobnie ukształtowanych i skupionych w jednym pionie organizacyjnym według określonej hierarchii[711]. Ogół poszczególnych grup organów tworzy system organów państwowych, gdyż rację bytu ma działanie organów w powiązaniu z innymi a nie w izolacji. Posługując się powszechnie spotykanym określeniem w nauce prawa konstytucyjnego, system organów państwowych określany jest jako całokształt cech wyróżniających formę organizacji aparatu państwowego, a w szczególności reguły określające jego budowę, formy organów

---

[708] Z. Husak, *Struktura organów władzy publicznej,* [w:] *Konstytucyjny system organów państwa*, D. Dudek, Z. Husak, G. Kowalski, W. Lis, Warszawa 2013, s. 39.
[709] W. Skrzydło, *System organów państwowych,* [w:] *Ustrój polityczny RP w świetle Konstytucji z 1997 roku*, Kraków 2007, s. 120.
[710] S. Sagan, *Pojęcie organu,* [w:] *Organy i korporacje ochrony prawa*, red. S. Sagan, J. Ciechanowska, Warszawa 2010, s. 16.
[711] R. M. Małajny, *Systematyka polskich organów państwowych i ich charakter prawny*, „Studia Prawnicze" 1989, z. 1, s. 4.

państwowych i wzajemny ich stosunek[712]. System organów państwowych ma spełniać określoną rolę; jest on powołany do realizacji zasad, na jakich został zbudowany ustrój polityczny państwa: demokratyczny, antydemokratyczny czy autorytarny. Każda konstytucja państwa musi zawierać zasady i regulacje w zakresie systemu organów państwowych, a ściślej ujmując, określać pozycję prawną, rolę ustrojową i wzajemne stosunki organów państwowych[713].

Pojęcie „systemu organów państwowych" nie jest synonimicznym terminem dla aparatu państwowego, który definiowany jest jako zespół instytucji (a więc nie tylko organów) służących realizacji zadań państwa[714]. Systemu organów państwowych nie należy także identyfikować z systemem rządów (tzw. inżynierią ustrojową)[715]. Pojęcia „organ" nie oznacza też „urzędu" państwowego. Chociaż pojęcia te bywają używane jako tożsame (np. w Konstytucji RP w art. 130 i art. 151 dotyczących treści przysięgi składanej przez Prezydenta RP i Prezesa RM), to najczęściej „urząd" rozumiany jest jako aparat pomocniczy przyznany organowi do pomocy w realizacji jego zadań (zespół ludzi i środków materialnych, np. urząd wojewódzki). Od organu państwowego odróżnić także trzeba konkretną osobę, która korzysta z kompetencji organu i bywa określana piastunem organu.

Podstawowy podział organów władzy publicznej zakłada podział na organy państwa i organy samorządu terytorialnego, gdyż normy prawa mogą powierzyć kompetencje państwa nie tylko organom państwa, ale i samorządowi terytorialnemu czy organizacji społecznej (zadania zlecone)[716].

Teoria organów państwowych, ich struktury, klasyfikacji czy wzajemnych prawnych i funkcjonalnych związków jest centralnym zagadnieniem z zakresu teorii państwa i nauki o ustrojach państwowych. Podstawy prawne dotyczące struktur i zasad funkcjonowania organów państwa stanowią materię konstytucyjną, gdyż łączy się to bezpośrednio ze sprawowaniem władzy politycznej w państwie[717]. Organizacja władzy wymaga więc

---

[712] Zob. W. Skrzydło, *Konstytucyjne założenia systemu organów państwa i ich wpływ na kształt aparatu państwowego,* [w:] *Ustrój i struktura aparatu państwowego i samorządu terytorialnego,* red. W. Skrzydło, Warszawa 1997, s. 8.
[713] W. Skrzydło, *Konstytucyjne…*, s. 7.
[714] J. Galster, *System organów państwowych,* [w:] *Prawo konstytucyjne*, red. Z. Witkowski, Toruń 2013, s. 65.
[715] *Ibidem,* s. 66.
[716] Tak: W. Orłowski, *Organy władzy publicznej oraz system organów państwa,* [w:] *Konstytucyjny system organów państwowych*, red. E. Gdulewicz, Lublin 2009, s. 107. Organy państwa powołane są do realizacji różnorodnych zadań, leżących w zakresie konstytucyjnych kompetencji państwa, zaś organy samorządu terytorialnego stanowią przykład organów wykonujących zadania z zakresu władzy wykonawczej, pełnią więc rolę zdecentralizowanej administracji i mogą być przeciwstawione administracji rządowej.
[717] S. Sagan, *Pojęcie…*, s. 15.

elastycznych rozwiązań przyjmujących postać organów państwowych wykonujących funkcję państwa[718].

Termin „organ" pochodzi od łacińskiego słowa *organum*, co oznacza narzędzie. Jak słusznie zauważa J. Trzciński, nie ma ustawowej definicji organu państwa, są natomiast określenia tego pojęcia podane przez naukę. Doktryna z kolei nie zawsze konstruuje definicję organu państwa na podstawie lektury aktów prawnych, gdyż akty prawne posługują się nieprecyzyjnie tym pojęciem, nie wskazując nigdzie, jakie podmioty zaliczyć można do organów państwa[719]. Akty normatywne używają terminu „organ państwa" w różnych znaczeniach (np. władza, urząd), stąd można przyjąć za autorem, że w Konstytucji i ustawach termin „organ państwa" użyty jest jako termin techniczny na oznaczenie pewnych jednostek organizacyjnych posiadających charakterystyczne cechy[720]. Także S. Sagan zwraca uwagę, że pojęcie „organu państwowego" nie jest ujmowane w literaturze przedmiotu jednolicie, co nie wynika, zdaniem autora, z rozbieżności merytorycznych, a raczej z faktu przyjęcia odmiennych koncepcji definicyjnych[721].

Generalnie przez organ rozumie się wewnętrzną jednostkę organizacyjną danego podmiotu prawa, która wyposażona jest w uprawnienie wyrażania woli tego podmiotu, co opiera się na obowiązującym prawie, a nie na pełnomocnictwie udzielonym mu przez dany podmiot[722]. Uprawnienie do wyrażania woli danego podmiotu zwykle ujęte jest w formie zadań i kompetencji danego organu, dlatego też nie każda jednostka organizacyjna będzie organem, a tylko taka, która posiada określone kompetencje do wyrażania woli danego podmiotu.

Wobec sporów terminologicznych istniejących wokół pojęcia „organ państwa" i braku jednej, powszechnie przyjmowanej w nauce prawa konstytucyjnego definicji, należałoby się ograniczyć zatem do wskazania kilku cech definiujących jego zakres. Do swoistych cech wyróżniających poszczególne organy państwowe zaliczyć zatem należy: usytuowanie w całym systemie organów (pozycja ustrojowa), specyficzne zadania, zakres kompetencji, formy i tryb działania oraz budowę (strukturę)[723].

---

[718] J. Galster, *op. cit.,* s. 65.
[719] J. Trzciński, *Pojęcie konstytucyjnego organu państwa socjalistycznego*, Warszaw-Kraków- Gdańsk 1974, s. 52.
[720] J. Trzciński, *op. cit.,* s. 56-57; Konstytucja RP stosunkowo rzadko odwołuje się do tego pojęcia, np. art. 210 Konstytucji RP formułujący zasadę niezależności RPO od innych organów państwowych.
[721] Zob. S. Sagan, *Pojęcie…,* s. 16.
[722] Por. S. Serafin, B. Szmulik, *Organy ochrony prawnej RP*, Warszawa 2010, s. 5.
[723] Zob. S. Jarosz-Żukowska, *Organ państwowy,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, red. W. Skrzydło, S. Grabowska, R. Grabowski, Warszawa 2009, s. 325.

Organ państwa określić można jako celowo zorganizowany i wyraźnie wyodrębniony zespół ludzi i środków, utworzony i działający na podstawie prawa, wykonujący w imieniu państwa określone zadania i mogący dla ich realizacji korzystać ze środków władczych i stosować przymus państwowy[724]. Organ musi być wyposażony w określony przez przepisy prawa zakres kompetencji do wykonywania działań w imieniu państwa, indywidualny i wyróżniający go od innych organów czy jednostek organizacyjnych[725]. Kompetencji organów państwa nie można domniemywać, opierać jej na wykładni celowościowej lub funkcjonalnej, lecz musi być ona jasno i precyzyjnie określona w przepisie prawa[726]. W demokratycznym państwie prawnym, stosownie do treści art. 7 Konstytucji RP (zasada legalizmu), organy państwowe działają na podstawie prawa i w granicach prawa, przez co rozumie się, że ich byt określa ustawa zasadnicza lub ustawy zwykłe, ale nigdy akty prawne niższego rzędu. Prawo określa nie tylko podstawy prawne, ale i granice działania organów państwa. Organy nie tylko mają działać na podstawie prawa , ale i tego prawa przestrzegać. Przez granice ich działania należy rozumieć nie tylko określenie materialnych kompetencji organu, lecz także stworzenie procedury ich wykonywania, co oznacza, że organy wydają swoje rozstrzygnięcia w określonej przez prawo formie, posiadając stosowną do tego podstawę prawną[727]. Adresatami, do których jest bezpośrednio skierowana zasada legalizmu, są wszystkie organy państwowe bez względu na ich klasyfikację jako organów sprawujących władzę ustawodawczą, wykonawczą lub sądowniczą czy pozostawania poza trójpodziałem, a także niezależnie od posiadania właściwości ogólnopaństwowej czy terytorialnie ograniczonej[728]. Przymiotnik „państwowy" może oznaczać „stanowiący część państwa", jak i „wykonujący uprawnienia przyznane przez państwo"[729].

Niewątpliwie z funkcjonowaniem organu państwa związana jest możliwość stosowania przymusu państwowego, tj. możliwość stosowania przez organy państwa środków wynikających z władczych funkcji państwa. Jest to cecha właściwa tylko organom państwa, która zarazem odróżnia organ od instytucji społecznych. Na zewnątrz korzystanie ze środków władczych przejawia się w uprawnieniu do stanowienia aktów prawnych posiadających moc

---

[724] Por. S. Serafin, B. Szmulik, *op. cit.*, s. 5.
[725] Kompetencja to zdolność organu do stosowania prawne określonych środków działania w celu zrealizowania powierzonych mu zadań. Jest to nie tylko uprawnienie, ale kompetencja nakłada na dany organ obowiązek podjęcia określonych działań. Kompetencje organu maja zazwyczaj charakter władczy (imperium), co oznacza, że organ ma prawo decydowania (określania) o prawach lub obowiązkach innych osób.
[726] Zob. orzeczenie TK z dnia 23 marca 2006 r. sygn. K 4/06, OTK ZU2006, seria A, nr 3, poz. 32, s. 351.
[727] W. Orłowski, *op. cit.*, s. 108.
[728] Zob. W. Sokolewicz, *Art. 7*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, Warszawa 2007, s. 7
[729] M. Wierzbowski red., *Prawo administracyjne*, Warszawa 2011, s. 112.

obowiązującą, zagwarantowanym możliwością zastosowania środków przymusu państwowego w celu doprowadzenia do ich wykonania[730].

Aby organy państwa mogły należycie wypełniać swoje obowiązki, stosownie do stawianych im zadań, wyposażone zostały także w środki materialno-techniczne. Funkcję pomocniczą względem organów państwa pełni aparat administracyjny, który stanowi jednostka lub ogół jednostek o charakterze osobowo-technicznym. Jego zadaniem jest obsługa organu poprzez umożliwienie techniczno-praktyczne wykonywania przez organ jego zadań.

Kompetencje organów państwowych powinny obejmować całość zadań państwa, ale by było to możliwe, muszą być one odpowiednio zorganizowane. Ogół organów państwa powinien tworzyć spójny i uporządkowany układ stosunków, pozwalający na uznanie całości jako zorganizowany system elementów określany systemem organów państwowych. Termin ten oznacza celowo i w szczególny sposób zorganizowaną całość organów państwa wypełniających zadania państwa. System organów państwowych charakteryzują dwie zasadnicze cechy: spójność i niesprzeczność. Spójność oznacza, że system tworzy zwartą całość, co jest możliwe poprzez współuzależnienie i powiązanie ze sobą wszystkich jego elementów. Niesprzeczność zakłada, że w systemie nie występują przeciwstawne cele i zadania, które realizowałyby poszczególne organy państwowe[731].

Można zatem przyjąć, iż organem państwowym jest wyodrębniona jednostka organizacyjna państwa, która składa się z zespołu ludzi i środków materialnych i realizuje zadania państwa o swoistych cechach. Organ państwowy powołany jest do wykonywania zwierzchniej władzy, której egzystencja i każdorazowe działanie w imieniu państwa (wyrażające wolę państwa) ma wyraźną podstawę prawną; korzysta z określonego prawem zakresu kompetencji i środków działania, wyróżniającego go względem innych podmiotów i jest uprawniony do korzystania ze środków władczych i stosowania przymusu państwowego dla zabezpieczenia realizacji swoich zadań[732].

c) klasyfikacja organów państwowych

Organy państwowe różnią się między sobą wieloma aspektami, a różnorodne kryteria determinują klasyfikację tych organów. Trzy najważniejsze kryteria to: zróżnicowanie pod względem kompetencji, czyli zadań powierzonych im do realizacji, zróżnicowanie pod

---

[730] Zob. E. Ochendowski, Prawo *administracyjne. Część ogólna*, Toruń 2013, s. 245.
[731] *Ibidem*, s. 39-40.
[732] Por. S. Jarosz- Żukowska, *Organ państwowy…*, s. 325.

względem budowy wynikającej z przyjętej przez ustawodawcę konstrukcji oraz zróżnicowanie pod względem trybu działania. Nie bez znaczenia na klasyfikację organów państwa pozostaje wpływ zasad ustroju politycznego państwa, które są zarazem katalogiem konstytucyjnych zasad sytemu organów państwowych. Jedne z nich mają większe, inne mniejsze znaczenie, jednak analizując poszczególne rodzaje i typy organów państwowych można ustalić związek pomiędzy strukturą organów a wspomnianymi zasadami.

Podział i klasyfikacja organów państwa zostały wypracowane przez doktrynę, a nie przez ustawodawcę konstytucyjnego, który proklamując zasadę podziału władzy, tym samym ustanowił organy ustawodawcze, wykonawcze i sądownicze. Na tej podstawie można ustalić ścisły związek pomiędzy zasadą podziału władzy a klasyfikacją organów państwowych. Podział władzy jest współcześnie związany z istotą demokratycznego państwa prawnego oraz uznawany za jedną z kluczowych jego wartości i głównych założeń konstytucyjnych. Ideę tego podziału „stanowi – zwłaszcza w obliczu zagrożeń, którym podlega współczesna demokracja – wyznacznik tożsamości konstytucjonalizmu, zarówno ze względu na jej znaczenie dla afirmacji i zagwarantowania praw człowieka, jak też jej rolę w dziedzinie kształtowania struktury i reguł funkcjonowania państwa demokratycznego”[733]. Wynikające z tej zasady konsekwencje – odrębność organizacyjna władzy ustawodawczej, wykonawczej i sądowniczej, niepołączalność stanowisk w różnych władzach i wzajemne ich na siebie oddziaływanie - powodują konieczność wprowadzenia do ustawy zasadniczej określonych uregulowań prawnych[734]. Mechanizm działania zasady trójpodziału władzy prowadzi nie tylko do rozdzielenia władz i tym samym organów w zakresie poszczególnej władzy, ale także do odpowiedniego wzajemnego ich usytuowania[735].

Sens podziału władzy polega na tym, iż prawna sfera działania przypisana jednemu organowi nie może być wykonywana przez organ realizujący inną sferę oraz żaden organ nie może wywierać – bezpośrednio lub pośrednio – dominującego wpływu na pozostałe organy. Nie ma tu mowy o separacji władzy (co oznacza sytuację, w której brak jest jakichkolwiek więzi pomiędzy oddzielanymi częściami), a jedynie o rozdzieleniu, które zakłada pewne minimum wewnętrznego powiązania[736]. Pozycje władz, a tym samym organów, jak wynika z

---

[733] Zob. R. Piotrowski, *Zasada podziału władz w Konstytucji RP*, „Przegląd Sejmowy” 2007, nr 4, s. 114.
[734] Zob. W. Skrzydło, *Konstytucyjne…,* s. 9.
[735] Zob. A. Pułło, *O jedno rozumienie podziału władz w nauce prawa konstytucyjnego*, „Państwo i Prawo” 1983, z. 6, s. 30-45.
[736] Zob. R. M. Małajny, *Zasada rozdziału władzy państwowej – prolegomena,* [w:] *Państwo i prawo wobec współczesnych wyzwań. Teoria i filozofia państwa i prawa oraz aksjologia demokracji i ochrony praw człowieka. Księga jubileuszowa Profesora Jerzego Jaskierni*, red. R.M. Czarny, K. Spryszak, Toruń 2012, s. 375.

klasycznych reguł podziału władzy, powinny być równorzędne, przez co rozumie się formalną niezależność i równorzędność organów oraz przynajmniej ich względną równowagę. W praktyce jest to jednak trudne do osiągnięcia z uwagi na różny rozkład sił politycznych w społeczeństwie, ukształtowanego w państwie systemu partyjnego czy innych czynników. Jak zauważa R. M. Małajny, „wymóg równowagi należy odczytywać przede wszystkim jako zakaz nadmiernego uzależnienia działania jednej grupy organów od drugiej, gdyż prowadziłoby to do supremacji tej ostatniej[737].

Zasada podziału władzy wyrażona w art. 10 Konstytucji RP okazuje się być obecnie problematyczna zwłaszcza w odniesieniu do klasyfikacji i podziału organów państwowych. Nie da się zmieścić bowiem w ramach sztywnego trójpodziału władzy wszystkich organów pełniących zróżnicowane funkcje we współczesnym państwie. Oczywiście, z uwagi na cechy właściwe i charakterystyczne poszczególnym władzom, organy władzy ustawodawczej, wykonawczej i sądowniczej bez problemu i jednoznacznie można zakwalifikować odpowiednio w obrębie każdej z tych władzy[738]. Współczesne konstytucje ustanawiają podstawy funkcjonowania wielu organów, wobec których klasyfikacja z czasów Monteskiusza okazuje się być jednak zawodna lub kontrowersyjna. Przykładem mogą być organy określone w polskiej ustawie zasadniczej jako organy kontroli państwowej i ochrony prawa (rozdział IX Konstytucji RP). Na tle założenia, które formułuje art. 10 Konstytucji RP stanowiącego o ścisłym trójpodziale władzy, organy te stanowią inną władzę, a koncepcja trójpodziału rozszerzyć się może w tym wypadku do formuły trzy plus jeden[739]. Jak uważa A. Sylwestrzak, „za taką interpretacją przemawia nie tylko systematyka Konstytucji RP, lecz głównie specyfika zadań organów kontroli w rzeczy samej pozostających poza trójpodziałem. Nie można ich w żaden sposób identyfikować z którąkolwiek z władz w ich Monteskiuszowskim rozumieniu, a zatem kontrola powinna być wyodrębniona, pozostając poza tradycyjnym trójpodziałem, tworząc osobną władzę konstruowaną w określonych relacjach z pozostałymi”[740].

Polski Trybunał Konstytucyjny skonstatował: „Historycznym celem zasady trójpodziału władzy była ochrona praw jednostki przed nadużyciami ze strony

---

[737] *Ibidem*, s. 377.

[738] Inne stanowisko przedstawia np. R. M. Małajny, który stwierdza, że o ile precyzyjnie zostały określone jedynie organy władzy prawodawczej, tj. Sejm i Senat, to wyliczenie organów wykonawczych jest jedynie przykładowej natury. Autor wskazuje, iż uznanie Prezydenta RP za organ władzy wykonawczej a Trybunału Konstytucyjnego za organ władzy sądowniczej jest mocno dyskusyjne. Por. R. M. Małajny, *Zasada…*, s. 381.

[739] Zob. A. Sylwestrzak, *Konstytucja RP z 1997 r. – nowe interpretacje podziału władz,* [w:] *Dziesięć lat Konstytucji Rzeczypospolitej Polskiej*, red. E. Gdulewicz, H. Zięba –Załucka, Rzeszów 2007, s. 269.

[740] Autor stwierdza, iż taka formuła czterech władz wydaje się całkowicie do przyjęcia na tle art. 10 Konstytucji RP, dowodząc jedynie pogłębiania procesów samokontroli władz i ich współdziałania. *Ibidem,* s. 269.

któregokolwiek organu państwowego. Ten cel pozostaje nadal ważny współcześnie, gdyż zasada podziału władz, chociaż dotyczy struktury i funkcjonowania władz państwowych «jest organicznie powiązana z wolnościowym statusem jednostki»"[741]. Zaznaczyć jednak należy, iż współcześnie modyfikowana jest pierwotna istota zasady trójpodziału władzy, której rozumienie ma być dostosowane do nowych zadań i mechanizmów funkcjonowania państwa i nie jest chyba przesadzona opinia, że nastąpiło „oderwanie się treści tej zasady od jej genezy"[742]. W obecnych czasach nie jest możliwa do zrealizowania w sposób dosłowny i absolutny koncepcja Monteskiusza, co wiązać należy ze skomplikowanym procesem sprawowania władzy w państwie. Organy państwowe realizują funkcje, które nie należą do istoty władzy, skutkiem czego dochodzi do krzyżowania i mieszania się sfer aktywności i uprawnień poszczególnych organów. To wszystko nie oznacza rezygnacji z idei podziału władzy, jednak stanowi o jej zmodyfikowanym charakterze.

Mając na uwadze powyższe ustalenia, można stwierdzić, iż określony model realizacji władzy determinuje istnienie poszczególnych rodzajów organów w państwie. Model realizacji władzy powinien określać jej podmiot, formy i sposoby działania, zakres, ale także cele i funkcje[743]. Słusznie zauważa R. M. Małajny, że racjonalny ustawodawca konstruując system organów państwowych, winien najpierw wyodrębnić funkcje państwa, czyli główne kierunki jego działalności, a przeprowadzenie organizacyjnego podziału aparatu państwowego na poszczególne organy lub ich grupy powinno zostać poprzedzone funkcjonalnym wyodrębnieniem odpowiednich sfer działania tego aparatu[744].

Wyodrębniając więc funkcje, czyli odpowiednie sfery działania aparatu państwowego, za podstawę uznajemy wspomniany wcześniej trójpodział władzy i rozróżnienie trzech podstawowych funkcji państwa: stanowienie prawa, administrowanie i nadzór przestrzegania prawa. Dokonując dalszych podziałów, sfera nadzoru nad przestrzeganiem prawa da się podzielić na wymierzanie sprawiedliwości oraz na kontrolę. W ramach wymiaru sprawiedliwości można wyróżnić dwie funkcje: ściganie przestępstw i sądzenie ich sprawców; w ramach kontroli można wyodrębnić kontrolę działalności organizacyjnej i merytorycznej oraz kontrolę konstytucyjności prawa[745]. W sumie prowadzi to do wyodrębnienia sześciu funkcji państwa: stanowienia prawa, administrowania, ścigania

---

[741] Postanowienie TK z dnia 8 czerwca 2009 r., SK 26/07; OTK-A 2009, nr 6, poz. 92.
[742] P. Sarnecki, *Współczesne rozumienie podziału władzy,* [w:] *Nowa konstytucja RP. Wartości, jednostka, instytucje*, red. K. B. Janowski, Toruń 1991, s. 20.
[743] Por. W. Skrzydło, *Konstytucyjne…,* s. 14.
[744] R. M. Małajny, *Systematyka…*, s. 3.
[745] W. Skrzydło, *Konstytucyjne…*, s. 14.

przestępstw, sądzenia, kontroli działalności organizacyjnej i kontroli przestrzegania prawa[746]. Rozróżnienie tych funkcji pozwala na przyjęcie założenia, iż - z uwagi na odrębność każdej z nich - powinny być one realizowane za pomocą odpowiednich form organizacyjnych. Stąd, stosownie do wyróżnionych wyżej funkcji państwa, w nowoczesnym państwie można wskazać za R. M. Małajnym następujące grupy organów państwowych: prawodawcze, wykonawcze i organy nadzoru nad przestrzeganiem prawa, (tj. sądy, prokuraturę, organy kontroli i Trybunał Konstytucyjny działający w zakresie kontroli konstytucyjności prawa)[747].

Aby dostosować do dzisiejszego funkcjonowania aparatu państwowego i charakteru działania organów państwowych istotę i sens podziału organizacyjnego władzy, w doktrynie prawa konstytucyjnego powstały dwie koncepcje: koncepcja domniemań kompetencyjnych i koncepcja rdzenia kompetencji.

Koncepcja domniemań kompetencyjnych opiera się na „ocenie charakteru poszczególnych uprawnień władczych" i zakłada, że „kompetencje dające się w miarę jednoznacznie określić z uwagi na treść, należy przyporządkować odpowiednim organom. Jeżeli np. dane uprawnienie polega na stanowieniu prawa – a ani konstytucja, ani ustawa nie precyzują, kto ma ustanowić daną regulację prawną – to ze swej istoty winno ono przypaść legislatywie. Wyjątki od tej reguły, jakkolwiek nieliczne, powinny zostać wymienione w konstytucji, względnie w ustawie wydanej na podstawie jednoznacznej delegacji konstytucyjnej"[748]. Jak wskazuje R. M. Małajny, „zasadę należy interpretować możliwie szeroko, zaś wyjątek możliwie wąsko"[749].

Koncepcja rdzenia kompetencji zakłada, że każdy organ (lub ich grupa) realizująca daną prawną sferę działania posiada *sui genesis* rdzeń kompetencyjny (*das Kernbereich*), zastrzeżony wyłącznie dla niego. Twórcą tej koncepcji był niemiecki Trybunał Konstytucyjny[750], a polski Trybunał Konstytucyjny stanowisko to podzielił, wskazując, że podział władzy nie jest naruszony, jeżeli organ (lub grupa organów) zachowuje „pewne minimum wyłączności kompetencyjnej"[751]. Oznacza to tyle, że organ lub grupa organów ma

---

[746] Zdaniem R. M. Małajnego podział władzy jest najbardziej wieloznacznym pojęciem, jakim operuje konstytucjonalizm i nie jest on regułą organizacyjną możliwą do normatywnego zastosowania, a co najwyżej abstrakcyjna ideą ustrojową konkretyzującą różne subreguły, jak np. podział kompetencji pomiędzy różne organy czy *incompatibilitas*. Trójpodział władzy jest sprawą konwencji i adekwatności zarazem, gdyż może istnieć także np. dwupodział, pięciopodział czy sześciopodział władzy. Zob. R. M. Małajny, *Alternatywne koncepcje podziału władzy państwowej w XX w.*, [w:] *Idee jako źródło instytucji politycznych i prawnych*, red. L. Dubel, Lublin 2003, s. 53-76.
[747] *Ibidem*, s. 372.
[748] Zob. R. M. Małajny, *Zasada…*, s. 381-382.
[749] *Ibidem*, s. 382.
[750] Zob. orzeczenie niemieckiego Federalnego Sądu Konstytucyjnego z 1959 r.; BVefGe 9.
[751] Zob. wyrok TK z dnia 15 stycznia 2009 r., K 45/07; OTK – A 2009, nr 1, poz. 3.

wyznaczony przez władzę ustawodawczą, wykonawczą czy sądowniczą główny kierunek działania i to jest rdzeń kompetencji i istota działalności tego organu, jednak poza tym ma do spełnienia szereg innych dodatkowych działań (kompetencji) pozostających w luźnym związku z zasadniczym kierunkiem jego działalności.

W nowoczesnym demokratycznym państwie podział i klasyfikacja organów państwowych, z uwagi na zasadę podziału władzy, ulegają pewnym modyfikacjom i ograniczeniom w zakresie jej dosłownego rozumienia. Jest to zjawisko jak najbardziej pożądane, gdyż rozszerza możliwość klasyfikacji nowych organów państwowych, których jednoznaczne zdefiniowanie i przyporządkowanie nie jest łatwe.

Biorąc pod uwagę podstawy prawne powoływania organów państwowych, można je sklasyfikować jako organy konstytucyjne i pozakonstytucyjne (ustawowe). Ten podział determinuje źródło prawne powstania organu, tzn. czy organ opiera swoją egzystencję na normie konstytucyjnej (np. Sejm, Senat, Prezydent RP, Rada Bezpieczeństwa Narodowego, Rada Ministrów, Najwyższa Izba Kontroli, Sąd Najwyższy, Trybunał Konstytucyjny, Trybunał Stanu) czy pozakonstytucyjnej (np. Państwowa Komisja Wyborcza, Prokuratura)[752].

Zasadniczo umieszczenie danego organu w Konstytucji nie wpływa na jego pozycję ustrojową, jak również na jego kompetencje, jednak nie jest bez znaczenia[753]. Już chociażby jego wymienienie w Konstytucji, bez szerszego odniesienia się do jego kompetencji (np. Rzecznika Praw Dziecka w art. 103 ust. 1 Konstytucji RP) stanowi pewnego rodzaju wyraz uznania jego szczególnej roli ustrojowej i zaliczenia go w związku z tym do podstawowych instytucji politycznych państwa[754]. Zapewnia także organowi większą trwałość ustrojową, gdyż w przypadku likwidacji czy zmiany charakteru prawnego takiego organu konieczna jest równoczesna zmiana ustawy zasadniczej.

Kolejność wymienienia w tekście Konstytucji poszczególnych grup organów państwowych niekoniecznie musi odzwierciedlać ich rangę ustrojową. Analizując systematykę obecnie obowiązującej polskiej ustawy zasadniczej, to w pierwszym rozdziale Konstytucji RP (art. 10 Konstytucji RP) zostały wskazane organy, które są organami powołanymi do realizacji jednego z trzech głównych zadań państwa: ustawodawstwa,

---

[752] S. Sagan, *Pojęcie…,* s. 18; B. Szmulik, B. Przywora, *Konstytucyjny system organów państwowych*, Warszawa 2014, s. 20.

[753] Wyjątkiem są kompetencje w zakresie: wydawania aktów normatywnych powszechnie obowiązujących (art. 92 ust. 1 Konstytucji RP), gdyż rozporządzenia są wydawane przez organy wskazane w Konstytucji czy występowania z wnioskiem o rozstrzygnięcie sporów kompetencyjnych (art. 189 Konstytucji RP stanowi, iż TK rozstrzyga spory kompetencyjne pomiędzy centralnymi konstytucyjnymi organami państwa). Por. W. Orłowski, *op. cit.*, s. 112.

[754] Por. R. M. Małajny, *Systematyka…*, s. 8.

działalności wykonawczej i sądzenia. Dopiero w rozdziale IX Konstytucji RP znajduje się regulacja dotycząca kolejnej grupy organów, tj. organów kontroli państwowej i ochrony prawa (art. 202 ust. 1 Konstytucji RP wskazuje, iż NIK jest organem kontroli państwowej, art. 208 ust. 1 Konstytucji RP określa, iż RPO stoi na straży wolności i praw człowieka i obywatela, a Krajowa Rada Radiofonii i Telewizji, na mocy art. 213 ust. 1 Konstytucji RP, stoi na straży wolności słowa, prawa do informacji oraz interesu publicznego w radiofonii i telewizji); w żaden to jednak sposób nie umniejsza pozycji ani znaczeniu tych organów na tle innych organów w Polsce.

Z uwagi na ogólne postanowienia Konstytucji RP nie jest możliwe wskazanie z nazwy wszystkich organów państwowych. W ustawie zasadniczej zostały z nazwy wymienione organy władzy ustawodawczej (art. 95 ust. 1 Konstytucji RP: „władzę ustawodawczą w Rzeczypospolitej Polskiej sprawuje Sejm i Senat"), względem zaś pozostałych władz, przepisy Konstytucji poprzestają na wskazaniu kategorii organów (np. Prezydent Rzeczypospolitej Polskiej - art. 126 Konstytucji RP, Rada Ministrów – art. 146 Konstytucji RP, art. 173 Konstytucji RP: „Sądy i Trybunały są władzą odrębną i niezależną od innych władz", art. 175 ust. 1 Konstytucji RP: „wymiar sprawiedliwości w Rzeczypospolitej Polskiej sprawują Sąd Najwyższy, sądy powszechne, administracyjne oraz sądy wojskowe").

Uwzględniając budowę (morfologię) oraz strukturę organu, wyróżniamy organy jednoosobowe, tj. składające się z jednej osoby i organy kolegialne (wieloosobowe). Tutaj kryterium podziału stanowi skład organu, czyli liczba osób tworzących dany organ (kryterium liczby piastunów). Kolegialność organu powoduje, że wolę organu wyraża uchwała zespołu osób i zwykle organy kolegialne tworzone są, aby ustalały ogólne kierunki działania, czy założenia polityki w poszczególnych dziedzinach działalności państwa (np. Sejm, Senat, NIK)[755]. Organ jednoosobowy (monokratyczny) jest powoływany przede wszystkim do załatwienia konkretnych spraw, licznych i wymagających szybkiego rozstrzygnięcia, gdy niezbędna jest wiedza fachowa i gdy chodzi o jasno określoną odpowiedzialność (np. Prezydent RP, wojewoda, minister). Każdy organ kolegialny jest organem wieloosobowym, zaś relacja odwrotna nie jest konieczna, ponieważ kolegialność jest cechą funkcjonalną związaną z procesem podejmowania decyzji większością głosów lub przez aklamację (do wyobrażenia jest organ wieloosobowy decydujący jednoosobowo, np. prezes, przewodniczący, a pozostałym członkom służy prawo doradzania i opiniowania)[756].

---

[755] Zob. E. Ochendowski, *op. cit.*, s. 252.
[756] Zob. J. Galster, *op. cit.*, s. 66.

Uwzględniając czas trwania pełnomocnictw wskazać można organy kadencyjne i organy powołane na czas nieokreślony (bezterminowo). Przykładem organów powołanych bezterminowo może być Rada Ministrów czy ministrowie. Organy kadencyjne to te, których funkcjonowanie związane jest z określonym czasem (kadencją), na jaki został powołany czy wybrany określony organ. O kadencji można mówić, gdy ma miejsce odnowienie całego wieloosobowego składu danego organu (np. Sejm, Senat), ale kadencyjność może być też cechą organu jednoosobowego, jak w przypadku Prezydenta RP (art. 127 ust. 1 i 2 Konstytucji RP), Rzecznika Praw Obywatelskich (art. 209 ust. 1 Konstytucji RP) czy Prezesa NIK (art. 205 ust. 1 Konstytucji RP). Gdy jednak organ jest odnawiany tylko częściowo, to wówczas kadencyjność dotyczy tylko członków tego organu (np. dziewięcioletnia kadencja sędziów Trybunału Konstytucyjnego - art. 194 Konstytucji RP).

Kolejnym kryterium wyznaczającym podział organów państwowych jest kryterium kompetencji. Na tej podstawie wyszczególnia się organy zwyczajne i specjalne. Organy specjalne są powoływane z uwagi na zaistnienie szczególnych okoliczności i wówczas organ wyposażony zostaje w specjalne kompetencje (np. Naczelny Dowódca Sił Zbrojnych). Organy zwyczajne zaś są powoływane i funkcjonują niezależnie od zaistnienia nadzwyczajnych okoliczności (np. Sejm, Senat, Najwyższa Izba Kontroli, Rzecznik Praw Obywatelskich).

W przypadku podziału organów na centralne i lokalne, jego kryterium jest terytorialny zasięg działania organu[757]. Zasięg kompetencji organów centralnych rozciąga się na obszar całego państwa (np. Rada Ministrów, Sejm, Senat) i najwięcej organów należących do tej kategorii odnaleźć można wśród organów administracji rządowej (np. ministrowie, Wyższy Urząd Górniczy, Główny Inspektor Sanitarny). Organy centralne administracji państwowej najczęściej powoływane są przez Prezesa Rady Ministrów, a organami zwierzchnimi względem nich jest Rada Ministrów, Prezes Rady Ministrów czy odpowiedni minister. Organy lokalne (terenowe) są związane w swej działalności tylko z określoną częścią terytorium państwa. Najczęściej zakres właściwości tych organów pokrywa się z granicami jednostek samorządu terytorialnego: gminą, powiatem, województwem (nie dotyczy to jednak podziału właściwości organów władzy sądowniczej i organów prokuratury, gdyż ich właściwość oparta jest o podział na rejony, okręgi i apelacje). Organy terenowe znajdują się

[757] Ten podział zakłada, iż państwo podzielone jest na mniejsze jednostki terytorialne przy zastosowaniu zasadniczego bądź specjalnego podziału terytorialnego. Zob. A. Wiktorowska, *Rodzaje organów administracji,* [w:] *Prawo administracyjne*, red. M. Wierzbowski, Warszawa 2011, s. 113-114.

na niższym szczeblu struktury zarządzania niż organy centralne[758]. Takie kryterium podziału organów wiąże się z wyrażoną w art. 15 i art. 16 Konstytucji RP zasadą samorządu terytorialnego. Pojawienie się w strukturach władzy organów samorządu terytorialnego działających lokalnie powoduje decentralizację władzy publicznej, prawne wyodrębnienie i oddzielenie władzy lokalnej od aparatu władzy państwowej oraz stanowi zaprzeczenie zasady jednolitości władzy.

Z uwagi na zakres samodzielności w relacjach z innymi organami wyodrębnia się organy samodzielne i niesamodzielne. Gdy akt organu nie może być zniesiony lub zmieniony przez inny organ mówi się o organie samodzielnym, a gdy akt organu może zostać zmieniony lub uchylony przez inny organ, a także gdy organ związany jest szczegółowo wytycznymi innych organów, to jest określany jako organ niesamodzielny.

Wśród organów państwowych zauważyć można jeszcze podział na organy decydujące (samoistne) i doradcze (pomocnicze)[759]. Tu kryterium podziału stanowią kompetencje organu tj. możliwość decydującego rozstrzygania spraw. Organy decydujące to takie, którym przepisy prawa przyznają prawo władczego rozstrzygania spraw w drodze decyzji wiążących inne podmioty, decydują o dojściu do skutku danego aktu oraz występują samodzielnie w stosunkach z innymi organami państwowymi (np. Prezydent RP, Sejm, Senat). Organy decydujące posiadają dwie grupy kompetencji, tj. kompetencje zewnętrzne, zmierzające do realizowania norm prawa materialnego lub procesowego i kompetencje wewnętrzne, prowadzące do kształtowania wewnętrznych struktur organu i ich funkcjonowania[760].

Organy doradcze stanowią niewielką grupę pozbawioną takich kompetencji, a posiadają tylko prawo badania spraw i wyrażania opinii oraz mogą występować z inicjatywą czy dokonywać czynności kontrolnych. Przykładem organów pomocniczych są komórki (jednostki) organizacyjne funkcjonujące w ramach lub obok organów samoistnych (np. komisje Sejmu i Senatu czy Rada Bezpieczeństwa Narodowego, która na mocy art. 135 Konstytucji RP jest organem doradczym Prezydenta RP w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa).

Stosując kryterium sposobu powołania organu można dokonać wyróżnienia na organy państwowe pochodzące z wyboru (Sejm, Senat, Prezydent RP) oraz organy pochodzące z nominacji (np. Prezes Rady Ministrów, wojewoda).

---

[758] Cz. Martysz, *Pozycja ustrojowa Generalnego Inspektora Ochrony Danych Osobowych,* [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009, s. 67-71.
[759] Tak: E. Ochendowski, *op. cit.,* s. 251-252.
[760] W. Orłowski, *op. cit.,* s. 112.

Uwzględniając natomiast tryb pracy organy państwowe można podzielić na organy działające sesyjne i organy działające permanentnie. Pierwsze z nich to takie, które mają prawo wykonywać swoją pracę w określonych okresach, tj. okresach trwania ich sesji (np. niektóre parlamenty, jednak w Polsce, co jest rzadziej spotykanym rozwiązaniem, Sejm i Senat od 1989 r. działają w trybie permanencji). Z kolei organy działające permanentnie wykazują tryb pracy ciągłej i w każdej chwili mogą podjąć działanie (np. Prezydent RP, Rada Ministrów, wojewoda).

d) usytuowanie GIODO w systemie organów państwowych

Aby dokonać szczegółowego opisu określonego organu państwowego, należy brać pod uwagę wszystkie wyodrębnione wyżej kryteria klasyfikacji. Mając je na uwadze można stwierdzić, iż Generalny Inspektor Ochrony Danych Osobowych bez wątpienia jest organem państwowym, któremu przepisy u.o.d.o. nadają charakter instytucji działającej w imieniu i na rzecz państwa w celu wykonywania nadzoru nad realizacją prawa do ochrony danych osobowych[761].

Prawne formy działania, sposób powołania i odwołania czy powiązanie Generalnego Inspektora z innymi organami zostały ściśle określone przez prawo. Podstawą działania tego organu jest ustawa o ochronie danych osobowych, zatem na tle wcześniej wskazanej kwalifikacji GIODO jest organem pozakonstytucyjnym, tj. ustawowym, którego źródłem prawnym powstania jest norma ustawowa. GIODO to organ kadencyjny. Jego kadencja trwa 4 lata, a ta sama osoba nie może być Generalnym Inspektorem więcej niż dwa razy.

Uwzględniając budowę oraz strukturę organu można stwierdzić, że GIODO to organ jednoosobowy (monokratyczny), samodzielny, działający jednoosobowo i we własnym imieniu, który został powołany przede wszystkim do załatwiania konkretnych, określonych przez u.o.d.o. spraw związanych z ochroną prywatności jednostki i ochroną jej danych osobowych. W przypadku podejmowania takich działań przez ten organ niezbędna jest wiedza fachowa, stąd u.o.d.o. stawia wysokie wymagania kandydatowi na stanowisko GIODO i konieczne warunki do spełnienia podczas realizacji przez niego podejmowanych zadań.

[761] Zob. M. Kawecki, *Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej*, „Przegląd Prawa Technologii Informacyjnych. ICT Law Review" 2013, nr 1, s. 40.

W celu zaakcentowania pozycji GIODO wśród innych organów państwowych należałoby jeszcze uszczegółowić, iż Generalny Inspektor jest organem wyróżniającym się spośród innych organów czy jednostek organizacyjnych kompetencjami, w które wyposażyła do u.o.d.o[762]. Na tej podstawie można go zakwalifikować także do kategorii organów zwyczajnych, a więc takich, które są powoływane do funkcjonowania niezależnie od zaistnienia szczególnych okoliczności i które realizują swoje działania w państwie w sposób stały. Ponadto, to także organ samoistny i decydujący, który ma prawo władczego rozstrzygania spraw w drodze decyzji wiążących inne podmioty[763].

GIODO należy do organów centralnych, chociaż u.o.d.o. wprost o tym nie stanowi. Za taką klasyfikacją przemawia jednak przede wszystkim jego pozycja ustrojowa. Właściwość miejscowa GIODO rozciąga się na całe terytorium państwa. Generalny Inspektor jest jedynym organem, który w skali całego kraju sprawuje nadzór nad realizacją prawa do ochrony danych osobowych. Tak jak inne organy centralne GIODO został ustanowiony na podstawie ustawy i na podstawie ustawy zostały mu przyznane określone kompetencje. Poza Sejmem, Generalny Inspektor nie podlega żadnemu innemu organowi, w szczególności rządowi czy któremukolwiek z ministrów.

Od chwili powołania urzędu Generalnego Inspektora Ochrony Danych Osobowych za uznaniem go za organ centralny opowiadał się J. Boć, który wśród organów centralnych, podległych Sejmowi wymienił (z pomyłką w nazwie) „Głównego Inspektora Ochrony Danych Osobowych"[764]. Zdecydowanie za uznaniem GIODO jako organu centralnego opowiedziała się także E. Kulesza[765], podkreślając, iż jest to organ całkowicie niezależny od rządu, podległy w zakresie wykonywania swoich zadań tylko ustawie oraz posiadający szerokie kompetencje w zakresie kontroli przestrzegania prawa ochrony danych osobowych[766].

Również J. Barta stanowczo stwierdza, iż dominujące w doktrynie jest stanowisko uznające GIODO za centralny organ administracji publicznej, które ten autor podziela. Według J. Barty GIODO jest organem centralnym (a nie tylko wyspecjalizowanym organem

---

[762] Zob. E. Kuczma, P. Kuczma, *Generalny Inspektor Ochrony Danych Osobowych jako organ kontroli i ochrony prawa*, „Zeszyty Naukowe Dolnośląskiej Wyższej Szkoły Przedsiębiorczości i Techniki" 2013, nr 6, s. 212 i n.

[763] Zob. G. Koksanowicz, *Generalny Inspektor Ochrony Danych Osobowych,* [w:] *Ustrój organów ochrony prawnej*, red. B. Szmulik, M. Żmigrodzki, Lublin 2005, s. 410.

[764] Zob. J. Boć, *Prawo…*, s. 153.

[765] E. Kulesza przez dwie kadencje, w latach 1998-2006, pełniła funkcję Generalnego Inspektora Ochrony Danych Osobowych.

[766] Zob. E. Kulesza, *Pozycja…*,s. 9; E. Kulesza, *Pozycja prawna Generalnego Inspektora Ochrony Danych Osobowych*, [w:] *Przetwarzanie i ochrona danych*, red. G. Szpor, Katowice 1998, s. 3.

kontroli), ponieważ żaden z ministrów i Prezydent RP nie sprawują w stosunku do niego funkcji nadzorczych lub kontrolnych. J. Barta sugeruje nawet, że gdyby Generalnego Inspektora nie uznać za organ centralny w znaczeniu ustrojowym, to z całą pewnością jest on takim organem w rozumieniu art. 5 § 2 pkt 3 k.p.a.[767].

Za uznaniem GIODO jako organu centralnego opowiadali się ponadto K. Wygoda[768] oraz G. Sibiga[769]. Stanowisko to podziela także E. Ura, wskazując, iż „funkcjonują w strukturze organów państwa i takie, które w przepisach nie są nazwane organami centralnymi, jednakże ze względu na ich usytuowanie, obszar działania i kompetencje należy je uznać za centralne organy administracji państwowej"[770]. Za zaliczeniem Generalnego Inspektora Ochrony Danych Osobowych do organów centralnych opowiada się ponadto R. Michalska-Badziak pisząc, że „oprócz organów centralnych podległych bądź nadzorowanych przez (Radę Ministrów, Prezesa Rady Ministrów i ministrów) występują także organy podległe Sejmowi. Organem takim, powołanym niedawno, jest Główny Inspektor Ochrony Danych Osobowych"[771]. Podobne stanowisko zdaje się zajmować również J. Sługocki, gdyż powołując się na literaturę, lecz bez podania źródła i biorąc pod uwagę kryterium podległości, przy wskazywaniu organów podległych Sejmowi podaje jako przykład „Głównego Inspektora Danych Osobowych" (czyniąc również błąd w nazwie organu)[772].

Z uwagi jednak na szeroki zakres zadań i środków, którymi dysponuje GIODO w trybie art. 12 u.o.d.o., należałoby przedstawić wielopłaszczyznowo walor jego działalności jako organu powołanego do ochrony prywatności jednostki w Polsce.

Wśród organów państwowych wyodrębniła się grupa takich organów, które wyspecjalizowały się w ochronie praw i wolności obywateli. Biorąc pod uwagę funkcje i zadania GIODO należałoby go do tej grupy także zaliczyć.

Jeszcze przed zmianą ustroju politycznego w 1989 r. wprowadzono w Polsce, odchodząc od doktryny i praktyki, niezwykle istotne dla ochrony praw i wolności człowieka zmiany instytucjonalne. Dnia 29 kwietnia 1985 r.[773] uchwalono ustawę o Trybunale

---

[767] J. Barta, [w:] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, s. 394.
[768] Por. K. Wygoda, *op. cit.*, s. 412.
[769] Por. G. Sibiga, *Postępowanie…,* s. 118.
[770]Autorka przez pomyłkę nazywa GIODO Głównym Inspektorem Ochrony Danych Osobowych. Zob. E. Ura, *Centralne organy administracji rządowej w okresie przemian ustrojowych państwa,* [w:] *Administracja i prawo administracyjne u progu trzeciego tysiąclecia. Materiały konferencji naukowej katedr prawa i postępowania administracyjnego*, Łódź 2000, s. 481-482.
[771]Autorka ta z kolei przez pomyłkę nazywa GIODO Głównym Inspektorem. Zob. R. Michalska-Badziak, [w:] *Prawo administracyjne*. *Pojęcia, instytucje, zasady w teorii i orzecznictwie*, red. Z. Zduniewska, B. Jaworska-Dębska, R. Michalska-Badziak, E. Olejniczak-Szałowska, M. Stahl, Warszawa 2000, s. 252.
[772] J. Sługocki, *Prawo administracyjne. Podstawowe zagadnienia ustrojowe*, Warszawa 2007, s. 107.
[773] Ustawa z dnia 29 kwietnia 1985 r. o Trybunale Konstytucyjnym (Dz. U. Nr 22, poz. 9).

Konstytucyjnym, który to rozpoczął swoją działalność orzeczniczą z początkiem 1986 r., a w 1987 r. powołano do życia instytucję Rzecznika Praw Obywatelskich (RPO rozpoczął swoją działalność od początku 1988 r.)[774]. Na tej podstawie wykształciły się specjalistyczne organy państwowe, zwane organami ochrony prawnej, które zobowiązane zostały do udzielania pomocy wszystkim, których dobra zostały naruszone lub zagrożone.

Problematyka ustroju organów ochrony prawnej ma charakter multidyscyplinarny i cieszy się dużym zainteresowaniem przedstawicieli różnych dyscyplin prawniczych, począwszy od konstytucjonalistów, administratywistów, procesualistów oraz historyków prawa, jednak analiza konstrukcji prawnej organu musi być oparta na fundamencie konstytucyjnym. To z postanowień ustawy zasadniczej wywodzą się zasady organizacji i prawne podstawy powołania organów ochrony prawnej, takich jak: Najwyższa Izba Kontroli, Rzecznik Praw Obywatelskich, Rzecznik Praw Dziecka czy Krajowa Rada Radiofonii i Telewizji.

Przez ochronę prawną należy rozumieć stałą i zorganizowaną działalność, podejmowaną głównie dla ochrony prawa[775]. Termin „ochrona prawna" może być rozumiany w znaczeniu szerokim (*sensu largo*), jak i w znaczeniu wąskim (*sensu stricto*). Ochrona prawna *sensu largo* to strzeżenie nienaruszalności norm prawnych będących regułami obowiązującego zachowania w państwie[776]. W takim sensie ochrona prawna służy praworządności oraz zapewnia ład społeczny[777]. Elementami ochrony w szerokim znaczeniu jest oprócz orzekania także: pojednawstwo, kontrola legalności (zapobieganie naruszeniu prawa, ochrona prawna na przedpolu) czy działalność opiniodawczo-doradcza[778].

Ochrona prawna w wąskim znaczeniu to element ochrony *sensu largo*. Ochrona ta to przede wszystkim działalność wyspecjalizowanych organów państwowych podejmowana w celu ochrony prawa[779]. Polega na orzekaniu (rozstrzyganiu), czyli ustalaniu, czy norma prawna określonego typu została naruszona, a jeśli tak, to przez kogo, oraz na wyciągnięciu w ustawie przewidzianych konsekwencji aplikowanych w sytuacji przekroczenia określonej normy prawnej[780].

---

[774] Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. Nr 21, poz. 123); art. 36a Konstytucji PRL, dodany w 1989 r.
[775] Zob. S. Włodyka, *Ustrój organów ochrony prawnej*, Warszawa 1975, s. 9.
[776] W. Skrzydło, S. Grabowska, R. Grabowski, *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, Warszawa 2009, s. 292.
[777] B. Janusz-Pohl, *Ustrój organów ochrony prawnokarnej. Zarys wykładu*, Poznań 2011, s. 13.
[778] *Ibidem*, s. 14.
[779] W. Skrzydło, S. Grabowska, R. Grabowski, *op. cit.*, s. 292.
[780] F. Prusak, *Ustrój organów ochrony prawnej. Wprowadzenie. Teksty ustaw*, Warszawa 1999, s. 3.

Zapewnienie ładu społecznego w demokratycznym państwie prawnym wydaje się oczywiste, jest to jednak efekt długiej drogi ewolucji, której rezultatem było wykształcenie zasad, które stały się podstawą funkcjonowania ochrony prawnej. Wśród nich istotną rolę odegrał nakaz skierowany do organów państwa, aby udzielały ochrony prawnej osobie, która o tę pomoc się zwróci[781]. Nakaz udzielania ochrony prawnej zakłada istnienie wyspecjalizowanych struktur, organów powołanych do ochrony prawnej, a każdy rodzaj ochrony prawnej powinien być wykonywany przez wyspecjalizowany organ ochrony prawnej.

Ochrona praw i wolności w danym państwie stanowić powinna sprawnie działający system, którego kluczowym elementem są wyspecjalizowane organy czy instytucje specjalnie powołane do realizacji ochrony praw i wolności[782].Wraz z nim powinien istnieć również system normatywny, zawierający właściwe normy używane w procesie stosowania prawa, będące podstawą funkcjonowania i działalności organów ochrony prawa. Na tej podstawie dopełnieniem systemu ochrony prawa byłyby także działania i decyzje organów czy instytucji ochrony prawa, realizujące w praktyce ochronę praw i wolności jednostki. Tło dla wspomnianych czynników stanowić ma w każdym państwie indywidualne i zróżnicowane otoczenie tego sytemu, w skład którego wchodzą uwarunkowania krajowe, międzynarodowe, uwarunkowania społeczne, historyczne czy prawne. Przedstawiając zatem system ochrony praw i wolności jednostki, za punkt wyjścia należałoby przyjąć działalność organów ochrony prawa.

Skomplikowanym zagadnieniem pozostaje to, które organy państwowe należy zaliczyć do grupy organów ochrony prawa. Jak wskazuje B. Janusz-Pohl, „to raczej sprawa konwencji niż istnienia zobiektywizowanych kryteriów pozwalających te organy wyodrębnić spośród innych wchodzących w skład mechanizmu państwowego”[783]. Jednym z kryteriów typologii organów ochrony prawnej jest kryterium kompetencji, na podstawie którego można określić, czy dany organ ochrony prawnej pełni szeroko rozumianą funkcję ochronną na gruncie prawa prywatnego czy publicznego.

Zwykle uznaje się, że organ ochrony prawa to szczególny organ powołany do ochrony prawnej i pod tym kątem wyspecjalizowany. Jest to wyodrębniony organizm prawny

---

[781] Pozostałe zasady to zakaz uciekania się do samopomocy, równość podziału środków ochrony prawnej dla wszystkich obywateli, a nawet innych osób znajdujących się na terytorium danego państwa i jednolitość gwarancji proceduralnych.

[782] Zob. I. Malinowska, *Rzecznik Praw Obywatelskich w systemie ochrony praw i wolności w Polsce*, Warszawa 2007, s. 38-52.

[783] B. Janusz-Pohl, *op. cit,* s. 13.

posiadający określoną organizację oraz kompetencje, powołany przez ustawę w celu sprawowania ochrony prawnej. O przynależności danego organu do grupy organów ochrony prawnej decyduje główna funkcja tego organu, a więc to, co stanowi główny przedmiot jego działalności. Do organów ochrony prawa należą te, których funkcje wiążą się z rozstrzyganiem spraw oraz ustalaniem, czy norma prawna została naruszona i przez kogo, oraz ze stosowaniem sankcji przewidzianych w ustawie[784].

Liczba organów ochrony prawa rośnie we wszystkich współczesnych państwach demokratycznych. To zjawisko związane jest z coraz szerszym zakresem ochrony praw podmiotowych jednostki. W latach 50. i 60. XX wieku w wielu państwach rozpoczął się proces powoływania instytucji rzeczników praw obywatelskich (ombudsmanów), a w latach 70. XX wieku wraz postępem technologicznym pojawiła się konieczność ochrony prywatności jednostki i tym samym rozwinął się proces instytucjonalizacji prawnej organów ochrony prywatności jednostki i ochrony danych osobowych. Standardy ochrony były też wdrażane poprzez funkcjonowanie międzynarodowych oraz ponadnarodowych organów i instytucji ochrony praw i wolności człowieka. W systemach prawnych poszczególnych państw spotkać się można z różnymi koncepcjami formy i charakteru prawnego organów ochrony praw i wolności jednostki. W przeważającej większości występują samodzielnie wyodrębnione takie organy działające albo jako organy kolegialne (w skład których wchodzi kilku lub kilkunastu członków, wybieranych lub desygnowanych przez rożne podmioty na kilkuletnią kadencję, (np. szwedzki Urząd Inspekcji Danych Osobowych - *Data inspektionen*) lub jako organy jednoosobowe, np. niemiecki Federalny Pełnomocnik Ochrony Danych Osobowych czy polski Generalny Inspektor Ochrony Danych Osobowych). Prawna konstrukcja niezależnego w zakresie działania GIODO, powołanego do ochrony prawa, w tym przypadku prawa do prywatności jednostki z uwzględnieniem ochrony jej danych osobowych jak najbardziej wpisuje GIODO w poczet polskich organów państwowych, które powołane zostały do ochrony praw i wolności jednostki, a tym samym ochrony prawa.

Zgodnie z klasyfikacją organów ochrony prawnej opartej na definicji ochrony prawnej S. Włodyki, organy ochrony prawnej dzielą się na: organy rozstrzygające (orzekające), organy pojednawcze (mediacyjne, rozjemcze), organy kontroli przestrzegania prawa oraz organy pomocy prawnej[785]. Wskazany wyżej podział organów ochrony prawnej oparty jest na kryterium treści ochrony prawnej. Ochrona prawna spełnia jeszcze jeden istotny cel, a

[784] S. Sagan, V. Serzhanova, *Organy i korporacje ochrony prawa*, Warszawa 2014, s. 13.
[785] S. Włodyka, *op. cit.*, s. 25-36.

mianowicie cel represyjny. W przypadku naruszenia normy prawnej zostają zastosowane określone sankcje lub charakter prewencyjny, polegający na zapobieganiu naruszenia prawa w przyszłości, tj. profilaktyce w dziedzinie prawa[786].

Wśród organów kontroli sprawowanej przez wyspecjalizowane instytucje niezależne od rządu, obok Najwyższej Izby Kontroli, Prokuratury, Państwowej Inspekcji Pracy, Rzecznika Praw Obywatelskich czy Rzecznika Praw Dziecka, wielu autorów umiejscawia konsekwentnie Generalnego Inspektora Ochrony Danych Osobowych[787]. Pewne podobieństwo stanowiska względem organów sprawujących funkcje kontrolne prezentuje np. J. Niczyporuk, wskazując że pozycja Generalnego Inspektora podobna jest do pozycji organów kontroli państwowej i ochrony prawa, które wymieniane są w rozdziale IX Konstytucji. Autor podkreśla jednak, że katalog konstytucyjnych organów kontroli państwowej i ochrony prawa jest katalogiem zamkniętym, bo obejmuje wyłącznie: Najwyższą Izbę Kontroli, Rzecznika Praw Obywatelskich oraz Krajową Radę Radiofonii i Telewizji, a pozycja prawna GIODO podobna jest do Państwowej Inspekcji Pracy, która co prawda podlega Sejmowi, lecz zaliczana jest np. w nauce prawa administracyjnego do organów administracji specjalnej[788].

Kontrola legalności przestrzegania prawa stanowi jeden z celów organów ochrony prawa i jest właśnie realizowana przez wyspecjalizowane organy ochrony prawnej, zwane organami kontroli legalności. Ich zadaniem jest badanie zachowania się określonych podmiotów pod kątem zgodności ich zachowania z obowiązującym prawem i występowanie z wnioskami o zastosowanie odpowiednich środków w przypadku naruszenia lub zagrożenia prawa[789]. Kontrola legalności występuje jako kontrola niesamoistna (gdy stanowi dodatkowy rodzaj działalności określonego organu) lub kontrola samoistna (gdy kontrola przestrzegania prawa jest wyłączną funkcją danego organu) oraz jako kontrola *sensu stricto* i *sensu largo*[790].

Kontrola *sensu stricto* polega na badaniu działalności określonych podmiotów, zaś kontrola *sensu largo* obejmuje działalność określonych podmiotów z punktu widzenia jej zgodności z prawem oraz występowanie do właściwych organów z wnioskami o zastosowanie odpowiednich środków przewidzianych na wypadek naruszenia lub zagrożenia prawa[791].

---

[786] B. Janusz-Pohl, *op. cit.*, s. 15.
[787] Zob. np. Z. Cieślak, I. Lipowicz, Z. Niewiadomski, G. Szpor, *Prawo administracyjne*, Warszawa 2013, s. 291-292; A. Wiktorowska, *op. cit.*, s. 113.
[788] J. Niczyporuk, *Administracja ochrony danych osobowych*, [w:] *Prawa jednostki w społeczeństwie informatycznym*, red. M. Grzybowski, Rzeszów 1999, s. 32.
[789] J. Bodio, *op. cit.*, s. 222.
[790] Tak: B. Janusz-Pohl, *op. cit.*, s. 16.
[791] *Ibidem*, s. 16.

Przykładem organu kontroli *sensu stricto* jest Prokuratura czy Rzecznik Praw Obywatelskich, zaś organu ochrony prawa przeprowadzającego kontrolę *sensu largo* Najwyższa Izba Kontroli oraz Generalny Inspektor Ochrony Danych Osobowych.

Jak już była mowa, w polskim systemie prawnym zagadnienia dotyczące organów kontroli państwowej i ochrony prawa zostały umiejscowione w rozdziale IX Konstytucji RP. Połączenie kontroli państwowej i ochrony prawa w tytule rozdziału IX Konstytucji wskazuje na dwie wiodące funkcje organów objętych regulacją tej części Konstytucji. Ustawa zasadnicza wskazuje jednak tylko trzy organy w grupie organów kontroli państwowej i ochrony prawa: Najwyższą Izbę Kontroli, Rzecznika Praw Obywatelskich i Krajową Radę Radiofonii Telewizji. W pracach nad Konstytucją RP poglądy na przedmiotowy zakres przepisów umieszczonych w rozdziale IX Konstytucji były niejednolite, co skutkowało także różnorodnymi postulatami i sugestiami co do treści tego rozdziału. Rozważano m. in. możliwość uwzględnienia w tym rozdziale przepisów o trybunałach, w szczególności o Trybunale Konstytucyjnym, co przewidywały projekty konstytucji: senacki i tzw. obywatelski[792]. Do rozdziału IX pierwotnie chciano także zaliczyć Prokuraturę i Państwową Komisję Wyborczą, ale ostatecznie zrezygnowano z konstytucjonalizacji tych organów[793]. W ostatecznym kształcie rozdział IX Konstytucji uregulował podstawy prawne funkcjonowania jedynie trzech organów kontroli państwowej i ochrony prawa.

Podzielam pogląd, że bezzasadna jest obawa, iż objęcie nazwą „organy ochrony prawa" organów, których status jest normowany w rozdziale IX Konstytucji RP, wyłączy z tej kategorii organy w nim pominięte, wspomniane w innych częściach ustawy zasadniczej, albo w żadnym sensie niemające przymiotu instytucji konstytucyjnych[794].

Należy bowiem przyjąć, że Generalny Inspektor Ochrony Danych Osobowych realizuje powierzone mu zadania jak najbardziej jako organ kontroli państwowej i ochrony prawa. Odnosząc się do jednego z ważniejszych zadań i pierwszego zadania w kolejności, (zgodnie ze stylizacją art. 12 pkt 1 u.o.d.o.), GIODO realizuje zadania z zakresu ochrony prawnej jako organ państwowy powołany do sprawowania kontroli legalności przestrzegania prawa. Jest to niewątpliwie jeden z głównych aspektów działalności GIODO, przez co może on być sytuowany wśród organów ochrony prawa z uwzględnieniem również jego działalności jako organu kontroli. Pamiętać jednak należy, iż działalność GIODO nie jest

---

[792] Zob. „Biuletyn Komisji Konstytucyjnej Zgromadzenia Narodowego", nr VIII, s. 24 i nr XXV, s. 38. Ostatecznie możliwość taką przekreśliła decyzja o włączeniu trybunałów do władzy sądowniczej i odpowiednie do niej ulokowanie stosowanych przepisów w rozdziale VIII Konstytucji RP.
[793] W Konstytucji znalazły się tylko wzmianki o prokuraturze m. in. w art. 103 ust. 2, art. 191 ust. 1 pkt 1.
[794] Zob. A. Sylwestrzak, *NIK a Konstytucja*, „Kontrola Państwowa" 1998, nr 1, s. 36.

ograniczona tylko do działań o charakterze kontrolno-nadzorczym, gdyż już okres dziewiętnastu lat obowiązywania u.o.d.o i istnienia tego organu wskazuje, iż szerzej należy patrzeć na zakres jego działania.

W oparciu o działalność Generalnego Inspektora, m. in. jako organu kontroli, niektórzy autorzy, w tym P. Szustakiewicz, klasyfikują Generalnego Inspektora Ochrony Danych Osobowych jako wyspecjalizowany organ kontroli, który wymyka się z tradycyjnie pojmowanego trójpodziału władzy, i uważają, iż z uwagi na wysoki stopień niezależności należy go uznać za organ należący do tzw. czwartej władzy - kontrolującej[795].

Zdaniem W. Sokolewicza „jest to nad wyraz wątpliwe, czy można kreować osobną funkcję («władzę» w znaczeniu funkcjonalnym) kontroli państwowej z pominięciem kontroli parlamentarnej, przypisanej, jak wskazuje sama nazwa, parlamentowi, a zatem legislatywie będącej zgoła inną «władzą» (w znaczeniu podmiotowym)”[796]. Pogląd ten popiera także B. Banaszak twierdząc, że „w nauce prawa konstytucyjnego nie znalazło powszechnej akceptacji stanowisko głoszące, wobec wyodrębnienia w konstytucjach organów kontroli, konieczność wyjścia poza zasadę trójpodziału władz i wzbogacenia jej o czwartą władzę - kontrolującą”[797]. W związku z tym możliwość wyodrębnienia tzw. czwartej władzy nie jest do przyjęcia na gruncie Konstytucji RP, który wyraźnie wprowadza w art. 10 zasadę trójpodziału władzy.

Art. 10 Konstytucji RP zawiera dyspozycję do powołania i istnienia w demokratycznym państwie prawnym trzech rodzajów władzy: legislatywy, egzekutywy i judykatywy. W moim przekonaniu art. 10 nakazuje istnienie w państwie wymienionych w nim władz, nie zakazując jednak tworzenia innych organów, których zakres zadań będzie odbiegał od tych, które wyznaczone są teorią monteskiuszowką. W samej Konstytucji zawarty jest przecież rozdział IX, wprowadzający organy kontroli państwowej i ochrony prawa, których funkcje i zadania wymykają się klasycznej, monteskiuszowskiej klasyfikacji. W systemie organów państwowych w Polsce występują różnorodne organy i wobec znacznej większości z nich rzeczywiście adekwatna do zastosowania jest tradycyjna zasada trójpodziału władzy i przypisanie im funkcji stamtąd płynących. Organy władzy ustawodawczej, wykonawczej i sądowniczej muszą istnieć w państwie prawa, gdyż to stanowi o jego demokratycznym charakterze. Obok nich jednak funkcjonowanie organów realizujących zadania nienależące zakresem do stanowienia i wykonywania prawa oraz

---

[795] Zob. P. Szustakiewicz, *Kontrole Generalnego Inspektora Ochrony Danych Osobowych*, „Kontrola Państwowa” 2007, nr 6, s. 55.
[796] W. Sokolewicz, *Art. 6,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, Warszawa 2007, s. 3.
[797] B. Banaszak, *Konstytucja…*, s. 884.

wymiaru sprawiedliwości także jest konieczne i znaczące. Z uwagi także na fakt, iż prawo powinno się dynamicznie dostosowywać do zmieniającej rzeczywistości, jest wskazane, aby w nowoczesnym demokratycznym państwie prawnym katalog organów również się poszerzał.

Sztywne klasyfikowanie takich organów jak GIODO jest trudne i kontrowersyjne i zawsze będzie powodowało wielość opinii i stanowisk w tym zakresie. Należy pamiętać, iż GIODO w porównaniu z innymi organami państwowymi jest stosunkowo nowym organem, dlatego mają prawo być głoszone w doktrynie nawet skrajne opinie względem usytuowania tego organu w systemie organów państwowych. Z uwagi na przyznane GIODO kompetencje oraz ustawowo przydzielone zadania do wykonania, zakres jego działalności jest o tyle charakterystyczny, że nie tak łatwo jest umieścić jednoznacznie ten organ w tradycyjnym trójpodziale władzy. GIODO powinien być traktowany przede wszystkim jako organ ochrony prawa do prywatności funkcjonujący w powiązaniu z władzą ustawodawczą i władzą wykonawczą: z władzą ustawodawczą z uwagi na podległość względem parlamentu, a z władzą wykonawczą chociażby ze względu na sferę swoich działań.

Stanowisko, iż GIODO realizuje zadania w ramach odrębnej czwartej władzy - kontrolującej i niezależnej względem trzech dotychczas istniejących w mojej opinii jest słuszne. Nie można odrzucić koncepcji R. M. Małajnego, dotyczącej klasyfikacji organów państwowych wychodzącej spoza sztywną klasyfikację trójpodziału władzy, o której była mowa w poprzednich podrozdziałach pracy. Generalny Inspektor jest doskonałym przykładem organu, względem którego jednoznaczna klasyfikacja nie jest możliwa. Pomocniczo zatem stosując podział organów państwowych proponowany przez tego autora, z powodzeniem GIODO zaliczyć można do organów kontrolnych. Nie pozostaje to w żadnej sprzeczności z jego głównym zakresem działania, tj. ochroną prywatności człowieka (realizując przy tym funkcje organu ochrony prawa), gdyż należy pamiętać, iż wszelkie działania kontrolne dokonywane przez ten organ nakierowane są na osiągnięcie głównego celu, tj. ochrony prawa do prywatności. Działania kontrolne GIODO są podejmowane w celu tej ochrony: dla zapewnienia przestrzegania zasad i norm odnoszących się do poszanowania prawa do prywatności człowieka. Aby właściwie chronić sferę prywatności jednostki, potrzebne są działania kontrolne, których celem jest sprawdzanie i weryfikacja stopnia i efektywności ochrony prywatności, w tym danych osobowych. Idąc dalej, można również zaryzykować tezę, iż GIODO łącząc uprawnienia kontrolne i pełniąc rolę organu ochrony prawa adekwatnie wpisuje się w grupę organów, które sama Konstytucja RP nazywa organami kontroli państwowej i ochrony prawa. Nie byłaby w tej sytuacji to klasyfikacja

chybiona, gdyż analizując główny cel ochrony prawa, jednym z jego elementów jest przecież kontrola legalności.

W doktrynie bywają wyrażane również poglądy o GIODO jako analogu Rzecznika Praw Obywatelskich. Podobieństwa tych dwóch organów można upatrywać głównie w ich pozycji ustrojowej, w sposobie powoływania i odwoływania, ich niezależności, czy uprawnieniach w zakresie rozpatrywanych spraw. Za tym stanowiskiem opowiada się m.in. E. Kulesza, która, pomimo wskazania pewnych wspólnych cech dla GIODO i RPO, zaznacza jednak, że wyposażenie GIODO w kompetencje władcze, w tym uprawnienie do prowadzenia postępowań administracyjnych oraz wydawanie decyzji administracyjnych, odróżnia pozycję ustrojową GIODO od pozycji ustrojowej RPO[798]. Upatrywanie zbieżności pomiędzy tymi dwoma organami wydaje się być zasadne z uwagi na klasyfikację Generalnego Inspektora oraz Rzecznika Praw Obywatelskich jako organów ochrony prawnej i na wspólny obszar ochrony, tj. praw i wolności jednostki.

W niektórych opracowaniach GIODO jest umiejscawiany w gronie rzeczników interesu społecznego (obok Rzecznika Praw Obywatelskich, Rzecznika Praw Dziecka, Rzecznika Praw Konsumentów czy Rzecznika Interesu Społecznego), przez co można rozumieć, że ich autorzy także widzą podobieństwo GIODO do wskazanych organów[799]. Także F. Prusak, formułując pogląd o „odrębności organów ochrony prawnej i ściśle z nią się wiążącą zasadę specjalizacji", zalicza Generalnego Inspektora Ochrony Danych Osobowych do grona organów ochrony prawnej, rzeczników interesu społecznego[800].

Część autorów odwołując się do podobieństw Generalnego Inspektora jako rzecznika interesu społecznego, klasyfikuje nawet GIODO jako *quasi*-ombudsmana. Wyodrębniają go w ramach podziału na: klasycznego ombudsmana, wyspecjalizowanego ombudsmana o centralnym usytuowaniu, wyspecjalizowanego ombudsmana lokalnego czy lokalnych ombudsmanów o kompetencjach ogólnych[801]. W takim ujęciu GIODO, tak jak *quasi*-ombudsman, jest powołany do strzeżenia praw obywateli, a będąc rzecznikiem interesu całego społeczeństwa lub poszczególnych grup społecznych, jego głównym celem jest dbałość o nienaruszalność wolności i praw obywateli[802].

---

[798] E. Kulesza, *Pozycja…,* s. 24.
[799] Zob. B. Szmulik, M. Żmigrodzki, *Ustrój organów ochrony prawnej*, Lublin 2005, s. 67 i n.; F. Prusak, *op. cit*, s. 13.
[800] F. Prusak, *op. cit*, s. 4.
[801] I. Malinowska, *Rzecznik…*, s. 58-73; I. Malinowska, *Ochrona praw i wolności w Polsce*, Warszawa 2009, s. 221.
[802] Zob. I. Malinowska, *Ochrona*…, s. 221.

J. Zimmerman uważa natomiast, że Generalny Inspektor jest organem o szczególnym statusie i zalicza GIODO do grupy organów podległych Sejmowi. Wskazuje on jednak, iż „są to organy mające częściowo charakter organów kontroli państwowej, a częściowo organów administracyjnych. Ich niezależność od rządu sprawia, że w istocie mają one status organów naczelnych i nie należą do administracji rządowej”[803]. J. Zimmerman dokonując analizy kontroli i wskazując na istnienie kontroli sprawowanej przez pozaadministracyjne organy państwowe, definiuje Generalnego Inspektora (obok Rzecznika Praw Dziecka czy Państwowej Inspekcji Pracy) jako organ państwowy, niewchodzący w skład administracji publicznej.

Z uwagi na zainteresowanie rangą i pozycją prawną GIODO także wśród administratywistów, warto jest przedstawić pokrótce klasyfikację tego organu występującą głównie w nauce administracji. Tu Generalny Inspektor zaliczany jest do organów administracyjnych , jednak rozbieżność głoszonych opinii dotyczy tego, czy powinien on być uznany za organ administracji publicznej czy organ administracji państwowej. Pojęcie organu administracji publicznej należy do podstawowych pojęć w nauce prawa administracyjnego i ma szerokie znaczenie[804]. Termin ten nie jest definiowany w aktach normatywnych, ani nawet Konstytucja RP nie posługuje się terminem „organ administracji publicznej”, a jedynie terminem „administracja publiczna”[805] oraz „administracja rządowa”[806]. Znaczący wpływ na pojmowanie organu administracji miało reaktywowanie samorządu terytorialnego. Przed 1990 r. w aktach prawnych funkcjonowało pojęcie organu administracji państwowej, zaś po tej dacie kompetencje dawnych organów administracji rozdzielono pomiędzy organy administracji rządowej i samorządowej, a pojęcie „organu administracji państwowej” zaczęto zastępować terminem „organ administracji publicznej” i to nie zawsze właściwie (bywa, że „organ administracji państwowej” jest utożsamiany z „organem administracji rządowej”)[807].

Analizując zatem prawną pozycję GIODO z punktu widzenia prawa administracyjnego pewne jest, że organ ten nie jest organem administracji samorządowej ani też nie podlega zwierzchnictwu Rady Ministrów (i Prezesa Rady Ministrów), tzn. nie jest organem administracji rządowej. Kompetencji nadzorczych ani kontrolnych względem Generalnego Inspektora nie można wywodzić z faktu, że u.o.d.o. upoważnia ministra

---

[803] J. Zimmerman, *op. cit*., s. 146.
[804] Zob. J. Filipek, *Prawo administracyjne. Instytucje ogólne. Część I*, Kraków 2003, s. 309; W. Dawidowicz, *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970, s. 61 i n.
[805] Np. w kontekście jej kontroli sprawowanej przez Naczelny Sąd Administracyjny - art. 184 Konstytucji RP.
[806] Np. w tytule rozdziału VI Konstytucji RP.
[807] Por. S. Jarosz-Żukowska, *Organ administracji publicznej,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, red. W. Skrzydło, S. Grabowska, R. Grabowski, Warszawa 2009, s. 320.

właściwego do spraw administracji do wydawania aktów wykonawczych do tej ustawy ani tym bardziej z faktu nadawania przez Prezydenta RP statutu dla Biura GIODO[808]. Parlament nie ma żadnych kompetencji merytorycznego wpływu na działalność Generalnego Inspektora, gdyż podlega on tylko ustawie. Jedynie z punktu widzenia ustrojowego GIODO podlega Sejmowi, z uwagi na tryb powołania i odwołania oraz obowiązek składania sprawozdań Sejmowi ze swojej działalności, o czym będzie mowa w dalszej części pracy.

Szerokie rozumienie we wspomnianej nauce pojęcia organu administracji publicznej, zawiera w sobie nie tylko państwowe podmioty administracji (zwłaszcza organy administracji rządowej), ale także i pozostałe podmioty, którym przysługują kompetencje z zakresu prawa administracyjnego[809]. Organami niewchodzącymi w skład administracji rządowej, ale będącymi organami administracji państwowej, jest więc np. Prezydent RP, Najwyższa Izba Kontroli, Rzecznik Praw Obywatelskich, Krajowa Rada Radiofonii i Telewizji czy Narodowy Bank Polski[810]. Na tej podstawie także i Generalnego Inspektora nienależącego do organów administracji rządowej ani samorządowej, można zakwalifikować do kategorii organów administracji państwowej[811] i tym samym przyjąć pogląd reprezentowany przez wielu przedstawicieli doktryny, którzy dokonują wyodrębnienia centralnych organów administracji państwowej mieszczących w swoim zakresie organy administracji rządowej, oraz te, których pozycja jest tożsama lub podobna do pozycji GIODO[812]. W takim ujęciu w nauce administracji Generalny Inspektor spełnia przesłanki centralnego organu administracji państwowej[813].

Niektórzy z przedstawicieli doktryny z kolei dość lakonicznie odnoszą się w ogóle do określenia pozycji Generalnego Inspektora w systemie polskich organów państwowych. W. Chróścielewski np. nie zalicza Generalnego Inspektora, ani do organów centralnych, ani nawet kierowników urzędów państwowych równorzędnych z centralnymi organami administracji rządowej, o czym stanowi w art. 5 § 2 pkt 4 k.p.a., ale włącza go do grupy

---

[808] M. Sakowska, *Pozycja ustrojowa i zadania Generalnego Inspektora Ochrony Danych Osobowych*, „Przegląd Sejmowy" 2006, nr 2, s. 84.
[809] S. Jarosz- Żukowska, *op. cit.*, s. 321.
[810] *Ibidem*, s. 321.
[811] Por. M. Gesdorf, *Komentarz do ustawy o Państwowej Inspekcji Pracy*, Warszawa 2008, s. 19 i n.
[812] Zob. E. Ura, *Prawo administracyjne*, Warszawa 2009, s. 155; E. Kulesza, *Pozycja i uprawnienie Generalnego Inspektora Ochrony Danych Osobowych w świetle ustawy o ochronie danych osobowych. Uwagi de lege lata i de lege ferenda*, „Przegląd Sejmowy" 1999, nr 6(35), s. 10.
[813] Tak: P. Fajgielski, *Kontrola*…, s. 113; A. Drozd, *Ustawa..*, s. 82; M. Sakowska, *Pozycja…*,s. 85; T. A. J. Banyś, J. Łuczak, *op. cit.*, s. 172; I. Zgoliński, I. Zduński, *op. cit.*, s. 30.

„innych organów państwowych sprawujących orzecznictwo administracyjne, a więc zaliczanych do organów administracji publicznej w znaczeniu funkcjonalnym”[814].

Chociaż niemożliwe, w mojej opinii, jest jednoznaczne i bezsprzeczne określenie pozycji GIODO pośród innych organów w systemie prawa, to na pewno warto podkreślić, że ustawodawca kreując taki organ miał zamiar wyeksponować potrzebę ochrony prywatności jednostki, a w tym jej prawo do ochrony danych osobowych w Polsce. Wyposażenie Generalnego Inspektora w liczne kompetencje, które ma prawo realizować jako organ niezawisły i niezależny względem innych potwierdza, że poprzez jego kreację została zaznaczona jego waga i pozycja wśród innych organów w państwie.

Warto nadmienić, iż w celu wyeliminowania istniejących rozbieżności w zakresie ustalenia pozycji ustrojowej Generalnego Inspektora Ochrony Danych Osobowych, spowodowanych istniejącą regulacją prawną, w literaturze przedmiotu postuluje się, aby wprowadzając kolejną nowelizację ustawy, wprost określić, że Generalny Inspektor Ochrony Danych Osobowych to organ centralny[815]. Przychylam się jak najbardziej do tego stanowiska, gdyż dotychczasowa pozycja GIODO została ukształtowana w niezbyt precyzyjnie, co rodzi w nauce wiele wątpliwości i rozbieżności co do określenia pozycji tego organu. Nie ułatwia jednoznacznej klasyfikacji także fakt, iż pozycja Generalnego Inspektora związana jest także z administracyjnym charakterem działalności tego organu. Co więcej, przy okazji zmian w ustawie warto byłoby zastanowić się także nad zmianą nazwy i zamiast „Generalny” zastąpić ją słowem „Główny”. Z uwagi na omyłki pisarskie (o których wspominałam już w pracy) i tendencyjne podejście do klasyfikacji organów oraz określanie organów jako „główne” z uwagi na ich pozycję ustrojową czy posiadane kompetencje, zdarzają się błędy w pisowni GIODO. W wielu publikacjach Generalny Inspektor Ochrony Danych Osobowych pojawia się jako „Główny Inspektor”, co wprowadza pewien chaos pojęciowy i klasyfikacyjny. Zmiana nazwy korespondowałaby z dotychczasową terminologią organów państwowych funkcjonujących w sferze prawnej, jak np. Główny Inspektor Sanitarny czy Główny Inspektor Ochrony Środowiska, przez co także uwypukliłaby i zaznaczyła istotę tego organu.

---

[814] W. Chróścielewski, *Organ administracji publicznej w postępowaniu administracyjnym*, Warszawa 2002, s. 52-53.
[815] Cz. Martysz, *op. cit.*, s. 75-76.

2. Kwalifikacje zawodowe i osobiste GIODO

Kandydat na Generalnego Inspektora Ochrony Danych Osobowych musi spełniać kierunkowe kryteria doboru, które zostały przedstawione w art. 8 ust. 3 u.o.d.o. Na stanowisko GIODO może być powołany ten, kto łącznie spełnia następujące warunki: jest obywatelem polskim i stale zamieszkuje na terytorium Rzeczypospolitej Polskiej, wyróżnia się wysokim autorytetem moralnym, posiada wyższe wykształcenie prawnicze oraz odpowiednie doświadczenie zawodowe i nie był karany za przestępstwo. Jak słusznie zauważa E. Kulesza, kryteria te „zostały sformułowane przez ustawodawcę z niejednakową precyzją […], a obok kryteriów ocennych są także kryteria sformułowane jednoznacznie”[816].

Jednoznacznie wskazane kryteria dla kandydata to: posiadanie obywatelstwa polskiego, stałe zamieszkiwanie na terytorium RP, wyższe wykształcenie prawnicze i niekaralność za przestępstwo. Posiadanie polskiego obywatelstwa, miejsce zamieszkania na terytorium RP i niekaralność za przestępstwa to minimum oczekiwań wobec kandydata na Generalnego Inspektora. Okolicznością dyskwalifikującą kandydata na urząd GIODO jest ukaranie go za jakiekolwiek przestępstwo, w tym popełnione z winy nieumyślnej.

Wyższe wykształcenie prawnicze oraz odpowiednie doświadczenie zawodowe mają zapewnić profesjonalizm działania GIODO i wyeliminować dowolne powoływanie osób na to stanowisko. Taki wymóg uzasadniony jest charakterem działalności Generalnego Inspektora i zakresem jego zadań. Zgodnie z art. 12 pkt 1 u.o.d.o. podstawowym jego zadaniem jest kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Kandydat na Generalnego Inspektora nie musi posiadać uprawnień do wykonywania konkretnego zawodu prawniczego, stażu lub doświadczenia w tym zawodzie, czy pełnienia obowiązków na stanowisku kierowniczym. Wystarczające jest, by spełnił warunek formalny, tj. posiadał wyższe wykształcenie prawnicze.

Powołując się na wskazane kryteria względem kandydata na stanowisko GIODO, na pewno ocenny jest wymóg przyjęty w stosunku do kandydata, by wyróżniał się wysokim autorytetem moralnym i posiadał odpowiednie doświadczenie zawodowe.

Formalna przesłanka posiadania „odpowiedniego doświadczenia zawodowego” jest na pewno niedookreślona, jednak mając na względzie szczególny charakter działalności tego

---

[816] E. Kulesza, *Pozycja…,* s. 12; J. Barta, P. Fajgielski, R. Markiewicz określają wymogi jako mające charakter obiektywny (obywatelstwo, miejsce zamieszkania i wykształcenie) oraz mające charakter subiektywny (wyróżnianie się wysokim autorytetem moralnym i posiadanie odpowiedniego doświadczenia zawodowego). Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, s. 393.

organu zasadne jest, by kandydat na stanowisko GIODO posiadał co najmniej stopień doktora nauk prawnych, uprawnienie do wykonywania zawodów prawniczych (radcy prawnego, adwokata, notariusza, sędziego czy komornika) lub legitymował się co najmniej pięcioletnim doświadczeniem na stanowisku kierowniczym w zakresie stanowienia lub stosowania prawa[817].

Brak jest jednak jednoznacznych przesłanek, za pomocą których można by zweryfikować wysoki autorytet moralny kandydata, gdyż ani w ustawie ani w żadnym innym akcie prawnym nie doprecyzowano, czym musiałby wykazać się kandydat, by mógł powołać się na wysoki autorytet moralny. Jest to na pewno warunek istotny wobec dużego stopnia samodzielności w sprawowaniu urzędu, jako że Generalny Inspektor w tym zakresie podlega tylko ustawie. W tej sytuacji zatem stawiane są dalej idące wymagania niż tylko możliwość spełnienia jednoznacznie określonych warunków formalnych np. względem wykształcenia czy posiadania polskiego obywatelstwa. Takie ustawowe certyfikowanie moralności służyć ma zapewne powołaniu na stanowisko kandydata, który swoją postawą i nienagannym zachowaniem gwarantowałby sumienne wykonywanie powierzonych obowiązków.

Co więcej, analizując dotychczasową działalność GIODO w kraju oraz na arenie międzynarodowej zasadne jest, by wśród ustawowych kwalifikacji na stanowisko GIODO został wprowadzony także warunek, by kandydat na nie znał co najmniej jeden język obcy spośród języków roboczych Unii Europejskiej, a także by korzystał z pełni praw publicznych.

W praktyce o wyborze GIODO decydują kwestie polityczne. Oczywiście kandydat powinien spełniać wszystkie wymogi ustawowe, aby móc ubiegać się o ten urząd, jednak wobec dość elastycznych i w większości uznaniowych kryteriów parlament ma tu duży margines swobody w zakresie nominacji i wyboru. Trudno jest jednak kwestionować obecny tryb wyboru, gdyż to przecież parlament stanowi najbardziej reprezentatywny organ wyrażający w najpełniejszym stopniu – wskutek ukształtowania jego kształtu - wolę suwerena. Zresztą dotychczasowa praktyka w zakresie powoływania na ten urząd wskazuje, że zajmowały go osoby o merytorycznym i fachowym przygotowaniu do pełnienia tej funkcji, posiadające adekwatną wiedzę, umiejętności i predyspozycje, które znacznie przewyższały ustawowe minimum. Służy to profesjonalnej realizacji powierzonych przez ustawę zadań. To między innymi dzięki osobom pełniącym funkcję GIODO organ ten cieszy się obecnie dużym uznaniem i prestiżem, a zgłaszane postulaty i uwagi związane z ochroną danych osobowych

---

[817] Tak: B. Przywora, *Generalny Inspektor Ochrony Danych Osobowych w Polsce – stan obecny i postulaty de lege ferenda*, [w:] *Państwo demokratyczne, prawne i socjalne. Studia konstytucyjne. Księga jubileuszowa dedykowana profesorowi Zbigniewowi Antoniemu Maciągowi. Tom 1*, Kraków 2014, s. 580.

traktowane są z właściwą uwagą i refleksją przez wszystkie opcje polityczne. Jak dotychczas organ ten nie był uwikłany w żadne spory partyjne, i – pomimo politycznego wyboru – w sposób neutralny politycznie zajmował się ochroną danych osobowych.

3. Procedura powołania GIODO

W myśl art. 8 ust. 2 u.o.d.o. Generalnego Inspektora Ochrony Danych Osobowych powołuje i odwołuje Sejm za zgodą Senatu. Powołanie GIODO przez Sejm gwarantuje mu niezależność od innych organów państwowych, których działanie podlega kontroli właśnie tego organu. Wybór przez parlament gwarantuje GIODO demokratyczną legitymację i zapewnia bezpieczny dystans w stosunku do administracji publicznej[818]. Taki model jest przyjmowany we wszystkich ustawodawstwach europejskich względem podmiotu zajmującego się ochroną prywatności i ochroną danych osobowych obywateli. Przyjęty został także w Konstytucji RP i innych polskich aktach prawnych stanowiących podstawę działania, np. Rzecznika Praw Obywatelskich czy Prezesa Najwyższej Izby Kontroli (którzy są powoływani są przez Sejm, za zgodą Senatu). Wskazana konstrukcja powoływania klasyfikuje Generalnego Inspektora wśród tzw. organów wtórnych, przy których tworzeniu obecny jest udział innego podmiotu (GIODO jest powoływany przez Sejm), a nie jest on tworzony tylko na podstawie normy prawnej.

Ustawa nie precyzuje, do kogo należy wyłonienie kandydata na to stanowisko, kto jest uprawniony do złożenia wniosku w sprawie jego powołania, nie określa także liczby głosów wymaganej dla powołania Generalnego Inspektora; dlatego znajdują tu zastosowanie przepisy art. 29 ust. 1 i 2, art. 30 i art. 31 regulaminu Sejmu[819] oraz art. 91 ust. 1 pkt 3 oraz art. 91ust. 2 i 3 regulaminu Senatu[820].

Pierwszą wątpliwością, która pojawia się w przypadku procedury powołania Generalnego Inspektora, jest konieczność wyjaśnienia, czy z formalnego punktu widzenia ma miejsce wybór czy powołanie Generalnego Inspektora Ochrony Danych Osobowych.

Co do zasady, mocą jednostronnego aktu mianowania na określone stanowisko, zostają wywołane skutki prawne zarówno w sferze prawa pracy (nawiązanie stosunku pracy) jak i w sferze prawa administracyjnego, gdyż obsadzone zostaje określone stanowisko. Do

---

[818] E. Kulesza, *Pozycja…,* s. 11.
[819] Uchwała Sejmu RP z dnia 30 lipca 1992 r. regulamin Sejmu Rzeczypospolitej Polskiej (M. P. z 2002 r. Nr 23, poz. 398 z późn. zm.).
[820] Uchwala Senatu RP z dnia 23 listopada 1990 r. regulamin Senatu (M. P. z 2002 r. Nr 54, poz. 741 z późn. zm.)

mianowania dochodzi także z racji uznania osoby, która jest właściwa do piastowania danego stanowiska, dlatego też w praktyce status pracowników mianowanych mają najczęściej m. in. urzędnicy służby cywilnej, pracownicy instytucji naukowych czy wymiaru sprawiedliwości.

W doktrynie wskazuje się z kolei, iż „powołanie" ma miejsce w przypadku, gdy zaistnieją następujące trzy okoliczności. Po pierwsze, powołanie zachodzi wówczas, kiedy właściwy organ (organ powołujący) powoła osobę na określone stanowisko, a o powołaniu mówi się w ustawie dotyczącej określonego organu. Po drugie, powołanie może następować za zgodą, a „wybór za czyjąś zgodą" byłby sformułowaniem niezręcznym. Po trzecie, wybór powinien być dokonywany spośród większej liczby kandydatów, a w danym wypadku Konstytucja powinna sugerować możliwość konsensusu co do jednej kandydatury[821].

Biorąc pod uwagę przedstawione powyżej warunki, można zauważyć pewne rozbieżności co do możliwości obsadzenia stanowiska GIODO, gdyż w stosunku do tego organu po części zostają spełnione zarówno przesłanki mianowania jak i powołania. Sugerując się jednak w pierwszej kolejności użytym wprost w art. 8 ust. 2 u.o.d.o. sformułowaniem „powołuje", stwierdzić należy, iż w przypadku Generalnego Inspektora wyraźnie mamy do czynienia z faktem powołania. Organem powołującym GIODO jest Sejm, a powołanie odbywa się za zgodą Senatu; u.o.d.o. dokładnie wskazuje, na jaki okres nastąpiło powołanie. Wymienne posługiwanie się każdym z tych dwóch wyrażeń konsekwentnie zaś służy do określenia powołania jako formalnoprawnego aktu obsadzenia urzędu GIODO.

Stosownie do postanowień art. 30 Regulaminu Sejmu RP wniosek w sprawie powołania kandydata może przedstawić Marszałek Sejmu albo grupa co najmniej 35 posłów. Wniosek powinien być uzasadniony i uzupełniony danymi o kandydacie oraz opatrzony zgodą kandydata na kandydowanie. Powinien zostać przedłożony Marszałkowi Sejmu lub zostać przez niego sporządzony na 30 dni przed upływem kadencji urzędującego GIODO. Głosowanie na posiedzeniu Sejmu nie może jednak odbyć się wcześniej niż następnego dnia po doręczeniu posłom opinii właściwej komisji, jeżeli tylko Marszałek Sejmu zwrócił się do niej o sporządzenie opinii w sprawie, co powinno być regułą.

Podjęcie uchwały następuje w trybie przewidzianym dla podejmowania przez Sejm uchwał z tą różnicą, iż dla jej podjęcia niezbędna jest bezwzględną a nie zwykła większość głosów (art. 31 ust. 1 Regulaminu Sejmu RP), co sprzyjać ma znalezieniu kandydata kompromisowego dla wszystkich reprezentantów różnych opcji politycznych[822]. Uchwała

---

[821] Zob. W. Sokolewicz, *Art. 209*…, s. 6.

[822] Odmienny pogląd prezentuje P. Barta i P. Litwiński [w:] *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2013, s. 152. Pogląd ten jest jednak niezgodny z treścią art. 31 ust. 1 Regulaminu Sejmu RP.

może być podjęta tylko przez Sejm obradujący na posiedzeniu (plenarnym). Jeżeli zgłoszono więcej niż jednego kandydata, a w pierwszym głosowaniu żaden z kandydatów nie uzyskał bezwzględnej większości głosów, przed kolejnymi turami głosowania usuwa się z listy kandydatów nazwisko tego kandydata, który w poprzedniej turze uzyskał najmniejszą liczbę głosów. Jeżeli tę samą najmniejszą liczbę głosów uzyskało dwóch lub więcej kandydatów, przed kolejną turą głosowania usuwa się nazwiska tych kandydatów. Gdy w wyniku zastosowania tej procedury nie dojdzie do wyłonienia kandydata, procedurę przeprowadza się ponownie.

Powołania na stanowisko GIODO może dokonać tylko Sejm, zaś Senat może zgodzić się lub nie na uprzednio powołaną osobę przez Sejm. Wydawać by się mogło zatem, iż zgoda Senatu w tym zakresie ma tylko charakter czysto formalny, gdyż może być dokonana jedynie po wcześniejszej decyzji Sejmu[823]. Taka procedura wynika jednak z podległości GIODO tylko Sejmowi i z wyłącznego prawa do przedstawiania kandydatów przez Marszałka Sejmu i posłów, a w żadnym stopniu nie jest w ten sposób pomniejszane znaczenie zgody Senatu[824].

Wyrażenie zgody przez Senat następuje w drodze uchwały podjętej w trybie art. 91 ust. 1 pkt 3 Regulaminu Senatu. Senat przed podjęciem przedmiotowej uchwały może wezwać kandydata na stanowisko GIODO do złożenia wyjaśnień i odpowiedzi na pytania senatorów. Głosowanie w Senacie odbywa się na zasadach ogólnych obowiązujących przy podejmowaniu uchwał przez Senat: zwykłą większością głosów w obecności co najmniej połowy ustawowej liczby członków Senatu (art. 120 w zw. z art. 124 Konstytucji RP oraz art. 3 ust. 1 Regulaminu Senatu RP). Z uwagi na personalny charakter sprawy uchwała ta powinna być podjęta w głosowaniu tajnym (art. 53 ust. 6 Regulaminu Senatu RP), za pomocą opieczętowanych kart do głosowania[825]. Uchwałę Senatu Marszałek Senatu przekazuje Marszałkowi Sejmu. Podjęcie uchwały przez Senat, jak wynika z treści art. 91 ust. 1 pkt 1 Regulaminu Senatu, niezależnie od zajęcia w niej stanowiska pozytywnego czy negatywnego, jest obowiązkiem Senatu.

Niepodjęcie uchwały przez Senat w terminie miesiąca jest równoznaczne z wyrażeniem zgody. Wyrażenie zgody przez Senat w uchwale lub milczenie tej izby kończy procedurę parlamentarną powołania Generalnego Inspektora.

---

[823] W stosunku do analogicznej procedury wyłaniania RPO twierdzi tak m. in. J. Boć [w:] *Komentarz do Konstytucji RP*, Wrocław 1998, s. 312.
[824] W. Sokolewicz, *Art. 209*…, s. 6.
[825] *Ibidem*, s. 8.

Ustawa nie precyzuje także skutków sytuacji, gdy brak będzie zgody Senatu przy powołaniu GIODO[826]. W razie zaistnienia takiej okoliczności należy przyjąć, że Sejm nie może ani powołać Generalnego Inspektora. Jak podkreśla W. Skrzydło, „brak zgody Senatu na kandydata powołanego przez Sejm wymaga ponownego rozpoczęcia […] procedury"[827]. Brak zgody Senatu jest kategoryczny i nie może zostać oddalony przez Sejm, a zatem kończy procedurę w sprawie powołania kandydata na Generalnego Inspektora. Sprzeciw Senatu uniemożliwia powołanie tego samego kandydata, zatem konieczne jest wszczęcie nowej procedury, co rodzi konieczność zgłaszania w Sejmie wniosków w sprawie powołania innego kandydata[828]. W moim przekonaniu jednak skutki, gdy Senat nie wyraża zgody na powołanie na stanowisko GIODO konkretnego kandydata powinny być jednoznacznie określone w ustawie, aby wyeliminować ewentualne nadużycia oraz uniemożliwiać z góry zaplanowane negatywne decyzje Senatu w stosunku do określonych kandydatów.

4. Zasady działania Generalnego Inspektora Ochrony Danych Osobowych

a) uwagi ogólne

Generalny Inspektor Ochrony Danych Osobowych będąc organem właściwym w zakresie ochrony prywatności, realizuje swoje funkcje przede wszystkim jako organ ochrony prawa. Głównymi zasadami kreującymi instytucję organów powołanych do ochrony prawnej, w tym także polskiego GIODO, są: zasada niezależności (niezawisłości), niepołączalności (*incompatibilitas*), ochrony immunitetowej, apolityczności oraz kadencyjności. Zasady te stanowią prawem określone przesłanki, które warunkują istotę istnienia i charakter tego organu, możliwości i uprawnienia GIODO w zakresie ochrony prywatności jednostki oraz wpływają na właściwe wykonywanie działań nałożonych przez ustawę.

---

[826] Inne akty prawne rozstrzygają takie sytuacje w sposób jednoznaczny, m. in. na podstawie art. 3 ust. 5 ustawy z dnia 15 lipca 1987 r. o RPO, gdy „Senat odmawia wyrażenia zgody na powołanie Rzecznika, Sejm powołuje na stanowisko Rzecznika inną osobę".

[827] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Komentarz*, Kraków 1998, s. 225.

[828] W. Sokolewicz, *Art. 209*…, s. 8.

b) zasada niezależności

Prawidłowe wykonywanie zadań powierzonych GIODO wymaga przyznania mu pełnej niezależności w strukturze organów państwowych[829]. Do scharakteryzowania pozycji prawnej GIODO zastosować należy dwa określenia, o treści podobnej, ale nie identycznej: niezawisłość oraz niezależność (od innych organów państwowych). Niezależność odnosi się do urzędu, zaś niezawisłość do osoby piastującej określony urząd. Konstrukcja w zakresie niezależności i niezawisłości organu kontroli i ochrony prawa jest bliska również cechom, które wymagane są np. w przypadku sędziego czy RPO (art. 178 ust. 1, art. 210 Konstytucji RP). Należy jednak mieć na uwadze, że analogia ta nie jest zupełna, a wskazane uwagi można odnosić tylko odpowiednio, tzn. z uwzględnieniem istotnych różnic zachodzących między GIODO a pozycją prawną sędziego czy RPO.

Niezależność od innych organów państwowych (władzy publicznej) zakazuje ustanawiania takich więzi strukturalnych i funkcjonalnych pomiędzy GIODO a innymi organami władzy publicznej, które mogłyby uzależnić GIODO od nich, oczywiście poza ustawowymi wyjątkami pozostającymi w zgodności z zakresem działań urzędu GIODO. Gwarancją niezależności Generalnego Inspektora są przede wszystkim zastosowane szczegółowe rozwiązania prawne, dotyczące m. in. trybu powoływania i odwoływania tego organu, podległości organizacyjnej czy przyznania immunitetu. Niezależność buduje autonomię określonego organu tylko zewnętrznie, zakładając jednocześnie podporządkowanie organizacyjne wewnątrz organów ochrony prawnej korzystającego z tego atrybutu. Niezależność Generalnego Inspektora Ochrony Danych Osobowych przejawia się w jego odrębności względem jakiegokolwiek innego organu, przez co rozumie się brak organizacyjnej podległości w stosunku do organu niezajmującego się ochroną prawa czy w stosunku do każdego innego organu ochrony prawa[830]. Decyzji GIODO nie jest w stanie zmienić inny organ (wyjątkiem jest art. 21 u.o.d.o). GIODO nie jest także związany wytycznymi żadnych innych organów przy wydawaniu swoich decyzji. W zakresie wykonywania swoich zadań podlega tylko ustawie, a zatem nikt nie może wydawać mu

[829] Niezależność i niezawisłość organu do spraw ochrony danych osobowych jest obecnie standardem europejskim, co znajduje swoje odbicie w dyrektywie 95/46/WE (pkt 62 preambuły głosi, iż organ ochrony danych osobowych sprawuje nadane mu funkcje całkowicie niezależnie), a także w orzecznictwie ETS. Zob. wyrok z dnia 9 marca 2010 r. w sprawie *Komisja Europejska v. Republika Federalna Niemiec*, Sprawa C-518/07.

[830] B. Janusz-Pohl, *op. cit.*, s. 19-20.

jakichkolwiek poleceń bądź wskazówek, co jest przejawem pełnej niezależności tego organu (art. 8 ust. 4 u.o.d.o).

Niezależność Generalnego Inspektora ma jednak charakter względny, gdyż konstrukcja ustrojowa GIODO podporządkowuje go w zakresie odpowiedzialności centralnemu, naczelnemu organowi władzy państwowej, jakim jest Sejm. Generalna zasada niezależności jest więc na tej podstawie ograniczona, jednak nie wyłączona, przez uwzględnienie odpowiedzialności GIODO w zakresie i w formie, które określa ustawa. Odpowiedzialności, i to ograniczonej, przed Sejmem nie należy utożsamiać z podległością (tj. podporządkowaniem). Odpowiedzialność Generalnego Inspektora ponoszona przed Sejmem, w ustawowo określonej formie i na ustawowo określonych zasadach, nie powoduje całkowitego wyłączenia zasady niezależności GIODO, a jedynie ogranicza jej zasięg. Co najważniejsze, formuła ponoszenia odpowiedzialności jedynie przed Sejmem nabiera szczególnego znaczenia w kontekście nieustanowienia konstytucyjnej odpowiedzialności GIODO przed Trybunałem Stanu (co wynika wprost z braku uwzględnienia GIODO w katalogu organów odpowiedzialnych przed Trybunałem Stanu na mocy art. 198 ust. 1 i 2 Konstytucji RP)[831].

Formy odpowiedzialności oraz wyraz pewnego podporządkowania GIODO przed Sejmem zostały określone w ustawie sposób dość restrykcyjny. Po pierwsze, GIODO jest powoływany przez Sejm (art. 8 ust. 2 u.o.d.o). Po drugie, bez uprzedniej zgody Sejmu GIODO nie może być pociągnięty do odpowiedzialności karnej ani pozbawiony wolności, a zatem ustawa uzależnia uchylenie immunitetu od wydania zgody przez Sejm (art. 11 u.o.d.o). Po trzecie, tylko w ściśle określonych przez ustawę okolicznościach Sejm (za zgodą Senatu) może odwołać GIODO przed upływem kadencji (art. 8 ust. 8 u.o.d.o). Po czwarte, przed Sejmem GIODO składa ślubowanie (art. 9 u.o.d.o). Po piąte, Marszałek Sejmu na wniosek Generalnego Inspektora może powołać zastępcę Generalnego Inspektora (art. 12a u.o.d.o); GIODO w trybie art. 20 u.o.d.o. ma obowiązek składać Sejmowi raz do roku sprawozdanie ze swej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych.

Obowiązek złożenia sprawozdania ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów jest to jedna z form odpowiedzialności

---

[831] W. Sokolewicz, *Art. 210* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom III, red. L. Garlicki, s. 6.

GIODO przed Sejmem. Sprawozdanie jest dobrą okazją do przedstawienia przez Generalnego Inspektora nie tylko wniosków co do stanu obecnego, ale także postulatów *de lege ferenda.*

U.o.d.o. nie precyzuje, w jakiej formie ma zostać złożone sprawozdanie. Nie zostało wprost określone, czy przedstawiana Sejmowi relacja z rocznej działalności ma być jedynie informacją, czy też pewnego rodzaju sprawozdaniem, nad którym należy głosować, i jak się wydaje, Sejm RP skłania się do drugiego rozwiązania[832]. Problem ten wystąpił na kanwie obrad Komisji Konstytucyjnej analizującej różnicę pomiędzy informacją a sprawozdaniem składanym przez RPO. Ostatecznie przyjęto, że dokument przedkładany Sejmowi przez RPO będzie informacją, kierując się argumentem, iż sprawozdanie musiałoby zakładać jakąś konsekwencję jego odrzucenia, a informacja powinna zostać wysłuchana i przyjęta do wiadomości nawet bez głosowania[833]. Analizując wyżej wskazane argumenty należy uznać zatem, że obowiązek Generalnego Inspektora wyrażony w art. 20 u.o.d.o. przyjmuje postać sprawozdania, zgodnie z brzmieniem *expressis verbis* tego artykułu. Wskazując dalej można zauważyć, iż sprawozdanie przedkłada się tylko Sejmowi, a informacja wiąże się z informowaniem co do Sejmu i Senatu (por. art. 212 Konstytucji RP). Ponadto z obowiązkiem informacyjnym nie wiążą się żadne konsekwencje prawne, a zwłaszcza dotyczące oceny pracy organu. Biorąc zatem pod uwagę wyżej wskazane rozważania należy uznać, że obowiązek Generalnego Inspektora wyrażony w art. 20 u.o.d.o. przyjmuje postać sprawozdania, które stanowi tym samym podstawę dla oceny działalności Generalnego Inspektora. Zakres tej oceny jest jednak ograniczony choćby z tego powodu, że ustawa nie przewiduje ani formy ani rodzaju przekazywanego sprawozdania. Ewentualna ocena Generalnego Inspektora ze strony Sejmu ma zatem charakter nieobiektywny. Negatywna ocena sprawozdania GIODO w Sejmie powinna pociągnąć za sobą postawienie wniosku o jego odwołanie z racji chociażby niewłaściwego realizowania obowiązków, jednak żaden przepis nie nakazuje wprost posłom takiego zachowania wobec braku akceptacji sprawozdania.

Realizacja obowiązku sporządzenia i przedstawienia Sejmowi przedmiotowego sprawozdania nastąpić ma do końca roku kalendarzowego. Art. 20 u.o.d.o. nie stanowi jednak o tym wyraźnie, lecz jego brzmienie uzasadnia założenie, że sprawozdania powinny być składane za miniony rok kalendarzowy. Dotyczy to także sytuacji, gdy kadencja GIODO

---

[832] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, s. 437.

[833] Zob. wypowiedzi posłów J. Cierniewskiego oraz I. Lipowicz, „Biuletyn Komisji Konstytucyjnej Zgromadzenia Narodowego", nr XXVI, s. 63.

rozpoczyna się po 1 stycznia danego roku kalendarzowego i wówczas sprawozdanie jest składane za niepełny rok kalendarzowy[834].

Wszystkie wskazane powiązania GIODO z Sejmem nie czynią na pewno z Generalnego Inspektora organu Sejmu. W stosunku do każdego innego podmiotu oraz organu państwowego, w tym organu ochrony prawa rodzajowo odmiennego od GIODO, Generalny Inspektor pozostaje organem niezależnym w zakresie pełnionych obowiązków.

Druga ze wskazanych zasad, charakterystyczna dla GIODO, to niezawisłość tego organu. Niezawisłość zawiera w sobie zarówno aspekt zewnętrzny i wewnętrzny powodując, że organ korzystający z tego przywileju pozostaje w niezależności organizacyjnej od każdego innego organu, czy to ochrony prawa czy też nie[835]. Przejawem niezawisłości GIODO jest chociażby istnienie przewidzianych ustawą zakazów względem osoby piastującej tę funkcję. Niezawisłość oznacza, że osoby korzystające z tego typu przywileju w zakresie pełnionych przez nie funkcji nie podlegają niczyim poleceniom, ale mają obowiązek wykonywania swoich czynności zgodnie z prawem i ich wewnętrznym, wolnym od wszelkiego nacisku, przekonaniem[836]. W takim ujęciu niezawisłość GIODO można byłoby interpretować w oparciu o reguły chociażby niezawisłości subiektywnej (wewnętrznej), zaliczone w orzecznictwie TK do standardów niezawisłości sędziowskiej[837]. Na tej podstawie wszelkie metaprawne motywy o charakterze politycznym, filozoficznym czy światopoglądowym powinny być odsunięte od prawnych działań organu. Jest to jak najbardziej stanowisko słuszne w wyjściowym punkcie, jednak w moim przekonaniu akurat w stosunku do Generalnego Inspektora zbyt daleko posunięte, zaś aspekt subiektywny (wewnętrzny) nie jest aż tak kluczowy w odniesieniu do niezawisłości GIODO jak chociażby w stosunku do sędziów. Pomimo to, w stosunku do żadnej z czynności podejmowanej przez Generalnego Inspektora nie jest dopuszczalna ingerencja z zewnątrz, ani stosowanie nacisków, włącznie z Sejmem, wobec którego GIODO pozostaje podległy. Nawet wymóg stawiany kandydatowi na stanowisko GIODO odróżniania się wysokim autorytetem moralnym wskazuje, iż osoba sprawująca to stanowisko powinna charakteryzować się wewnętrznymi cechami, zapewniającymi jej neutralność i bezstronność w sprawowaniu powierzonych obowiązków. Realizowanie zatem ustawowych wytycznych powinno opierać się na stosowaniu

---

[834] A. Drozd, *op. cit.*, s. 112.
[835] Zasada niezawisłości zwykle najbardziej dotyczy organów o charakterze rozstrzygającym, sprawujących wymiar sprawiedliwości w RP tj. sędziów sądów powszechnych, wojskowych i administracyjnych, sędziów Sądu Najwyższego czy sędziów Trybunału Konstytucyjnego. Zob. art. 178 ust. 1 Konstytucji RP.
[836] B. Janusz-Pohl, *op. cit.*, s. 20.
[837] Zob. wyrok TK z dnia 24 czerwca 1998, K 3/98, OTK ZU 1998, nr 4, poz. 52, s. 430 i n.

obiektywnych argumentów zebranych chociażby w trakcie przeprowadzanej kontroli czy będących podstawą do wydawania decyzji administracyjnych.

c) zasada niepołączalności (*incompatibilitas*)

Na wybranego już Generalnego Inspektora ustawa nakłada warunki, które zobowiązany jest spełnić, by móc należycie sprawować urząd, a które także pozwalają zagwarantować mu całkowitą niezależność zawodową, polityczną i związkową.

Generalny Inspektor nie może zajmować innego stanowiska, z wyjątkiem stanowiska profesora szkoły wyższej, ani wykonywać innych zajęć zawodowych, co stanowi gwarancję niezależności urzędu GIODO (art. 10 ust. 1 u.o.d.o). Zakaz dotyczący podejmowania przez GIODO innych zajęć zawodowych został sformułowany bardzo restrykcyjnie[838]. Niepołączalność urzędu GIODO z innymi stanowiskami i zajęciami obejmuje wszelkie inne poza urzędem GIODO stanowiska publiczne, zajmowane na podstawie mianowania, powołania, wyboru czy umowy, w tym niezależnie czy będzie to umowa o pracę, umowa o dzieło, czy każda inna umowa zobowiązująca daną osobę do wykonania określonych zajęć zawodowych. Zakaz wykonywania innych zajęć zawodowych rozciąga się też na wszelkie zajęcia zawodowe, niezależnie od ich rodzaju, wymiaru czasu czy podstawy prawnej ich podejmowania. Jedyny wyjątek, określony bardzo wąsko, dotyczy zajmowania stanowiska profesora szkoły wyższej, który rozciąga się na wszystkie rodzaje szkół wyższych, w tym publiczne i niepubliczne[839]. Wyjątek dotyczy tylko stanowiska profesora, a nie w ogólności nauczyciela akademickiego[840]. Obejmuje osoby zajmujące stanowisko profesora, bez względu na to, czy mają tytuł naukowy profesora, a zatem praktycznie wszystkich wykładających w szkołach wyższych, mających ku temu kwalifikacje potwierdzone habilitacją, a w wielu przypadkach także i doktoratem, jeśli przez władze uczelni zostali powołani na stanowisko profesora[841]. Nie obejmuje jedynie stanowiska profesora w placówkach PAN oraz w placówkach badawczo-rozwojowych[842]. W przypadku przedmiotowego zakazu nie ma także

---

[838] Zakaz innych zajęć zawodowych zawarty w art. 10 ust. 1 u.o.d.o. obejmuje dokładnie takie same przesłanki jak w przypadku zakazu dotyczącego RPO zawartego w art. 209 ust. 2 Konstytucji RP, a także w stosunku do prezesa NIK na podstawie art. 205 ust. 3 Konstytucji RP. Zob. W. Sokolewicz, *Art. 210*…, s. 8 oraz W. Sokolewicz, *Art. 205*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom III, red. L. Garlicki, s. 9-13.

[839] Identyczny zakaz został sformułowany w stosunku do Rzecznika Praw Obywatelskich w art. 209 ust. 2 Konstytucji RP oraz prezesa NIK w art. 205 ust. 2 Konstytucji RP.

[840] A. Sylwestrzak, *op. cit.*, s. 202.

[841] W. Sokolewicz, *Art. 205*…, s. 8.

[842] *Ibidem*, s. 8; W. Sokolewicz, *Artykuł 210*…, s. 8.

znaczenia podstawa prawna objęcia stanowiska profesora, czy jest nią akt mianowania, czy umowa o pracę[843].

Wskazane w art. 10 ust. 1 u.o.d.o. gwarancje niezależności zawodowej obejmują także *incompatibilitas,* tj. zakaz kumulacji pełnionych funkcji w stosunku do organu ochrony prawnej, równoczesnego wykonywania czynności ochrony prawnej różnego rodzaju przez ten sam podmiot, a także kumulacji różnorodnych funkcji publicznych, w ramach których są realizowane zadania ochrony prawnej[844]. Oznacza to także niemożność wykonywania innych czynności zawodowych.

Wbrew podnoszonym w doktrynie opiniom uzyskanie urlopu bezpłatnego u dotychczasowego pracodawcy jest wystarczające dla spełnienia wymogu *incompatibilitas*[845]. Rozwiązanie takie pociąga za sobą zaprzestanie wykonywania innych czynności zawodowych, a ustawodawca posługuje się właśnie konstrukcją urlopu bezpłatnego dla osób zobowiązanych do niełączenia funkcji i stanowisk[846]. W przypadku jednak prowadzenia działalności gospodarczej, konieczne będzie jej zawieszenie przez nowo wybranego Generalnego Inspektora[847]. Zakazu *incompatibilitas* nie narusza jednak osiąganie przychodów z praw majątkowych, najmu czy dzierżawy[848].

d) zasada apolityczności

Sprawowanie urzędu GIODO obejmuje także zakaz przynależności do partii politycznej i związku zawodowego oraz zakaz prowadzenia działalności publicznej niedającej się pogodzić z godnością jego urzędu (art. 10 ust. 2 u.o.d.o.). Zakazy te mają zapewnić apolityczność urzędu, zasadę obiektywizmu i bezstronności w działaniach, a także ochronę autorytetu GIODO.

Nakaz apolityczności formalnej został sformułowany bardzo rygorystycznie. Obejmuje, po pierwsze, już samą formalną przynależność partyjną, bez względu na rozmiary, czy rodzaj partii i faktycznie prowadzonej w ramach partii działalności. Po drugie, wyklucza także jakąkolwiek aktywność w partii politycznej, w tym zasiadanie we władzach partyjnych, zajmowanie stanowisk o charakterze politycznym, czy nawet ubieganie się o te stanowiska, w

---

[843] P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z 2 IV 1997*, Warszawa 2000, s. 263.
[844] B. Janusz-Pohl, *op. cit*., s. 22.
[845] A. Drozd, *Ustawa…*, s. 86.
[846] Zob. art. 24b ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. Nr 16, poz. 95 z późn. zm.)
[847] Prawo do zawieszenia działalności gospodarczej przewiduje art. 14a ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. Nr 173, poz. 1807 z późn. zm.)
[848] T. Szewc, *op. cit*., s. 89.

szczególności kandydowanie w wyborach[849]. Zakaz aktywnej przynależności partyjnopolitycznej dotyczy na tych samych zasadach przynależności oraz aktywności w stosunku do każdego związku zawodowego. Ma to swoje uzasadnienie w osobliwościach polskiego systemu politycznego i charakterze społeczeństwa obywatelskiego, w którym związki zawodowe nierzadko wypełniały funkcje partii, a partie - już nie tak często - związków[850].

Zakaz przynależności do partii politycznych czy związków zawodowych to całkowita niemożność pozostawania w stosunku członkostwa z tymi organizacjami. Słusznie zatem zauważa się, że zawieszenie członkostwa w partii politycznej lub w związku zawodowym narusza ten zakaz[851]. Jak stwierdził Trybunał Konstytucyjny: „partyjność ma na celu usunięcie zagrożenia płynącego z faktu istnienia organizacyjnych i politycznych więzi pomiędzy osobą sprawującą funkcje publiczne a partią polityczną. Zagwarantowanie apolityczności służb publicznych nie jest możliwe do realizacji w sytuacji, gdy osoby pełniące takie funkcje są członkami ugrupowań politycznych”[852]. W tym samym wyroku Trybunał Konstytucyjny, badając zgodność art. 10 ust. 2 u.o.d.o. z Konstytucją RP (obok innych przepisów wprowadzających podobne ograniczenia), przedstawił następującą argumentację: „zakaz członkostwa w partii politycznej Generalnego Inspektora Ochrony Danych Osobowych […], gwarantuje niezawisłość i niezależność tego organu względem organów administracji publicznej, a także zapewnia apolityczność i wzmacnia autorytet Generalnego Inspektora Ochrony Danych Osobowych. Niezawisłość i niezależność organu czuwającego nad ochroną danych osobowych uznane mogą być obecnie za standard europejski […]. Generalny Inspektor w zakresie swoich zadań podlega tylko ustawie (art. 8 ust. 4 u.o.d.o.). W zakresie wykonywanych zadań nikt nie może wydawać Generalnemu Inspektorowi jakichkolwiek poleceń czy wskazówek. Niezależność Generalnego Inspektora można pod tym względem porównać do niezależności sądu czy sędziego. Fakt przyznania Generalnemu Inspektorowi kompetencji władczych uzasadnia, w ocenie Trybunału Konstytucyjnego, wprowadzenie ustawowych ograniczeń wolności zrzeszania się”[853]. Zawarte w art. 10 ust. 2

---

[849] A. Pieniążek, *Rzecznik Praw Obywatelskich w systemie organów państwa,* [w:] *Ustrój i struktura aparatu państwowego i samorządu terytorialnego*, red. W. Skrzydło, Warszawa 1997, s. 202; L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu,* Warszawa 2004, s. 413.
[850] W. Sokolewicz, *Artykuł 205*..., s. 11.
[851] A. Drozd, *Ustawa…*, s. 87.
[852] Wyrok TK z dnia 10 kwietnia 2002 r., K 26/00, OTK-A 2002, nr 2, poz. 18 z aprobującą glosą M. Granata, „Przegląd Sejmowy” 2002, nr 4, s. 79.
[853] *Ibidem*, s. 79.

u.o.d.o. przesłanki w stosunku do Generalnego Inspektora nakazują mu zatem zachowanie przynajmniej neutralności politycznej, a najlepiej apolityczności.

To nie koniec ograniczeń, jakie u.o.d.o. w art. 10 nakłada na Generalnego Inspektora. O ile zakaz przynależności do partii politycznej lub związku zawodowego ma łatwą do odczytania treść, o tyle treści zakazu dotyczącego prowadzenia działalności publicznej nie jest tak łatwo ustalić. Ograniczenie dotyczy działalności publicznej, ale tylko takiej, której nie da pogodzić się z godnością urzędu. Nawiązując analogicznie do takich samych restrykcji, które w art. 205 ust. 3 Konstytucji RP zostały nałożone na Prezesa NIK, można wnioskować, iż stylizacja przedmiotowego zakazu nie jest fortunna, gdyż nie chodzi w nim o zakaz prowadzenia takiej działalności publicznej, która godziłaby w godność sprawowanego urzędu, lecz w istocie takiej, która podważa wymóg bezstronności i politycznej neutralności. Każda zatem działalność o charakterze politycznym, angażowanie się po stronie określonego ugrupowania politycznego i rywalizacja polityczna jest zakazana i nie do pogodzenia z godnością urzędu GIODO, gdyż naruszać będzie neutralność i bezstronność polityczną tego urzędu.

Omawiany zakaz obejmuje prowadzenie działalności, a nie jedynie sprawowanie funkcji. Jak wyjaśnił Trybunał Konstytucyjny, „funkcja" oznacza trwałe wykonywanie określonych obowiązków lub realizowanie uprawnień w zakresie sprawowania władzy publicznej w jakimkolwiek segmencie tej władzy[854]. Użycie określenia „działalność", a nie „funkcja", oznacza rezygnację z cechy polegającej na wykonywaniu trwałym, przez co zakaz obejmujący prowadzenie działalności publicznej został w ten sposób rozciągnięty na wykonywanie czasowe, a nawet jednorazowe wykonywanie obowiązków czy realizowanie uprawnień w sferze władzy publicznej[855].

Przedstawione w art. 10 ust. 2 u.o.d.o. zakazy względem Generalnego Inspektora mają taką samą konstrukcję jak zawarte w art. 209 ust. 3 Konstytucji RP w przypadku RPO czy Prezesa NIK w art. 205 ust. 3 Konstytucji RP. Jak najbardziej zatem można się tu posłużyć uzasadnieniem sformułowanym przez B. Banaszaka, adekwatnym wobec pozycji GIODO. Autor ten definiując pojęcie działalności publicznej, proponuje rozumieć je podobnie, jak użyte zostało to określenie w innych postanowieniach Konstytucji (np. art. 178 ust. 3), a dla ustalenia jego sensu postuluje, by wziąć pod uwagę zasadę niezawisłości i niezależność od innych organów[856]. Chodzi zatem o to, by osoba piastująca np. funkcję RPO nie podejmowała

---

[854] Wyrok TK z dnia 17 listopada 1998, K 42/97, OTK ZU 1998, nr 7, poz. 113.
[855] W. Sokolewicz, *Artykuł 205*…, s. 11.
[856] B. Banaszak, *Konstytucja…*, s. 910.

działań publicznych mogących podważyć zaufanie do jej niezawisłości i niezależności. Zakaz prowadzenia działalności publicznej obejmuje także zakaz przynależności do ruchów o charakterze politycznym czy stowarzyszeń.

Analizując zakazy o charakterze zawodowym i polityczno-związkowym dotyczące urzędu GIODO, warto jest też wspomnieć, że w doktrynie podnosi się, iż zakaz podejmowania określonej działalności publicznej należy także rozpatrywać w kontekście zasady „twardej apolityczności”[857]. Pogląd ten wprawdzie bezpośrednio dotyczy RPO, ale z uwagi na wspomniane identyczne zakazy w stosunku do GIODO jest on w tym miejscu właściwy. „Twarda apolityczność” obejmuje nie tylko zakaz angażowania się w bieżące wydarzenia polityczne w charakterze uczestnika tych wydarzeń, lecz również powstrzymywanie się od wypowiedzi politycznych, zawierających politycznie motywowane oceny albo dotyczących często politycznych tematów[858].

Zachowania GIODO respektujące zasadę apolityczności urzędu czy niezależności zawodowej przyczyniają się do wzmocnienia prestiżu instytucji i samej osoby GIODO w opinii publicznej, a także pozytywnej oceny pracy Generalnego Inspektora. Także kandydat na stanowisko GIODO nie powinien uchybiać wskazanym zakazom już w momencie podejmowania przez Sejm uchwały o powołaniu.

e) zasada ochrony immunitetowej

Biorąc pod uwagę status Generalnego Inspektora Ochrony Danych Osobowych, jego rangę i wyznaczone zadania, ustawodawca przyznał mu immunitet (art. 11 u.o.d.o.o), na równi z immunitetem przysługującym Rzecznikowi Praw Obywatelskich (art. 211 Konstytucji RP), Prezesowi Najwyższej Izby Kontroli (art. 206 Konstytucji RP) czy posłom i senatorom (art. 105 Konstytucji RP). Generalny Inspektor nie może być bez uprzedniej zgody Sejmu pociągnięty do odpowiedzialności karnej ani pozbawiony wolności. Nie może być zatrzymany lub aresztowany, z wyjątkiem ujęcia go na gorącym uczynku przestępstwa i jeżeli jego zatrzymanie jest niezbędne do zapewnienia prawidłowego toku postępowania. O zatrzymaniu niezwłocznie powiadamia się Marszałka Sejmu, który może nakazać natychmiastowe zwolnienie zatrzymanego.

---

[857] Zob. Z. Witkowski, *Prawo konstytucyjne*, Toruń 1998, s. 436.
[858] Zob. T. Bichta, *Rzecznik Praw Obywatelskich,* [w:] *Ustrój organów ochrony prawnej,* red. B. Szmulik, M. Żmigrodzki, Lublin 2003, s. 243.

Ustawa gwarantuje Generalnemu Inspektorowi niekaralność i nietykalność osobistą. Posiadanie immunitetu formalnego (procesowego) gwarantuje zakaz pociągnięcia do odpowiedzialności karnej lub pozbawienia wolności bez względu na przesłanki prawne. Generalny Inspektor nie może zostać zatrzymany ani aresztowany z wyjątkiem ujęcia *in flagranti delicti* oraz nie może być pociągnięty do odpowiedzialności karnej ani pozbawiony wolności bez uprzedniej zgody Sejmu. Immunitet Generalnego Inspektora obejmuje wszelką odpowiedzialność prawnokarną, także za wykroczenia, obejmując czyny ścigane z oskarżenia publicznego i prywatnego. Nie obejmuje jednak odpowiedzialności cywilnej ani dyscyplinarnej.

W ramach immunitetu GIODO uwzględniona została gwarancja nietykalności, która chroni Generalnego Inspektora przed wszelkimi przewidzianymi prawem formami pozbawienia wolności, tj. zatrzymaniem, aresztowaniem, a więc skutkami działań nawet uprawnionych i podejmowanych przez kompetentne organy państwa. Gwarancja ta rozciąga się na swobodę dysponowania własną osobą i wynika z niej zakaz np. osobistego przeszukania (tzw. rewizji osobistej) czy polecenia określonego zachowania, np. poddania się jakiemuś badaniu (np. na wariografie)[859].

Immunitet GIODO ma charakter względny, co oznacza, że nie ma charakteru absolutnego. Odstąpienie od niekaralności i nietykalności jest możliwe za zgodą Sejmu. W takim ujęciu Sejm występuje jako najwyższy gwarant skuteczności immunitetu[860]. Co więcej, Generalny Inspektor może być zatrzymany w przypadku ujęcia na gorącym uczynku przestępstwa i jeżeli jego zatrzymanie jest niezbędne do zapewnienia prawidłowego toku postępowania. Te dwie przesłanki muszą zostać jednak spełnione łącznie, by można było odstąpić od zatrzymania lub aresztowania Generalnego Inspektora. W doktrynie i orzecznictwie sądowym oraz sądowokonstytucyjnym uznaje się również, iż dopuszczone jest pozbawienie wolności osoby chronionej immunitetem w okolicznościach nadzwyczajnych, zwłaszcza spowodowanych bezprawnym działaniem danej osoby (np. zablokowanie kierowanym pojazdem drogi publicznej), stosując tu znaną prawu karnemu konstrukcję stanu wyższej konieczności[861]. W ostatnim przypadku i w przypadku ujęcia GIODO *in flagranti* o zatrzymaniu niezwłocznie należy poinformować Marszałka Sejmu, który może nakazać natychmiastowe zwolnienie zatrzymanego.

---

[859] W. Sokolewicz, *Artykuł 206*…,s. 3.
[860] Z. Witkowski, *op. cit.,* s. 516.
[861] W. Sokolewicz, A*rtykuł 206*…, s. 3.

Immunitet przyznany Generalnemu Inspektorowi ma go chronić m. in. przed nieuzasadnionym wszczynaniem postępowania karnego, zwłaszcza z oskarżenia prywatnego dokonanego w rewanżu np. za przeprowadzone kontrole czy wydane decyzje administracyjne. Jest gwarancją bezstronnego i wolnego od nacisków wykonywania przez GIODO funkcji kontrolnych. Osoba nim objęta nie może, w przeciwieństwie do parlamentarzysty objętego immunitetem parlamentarnym (art. 105 ust. 4 Konstytucji RP), z własnej woli zrezygnować z obrony[862].

f) zasada kadencyjności

W literaturze podkreśla się, iż zasadą funkcjonowania organów państwowych jest ich kadencyjność, polegająca na udzieleniu danemu organowi w konkretnym składzie personalnym pełnomocnictw na określony czas. Kadencyjność zapewnia rotację składu osobowego; gwarantuje horyzont wykonywania kompetencji przypisanych danemu organowi i pewną cykliczność poddawania kontroli sposobu zajmowania stanowisk; zapewnia, że dane stanowisko nie będzie personalnie związane z określoną osobą oraz daje szanse zapewnienia stabilizacji składu osobowego, aby umożliwić niezależne wykonywanie zadań organu w ramach danej kadencji[863].

Czas trwania kadencji organu nie jest pozbawiony znaczenia, gdyż dla zapewnienia prawidłowego funkcjonowania organu kadencja nie powinna być ani za długa, ani za krótka[864]. Wskazuje się, że im krótsza kadencja np. organu przedstawicielskiego, tym bardziej z wyborcami związani są przedstawiciele, gdyż częste wybory zapewniają odzwierciedlenie poglądów społeczeństwa. Piastujący urząd są jednak wówczas mniej aktywni, gdyż prawie wyłącznie skupiają się na zapewnieniu sobie reelekcji. Zbyt krótka kadencja nie daje także możliwości prawidłowego wdrożenia się w pełnieniu nowych obowiązków, gdyż nowo wybrani piastunowie niejednokrotnie potrzebują więcej czasu na zapoznanie się z pracą, a wówczas kończy się kadencja. Z kolei zbyt długa kadencja organu powodować może zasiedziałość i zbytnią pewność w sprawowaniu władzy, co utrudnia egzekwowanie wykonywania powierzonych obowiązków przez organ. Aczkolwiek dłuższa kadencja zapewniać ma stabilność i rzetelność w wykonywaniu powierzonych zadań, gdyż organ ma

---

[862] P. Winczorek, *op. cit.*, s. 264.
[863] M. Zubik, *Powoływanie członków Rady Polityki Pieniężnej w świetle zasad kadencyjności oraz działalności organów państwa*, „Przegląd Sejmowy" 2005, nr 4, s. 41.
[864] Zob. B. Banaszak, *Prawo konstytucyjne*, Warszawa 1999, s. 458.

już wystarczającą ilość czasu na zapoznanie się z powierzonymi obowiązkami oraz na ich prawidłową realizację.

U.o.d.o. w art. 8 ust. 5 i ust. 6 wprowadza kadencyjność urzędu GIODO, wskazując iż kadencja Generalnego Inspektora trwa 4 lata. Kadencja GIODO liczy się od dnia złożenia ślubowania na zasadach i według roty, której treść zawiera art. 9 u.o.d.o. Dzień złożenia ślubowania jest więc zarazem dniem objęcia stanowiska przez Generalnego Inspektora, tj. dniem przystąpienia do wykonywania przez niego obowiązków. W przypadku GIODO w ustawie przyjęto kadencję czteroletnią, i jest o rok krótsza od kadencji porównywanego do GIODO – RPO. Kadencja Generalnego Inspektora została zrównana z kadencją izb parlamentarnych, co wprowadziło niewątpliwie widoczny aspekt polityczny w wyborze i zasadach funkcjonowania tego organu. W moim przekonaniu słuszne byłoby zróżnicowanie kadencji Generalnego Inspektora w stosunku do kadencji parlamentu. Z uwagi na monokratyczny (jednoosobowy) charakter instytucji GIODO, wydłużenie kadencji do 5 lat zapewniłaby dodatkową gwarancję niezależności i stabilności tego organu. Kadencja GIODO nie pokrywałaby się z kadencją parlamentu, co zapewniłoby stabilność, samodzielność i neutralność w wykonywaniu obowiązków przez GIODO.

Wydłużenie kadencji tego organu wpłynęłoby także korzystnie na postrzeganie GIODO jako jednego z organów powołanych do ochrony prawa, podobnego w zasadach funkcjonowania do rzeczników, których głównym zadaniem - jak i GIODO - jest ochrona praw i wolności jednostki. Brak zrównania długości kadencji GIODO z RPO zdaje się sugerować, że znaczenie Generalnego Inspektora w systemie organów państwowych jest mniejsze. Tymczasem współcześnie, wobec narastających w lawinowym tempie różnych form nadużyć praw człowieka związanych z ochroną prywatności poprzez wykorzystywanie nowych technologii, taka odmienność w ujmowaniu pozycji ustrojowej obu organów za pomocą kryterium kadencji nie wydaje się być uprawniona.

Po upływie kadencji Generalny Inspektor pełni swoje obowiązki do czasu objęcia stanowiska przez nowego Generalnego Inspektora. Taka konstrukcja stanowi zabezpieczenie na wypadek, gdyby parlamentarna procedura powołania nowego Generalnego Inspektora nie zakończyła się w czasie gwarantującym płynność przejęcia stanowiska przez kolejną osobę z chwilą upływu kadencji poprzedniej[865].

[865] R. Szałowski, *op. cit.,* s. 39.

Ta sama osoba nie może sprawować tego urzędu więcej niż przez dwie kadencje[866]. Nie jest istotne przy tym, czy kadencje następują bezpośrednio po sobie, czy są oddzielone kadencją lub kadencjami innych osób sprawujących urząd GIODO. *Ratio legis* takiego rozwiązania jest dążenie do jak najskuteczniejszego zabezpieczenia niezawisłości tego urzędu przed wszelkimi zewnętrznymi i wewnętrznymi wpływami, zwłaszcza w obliczu możliwości objęcia kolejnych kadencji. Co więcej, obowiązywanie tego zakazu ma także na celu wprowadzenie rotacji na stanowisku, chroniąc Generalnego Inspektora przed popadnięciem w rutynę w pełnieniu obowiązków oraz przed traktowaniem spraw szablonowo i bez większego zaangażowania.

Przedterminowe wygaśnięcie kadencji następuje z chwilą śmierci, odwołania lub utraty obywatelstwa polskiego przez Generalnego Inspektora (art. 8 ust. 7 u.o.d.o.) i w tych wyjątkowych przypadkach kadencja Generalnego Inspektora może zakończyć się przed upływem 4-letniego okresu.

Przedterminowe odwołanie Generalnego Inspektora przez Sejm za zgodą Senatu następuje z kolei tylko w wyraźnie wskazanych przypadkach, tj. w wyniku zrzeczenia się przez niego stanowiska, gdy stał się on trwale niezdolny do pełnienia obowiązków na skutek choroby, sprzeniewierzył się złożonemu ślubowaniu lub gdy został skazany prawomocnym wyrokiem sądu za popełnienie przestępstwa (art. 8 ust. 8 pkt 1-4 u.o.d.o.) [867].

W przypadku trwałej niezdolności do pełnienia obowiązków na skutek choroby, ustawodawca pozostawił dokonanie oceny sytuacji samemu Sejmowi, czy rzeczywiście Generalny Inspektor jest trwale niezdolny do pełnienia obowiązków na skutek choroby. W przypadku zaś zrzeczenia się stanowiska przez samego GIODO, sprzeniewierzenia się złożonemu ślubowaniu czy skazania skazany prawomocnym wyrokiem sądu za popełnienie przestępstwa Sejm nie może nie podjąć uchwały o odwołaniu.

O ile okoliczności z art. 8 ust. 8 pkt 1-2 i 4 są oczywiste , to wykazanie w praktyce, że Generalny Inspektor dopuścił się sprzeniewierzenia ślubowaniu jest wysoce utrudnione. „Sprzeniewierzyć się" oznacza dopuścić się zdrady, odstępstwa lub nie dotrzymać czegoś[868]. Z uwagi na ogólne sformułowanie roty ślubowania, zgodnie z którym Generalny Inspektor zobowiązuje się dochować wierności postanowieniom Konstytucji oraz sumiennie i

---

[866] Zob. W. Sokolewicz, *Artykuł 209,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, s. 3.

[867] Stosowanie do wytycznych z art. 8 ust. 8 pkt 4 u.o.d.o., Generalny Inspektor może zostać odwołany ze swojego stanowiska w przypadku popełnienia jakiegokolwiek przestępstwa, np. zniewagi - czynu ściganego z oskarżenia prywatnego.

[868] *Słownik języka polskiego*, t. 3, red. M. Szymczak, Warszawa 1995, s. 288.

bezstronnie wykonywać powierzone mu obowiązki, trudno jest jednoznacznie ustalić czy doszło do sprzeniewierzenia. W nawiązaniu do podobnego rozwiązania, zawartego w art. 7 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich, w literaturze podkreśla się, że za sprzeniewierzenie się mogą zostać uznane powtarzające się i przybierające postać utrwalonej praktyki: podejmowanie działań mających na celu ograniczenie praw i wolności obywatelskich, uporczywa bezczynność organu, przejawiająca się brakiem działań na rzecz ochrony praw i wolności obywatelskich w sprawach, w których w sposób niebudzący wątpliwości pożądana byłaby aktywność organu, czy też brak bezstronności, polegający np. na angażowaniu się w trakcie pełnienia funkcji w działalność polityczną lub publiczną, niedającą się pogodzić z godnością urzędu[869]. Wszystkie przykładowo wymienione działania spełniające kryterium zachowania sprzeniewierzającego się złożonemu ślubowaniu pozostawałyby w jawnej sprzeczności z niezależnością i niezawisłością urzędu GIODO. Podstawą do oceny, czy doszło do sprzeniewierzenia się złożonemu ślubowaniu, nie powinien być jednak incydentalny przypadek, a raczej długotrwała niezgodna ze złożonym ślubowaniem działalność GIODO. Możliwość odwołania GIODO w przypadku, gdy sprzeniewierzył się złożonemu ślubowaniu, jest wyrazem odpowiedzialności Generalnego Inspektora przed Sejmem, z uwagi na kryteria ocenne wynikające z treści roty ślubowania, co nie wyklucza także upolitycznionego charakteru tej odpowiedzialności.

Stosownie do wytycznych z art. 8 ust. 8 pkt 4 u.o.d.o., Generalny Inspektor może zostać odwołany ze swojego stanowiska także w przypadku popełnienia jakiegokolwiek przestępstwa, czy to ściganego z oskarżenia prywatnego, czy publicznego.

Katalog przesłanek uzasadniających odwołanie GIODO jest wyczerpujący i zamknięty, co stanowić ma po raz kolejny istotną gwarancję niezależności tego organu. Nie jest możliwe odwołanie Generalnego Inspektora z innych, niewskazanych w art. 8 ust. 8 u.o.d.o. przyczyn.

W tym przypadku ustawa także nie konkretyzuje (jak i w przypadku powołania), do kogo należy inicjatywa, kto może wystąpić z wnioskiem o odwołanie tego organu. Kwestię tę rozstrzyga regulamin Sejmu odwołując się do regulacji dotyczących powołania GIODO. Uchwała Sejmu w przedmiocie odwołania GIODO jest przesyłana przez Marszałka Sejmu niezwłocznie Marszałkowi Senatu w celu wyrażenia zgody przez Senat. Senat przed podjęciem uchwały może wezwać Generalnego Inspektora do złożenia wyjaśnień i

[869]Zob. S. Trociuk, *Ustawa o Rzeczniku Praw Obywatelskich*. *Komentarz*, Biuro Rzecznika Praw Obywatelskich, Warszawa 2005, s. 25-29.

odpowiedzi na pytania senatorów. Głosowanie w Senacie odbywa się na zasadach ogólnych obowiązujących przy podejmowaniu uchwał przez Senat, zwykłą większością głosów w obecności co najmniej połowy ustawowej liczby członków Senatu, tak samo jako w przypadku powołania kandydata na stanowisko GIODO. Uchwałę Senatu w sprawie odwołania Generalnego Inspektora z pełnionej funkcji Marszałek Senatu przekazuje Marszałkowi Sejmu.

5. Aparat pomocniczy GIODO

Już sama konstrukcja urzędu GIODO wskazuje, iż jest to organ jednoosobowy, a wszystkie kompetencje przyznane zostały jednej osobie i na jej odpowiedzialność. U.o.d.o. przewiduje jednak, że Generalny Inspektor na mocy art. 12 a u.o.d.o. może posiadać zastępcę, a zgodnie z art. 13 ust. 1 wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. Aparat pomocniczy GIODO to urząd, czyli struktura organizacyjna i majątkowa oraz zespół ludzi wyodrębniony do realizacji zadań tego organu. Jego istnienie ma zapewnić wykonanie zadań wynikających z kompetencji Generalnego Inspektora określonych w u.o.d.o., a także w innych przepisach powszechnie obowiązującego prawa.

W pierwotnej wersji u.o.d.o. nie przewidywała możliwości powołania zastępcy GIODO, jednak stało się to konieczne w obliczu potencjalnych problemów mogących zaistnieć w zakresie kierowania pracami Biura GIODO w sytuacji chociażby urlopu czy czasowej niezdolności do pracy Generalnego Inspektora. Na mocy art. 1 pkt 5 ustawy z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe[870] stworzono stanowisko zastępcy GIODO[871].

Zastępca GIODO jest mianowany przez Marszałka Sejmu na wniosek Generalnego Inspektora; jego odwołanie również następuje w tym samym trybie. Zasady powoływania i odwoływania zastępcy GIODO oraz określenie zakresu jego zadań wzorowane jest na rozwiązaniach prawnych zastosowanych w stosunku do zastępców Rzecznika Praw

---

[870] Dz. U. Nr 33, poz. 285.

[871] W projekcie nowelizacji przewidziano możliwość powołania dwóch zastępców Generalnego Inspektora, jednak Senat wprowadził zmianę w tym zakresie, kierując się koniecznością dokonywania oszczędności w budżecie państwa. Zob. uzasadnienie uchwały Senatu RP z dnia 9 stycznia 2004 r. w sprawie ustawy o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe, druk sejmowy nr 2406 z dnia 9 stycznia 2004 r.

Obywatelskich. Wymogi względem zastępcy Generalnego Inspektora są zbliżone do tych, które ustawa przewiduje względem Generalnego Inspektora. Różnica pojawia się w zakresie wymogu posiadania wyższego wykształcenia, gdyż ustawa nie wskazuje, iż chodzi o wykształcenie prawnicze, co można interpretować jako wymóg posiadania dowolnego wykształcenia wyższego i posiadania odpowiedniego doświadczenia zawodowego (art. 12a ust. 3 u.o.d.o.).

Do zastępcy Generalnego Inspektora nie mają także zastosowania zakazy wynikające z *incompatibilitas*, ani nie przysługuje mu immunitet. Ustawodawca odniósł immunitet tylko do samego GIODO, a to głównie z uwagi na niechęć do rozciągania tych immunitetów na zastępców. Takie samo rozwiązanie zostało zastosowane w przypadku zastępców RPO i odnosząc się po raz kolejny do analogicznych rozwiązań zastosowanych także w stosunku do Rzecznika, postulowano, by ustawodawca objął zastępców RPO pewną odmianą immunitetu („immunitet rzeczniowski"). Rozwiązanie to byłoby zatem równie adekwatne w przypadku zastępcy Generalnego Inspektora, który mógłby zostać wyposażony w immunitet, ograniczony wprawdzie materialnie, ale stworzony np. na wzór immunitetu kontrolerskiego, przyznanego w trybie ustawowym merytorycznym pracownikom NIK[872].

Należy zaznaczyć również zasadniczy fakt, iż organem państwowym jest tylko Generalny Inspektor, a status ten nie przynależy ani jego zastępcy ani pracownikom Biura Generalnego Inspektora Ochrony Danych Osobowych[873]. Zastępca bowiem nie wykonuje żadnym własnych, indywidualnych funkcji. Zastępuje jedynie GIODO i z tego wypływają jego uprawnienia. Stosownie do wytycznych art. 12a ust. 2 u.o.d.o. to Generalny Inspektor określa zadania swojego zastępcy. Zgodnie z założeniami utworzenia tego stanowiska, to właśnie zastępca ma przejąć część obowiązków Generalnego Inspektora[874].

Aby Generalny Inspektor Ochrony Danych Osobowych mógł wykonywać powierzone mu zadania, ustawodawca przewidział utworzenie profesjonalnego urzędniczego aparatu obsługującego Generalnego Inspektora (art. 13 u.o.d.o.). Biuro Generalnego Inspektora Ochrony Danych Osobowych posiada status jednostki pomocniczej, tj. jednostki przydatnej Generalnemu Inspektorowi do pomocy w wykonywaniu jego funkcji, zapewniającej merytoryczną i techniczną obsługę jego działalności, jednak jest całkowicie pozbawione

---

[872] Immunitet kontrolerski przyznawany jest w trybie art. 88 ust. 1 ustawy z 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. Nr 13, poz. 59) wszystkim, nie wyłączając prezesa, merytorycznym pracownikom NIK. Zob. W. Sokolewicz, *Artykuł 206…*, s. 1; W. Sokolewicz, *Artykuł 211,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom III, red. L. Garlicki, s. 2.

[873] M. Sakowska, *Pozycja…,* s. 87.

[874] Zob. uzasadnienie projektu ustawy o zmianie ustawy o ochronie danych osobowych, druk sejmowy nr 2120 z dnia 16 października 2003 r.

jakiejkolwiek samoistności prawnej i ustrojowej. Biuro zapewnia wykonywanie zadań wynikających z kompetencji Generalnego Inspektora, określonych w ustawie i innych przepisach prawa, a zakres wykonywanych przez Biuro zadań wyznaczają środki finansowe przewidziane w ustawie budżetowej[875].

Tworząc jednostkę organizacyjną („jednostkę pomocniczą"), polski ustawodawca poszedł w odmiennym kierunku niż przyjęty w wielu państwach model, w którym pomoc w działaniu organu ochrony danych osobowych zapewnia stosowny urząd państwowy[876]. Celem takiego rozwiązania jest zagwarantowanie - również w aspekcie organizacyjnym - niezależności Generalnego Inspektora, a także ułatwienie jemu podejmowania działań bezpośrednio po wyborze, co zwalnia go z konieczności zajmowania się sprawami organizacyjnymi[877].

Struktura organizacyjna i organizacja pracy Biura została określona w statucie stanowiącym załącznik do rozporządzenia Prezydenta RP z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych[878]. W obliczu powoływania GIODO przez Sejm oraz dość silnej relacji Generalnego Inspektora z parlamentem, kompetencja Prezydenta w stosunku do określenia szczegółowego trybu wewnętrznej organizacji Biura GIODO może zastanawiać. Na mocy wyraźnego upoważnienia zawartego w ustawie Prezydent RP, po zasięgnięciu opinii Generalnego Inspektora, w drodze rozporządzenia, nadaje statut Biuru, określając jego organizację, zasady działania oraz siedziby jednostek zamiejscowych i zakres ich właściwości terytorialnej, mając na uwadze stworzenie optymalnych warunków organizacyjnych do prawidłowej realizacji zadań Biura (art. 13 ust. 3 u.o.d.o.).

Zgodnie z treścią statutu tryb pracy Biura Generalnego Inspektora, organizację wewnętrzną i szczegółowy zakres zadań statutowych jednostek organizacyjnych Biura określił GIODO w regulaminie organizacyjnym Biura Generalnego Inspektora Ochrony Danych Osobowych, stanowiącym załącznik do zarządzenia nr 29/2007 Generalnego Inspektora Ochrony Danych Osobowych[879].

---

[875] § 2 regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych stanowiący znacznik do zarządzenia nr 1/2012 Generalnego Inspektora ochrony Danych Osobowych, dostępny na stronie: http://www.giodo.gov.pl/548/j/pl/.

[876] Tak jest np. w Niemczech, gdzie obsługę inspektora zapewnia resort spraw wewnętrznych. Zob. G. Sibiga, *Postępowanie…*, s. 122.

[877] E. Kulesza, *Pozycja…,* s. 23.

[878] Dz. U. Nr 225, poz. 1350.

[879] Regulamin dostępny jest na stronie internetowej: http://www.giodo.gov.pl.

Siedziba Biura GIODO mieści się w Warszawie. Zgodnie z art. 13 a ust. 1a ustawy o ochronie danych osobowych, w przypadkach uzasadnionych liczbą i charakterem spraw z zakresu ochrony danych osobowych na danym terenie, Generalny Inspektor może wykonywać swoje zadania przy pomocy jednostek zamiejscowych Biura. W § 4 ust. 1 statutu Biura GIODO ustalona została siedziba oraz właściwość miejscowa dwóch jednostek zamiejscowych Biura, tj. Jednostki Zamiejscowej Biura Ochrony Danych Osobowych w Katowicach, obejmującej swoim zasięgiem obszar województw: śląskiego, opolskiego, dolnośląskiego, małopolskiego i podkarpackiego oraz Jednostki Zamiejscowej Biura Ochrony Danych Osobowych w Gdańsku, obejmującej swoim zasięgiem obszar województw: pomorskiego, warmińsko-mazurskiego, zachodniopomorskiego. Jednostkami zamiejscowymi kierują dyrektorzy tych jednostek.

Generalny Inspektor kieruje Biurem przy pomocy Dyrektora Biura, sam zaś sprawuje nadzór nad pracą Biura. Przysługują mu również uprawnienia pracodawcy wobec pracowników Biura. Dyrektor kieruje Biurem przy pomocy dyrektorów departamentów oraz kierowników innych jednostek organizacyjnych zgodnie z zarządzeniami, decyzjami, wytycznymi i poleceniami Generalnego Inspektora. Kompetencje osoby zastępującej dyrektora biura określa Generalny Inspektor lub jego zastępca. Dyrektor Biura odpowiada za funkcjonowanie urzędu, warunki jego działania oraz organizację pracy, a także reprezentuje Biuro na zewnątrz.

Do obowiązków dyrektora Biura należy: sprawowanie bezpośredniego nadzoru nad jednostkami organizacyjnymi Biura, zatwierdzanie dokumentów określających struktury wewnętrzne poszczególnych jednostek organizacyjnych, przedkładanych przez dyrektorów tych jednostek, przedkładanie Generalnemu Inspektorowi wniosków w zakresie ilości etatów w Biurze i ich podziału pomiędzy jednostki organizacyjne Biura oraz wniosków personalnych dotyczących stanowisk dyrektorów departamentów, rozpatrywanie skarg na pracowników Biura, zapewnienie przestrzegania przepisów o tajemnicy państwowej i służbowej, przedkładanie Generalnemu Inspektorowi projektów zarządzeń, decyzji, postanowień i zaświadczeń, zlecanie ekspertyz i opinii prawnych, nadzorowanie gospodarowaniem mienia Biura, dokonywania zamówień publicznych przez Biuro, a także nadzorowanie sporządzania projektu i wykonania budżetu Biura i przyjmowanie oświadczeń majątkowych. Dyrektor Biura GIODO jest uprawniony do wydawania w imieniu GIODO decyzji administracyjnych[880].

[880] Wyrok NSA w Warszawie z dnia 12 maja 2000 r., II SA 52/00, niepublikowany.

Dyrektor Biura z upoważnienia Generalnego Inspektora podpisuje również decyzje, postanowienia i zaświadczenia oraz zaciąga zobowiązania finansowe, w granicach przyznanych środków oraz na zasadach i w trybie określonym w zarządzeniach GIODO i w przepisach prawa. Dyrektor Biura wykonuje również inne zadania zlecone przez Generalnego Inspektora oraz składa stałe informacje dla Generalnego Inspektora o pracy Biura i realizacji jego zadań. Obsługę Dyrektora Biura tworzą sekretariat i radcy prawni podlegli bezpośrednio Dyrektorowi Biura (§ 6 regulaminu Biura GIODO).

Zgodnie z § 3 ust. 1 statutu jednostkami organizacyjnymi Biura GIODO są: 1) Departament Organizacyjno-Administracyjny; 2) Departament Orzecznictwa, Legislacji i Skarg; 3) Departament Edukacji Społecznej i Współpracy Międzynarodowej; 4) Departament Inspekcji; 5) Departament Rejestracji Zbiorów Danych Osobowych; 6) Departament Informatyki; 7) Zespół do Spraw Egzekucji Administracyjnej; 8) Dział Finansowy; 9) Samodzielne stanowisko do Spraw Ochrony Informacji Niejawnych; 10) Samodzielne stanowisko do Spraw Pracowniczych; 11) Samodzielne stanowisko do Spraw Audytu Wewnętrznego; 12) Zespół Rzecznika Prasowego.

Ze względu na wykonywane zadania w strukturze Biura GIODO można wyróżnić departamenty merytoryczne oraz inne komórki zajmujące się obsługą Biura oraz wykonywaniem prawnych obowiązków związanych z funkcjonowaniem urzędu (np. ochroną zgromadzonych informacji niejawnych)[881]. Departamenty merytoryczne zapewniają realizację ustawowych kompetencji GIOD; należą do nich komórki organizacyjne wymienione w punktach 2-7, a podstawą ich wyodrębnienia są zadania przydzielone Generalnemu Inspektorowi do realizacji na mocy ustawy w art. 12 u.o.d.o. Szczegółowe zadania tych departamentów określa regulamin, a departamenty wykonują ponadto zadania przydzielone im przez Generalnego Inspektora oraz zastępcę Generalnego Inspektora lub dyrektora departamentu. Każdy z departamentów zgodnie z wytycznymi § 14 regulaminu opracowuje projekty zarządzeń, decyzji, postanowień i zaświadczeń Generalnego Inspektora czy projekty pism przedkładanych do podpisu Generalnemu inspektorowi, jego zastępcy czy dyrektorowi departamentu, a w miarę potrzeby uzgadnia także projekty zarządzeń, decyzji czy postanowień z innymi departamentami.

Część II regulaminu Biura GIODO szczegółowo określa zakres działania i zadania wykonywane przez poszczególne jednostki organizacyjne.

---

[881] G. Sibiga, *Postępowanie…*, s. 122.

Departament Organizacyjno-Administracyjny (DOA), zgodnie z § 18 regulaminu Biura GIODO, ma zapewnić w szczególności obsługę organizacyjną Biura GIODO i prowadzić sprawy związane z administrowaniem Biura, przygotowywać i prowadzić postępowania w zakresie zamówień publicznych oraz wykonywać realizację budżetu zgodnie z planem rzeczowym we współpracy z Departamentem Finansowym, jak też zapewniać techniczną obsługę podróży służbowych oraz delegacji krajowych i zagranicznych.

Dział Finansowy ma obowiązek realizować wszelkie zadania wyznaczone w § 25 regulaminu, które związane są z prowadzeniem spraw finansowych, rachunkowych i dotyczą budżetu urzędu.

Do zadań osoby zajmującej Samodzielne Stanowisko do Spraw Ochrony Informacji Niejawnych (SOIN) należy, zgodnie z § 26 regulaminu, zapewnienie przestrzegania przepisów o ochronie informacji niejawnych - stosownie do ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[882].

Z kolei osoba piastująca Samodzielne Stanowisko do Spraw Pracowniczych (SP) zajmuje się w szczególności prowadzeniem spraw pracowniczych związanych z zatrudnieniem oraz przebiegiem stosunku pracy pracowników Biura GIODO (§ 27 regulaminu Biura GIODO).

Natomiast osoba zatrudniona na Samodzielnym Stanowisku do Spraw Audytu Wewnętrznego (SAW) wykonuje zadania określone w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych oraz przepisach wydanych na jej podstawie (§ 28 regulaminu Biura GIODO).

Ostatnią jednostką organizacyjną Biura GIODO jest Zespół Rzecznika Prasowego (ZP), którego główne działanie związane są z utrzymywaniem kontaktu z mediami, organizacją konferencji krajowych i zagranicznych, redagowaniem strony internetowej generalnego Inspektora Ochrony Danych Osobowych, a także inne czynności mające na celu popularyzowanie wiedzy z zakresu ochrony danych osobowych za pośrednictwem mediów (§ 29 regulaminu Biura GIODO).

W skład komórek merytorycznych wchodzi w pierwszej kolejności Departament Orzecznictwa, Legislacji i Skarg (DOLiS). Jest to departament, który ma szereg zadań *stricte* związanych z realizacją uprawnień GIODO, o których mowa w art. 12 u.o.d.o. Zgodnie z treścią § 19 regulaminu, departament ten m.in. prowadzi postępowania administracyjne w sprawach wykonania przepisów o ochronie danych osobowych, opiniuje projekty ustaw i

[882] Dz. U. Nr 182, poz. 1228 z póz. zm.

rozporządzeń dotyczących ochrony danych osobowych, przygotowuje projekty wystąpień Generalnego Inspektora do podmiotów z sektora publicznego i prywatnego dotyczących problematyki przestrzegania przepisów o ochronie danych osobowych, sporządza opinie na potrzeby Generalnego Inspektora, zastępcy czy kierowników jednostek organizacyjnych Biura, przygotowuje stanowiska doktryny i orzecznictwa Sądu Najwyższego, sądów powszechnych i administracyjnych, Trybunału Konstytucyjnego w sprawach ochrony danych osobowych, bierze udział w pracach komisji i podkomisji rządowych, sejmowych i senackich w związku z rozpatrywaniem przez te organy projektów aktów prawnych dotyczących ochrony danych osobowych, przyjmuje i rozpatruje skarg i wnioski dotyczące wykonania ustawy o ochronie danych osobowych czy dotyczące funkcjonowania i organizacji pracy Biura GIODO.

Departament Edukacji Społecznej i Współpracy Międzynarodowej (DESiWM) powstał wraz z wprowadzeniem nowego statutu Biura GIODO. Departament ten ma za zadanie: popularyzację wiedzy z zakresu ochrony danych osobowych, opracowywanie projektów edukacyjnych dla różnych grup docelowych, organizację i realizację działań edukacyjnych, w tym szkoleń, konferencji i seminariów, utrzymywanie kontaktów z organami administracji rządowej i pozarządowymi organizacjami oraz innymi instytucjami w celu wymiany doświadczeń w zakresie ochrony danych osobowych i prawa do prywatności, organizację w kooperacji z innymi departamentami współpracy międzynarodowej Generalnego Inspektora, a także wydawanie materiałów i publikacji popularyzujących zagadnienia ochrony danych osobowych. Powstanie DESiWM jest - jak się wydaje - wynikiem planowanego przez Generalnego Inspektora zwiększenia roli edukacyjnej organu, która ma doprowadzić do zwiększenia świadomości społeczeństwa w zakresie danych osobowych[883].

Departament Inspekcji (DIS) w szczególności wykonuje z upoważnienia Generalnego Inspektora kontrole zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych oraz wszystkie czynności kontrolne i pokontrolne jak: sporządzanie protokołów z przeprowadzonych kontroli, opracowywanie projektów decyzji, postanowień i innych pism Generalnego Inspektora wydawanych w wyniku przeprowadzonych kontroli, wnioskowanie na podstawie ustaleń kontroli o wszczęcie stosownych postępowań przeciwko osobom odpowiedzialnym za zaistniałe nieprawidłowości, przygotowanie projektów zawiadomień o popełnieniu przestępstwa oraz wniosków o

[883] *GIODO potrzebuje więcej*, „Gazeta Prawna" z 29 stycznia 2007 r., nr 20 (1890), s. 16.

wszczęcie postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania. Ponadto, departament ten wszczyna i prowadzi w imieniu GIODO postępowania administracyjne na skutek stwierdzonych w toku kontroli uchybień oraz w razie stwierdzenia niewykonania decyzji GIODO, kieruje do zobowiązanych pisemne upomnienia oraz kieruje do egzekutora wnioski o wszczęcie postępowania egzekucyjnego.

Departament Rejestracji Zbiorów Danych Osobowych (DRZDO) został stworzony, stosownie do ustawowego obowiązku zawartego w art. 40 u.o.d.o. dotyczącego notyfikacji zbiorów danych osobowych. Jednostka ta na podstawie § 22 regulaminu przyjmuje i rozpatruje zgłoszenia zbiorów danych do rejestracji, wykonuje wszelkie czynności w zakresie prowadzenia ogólnokrajowego, jawnego rejestru zbiorów danych osobowych oraz wykonuje zadania związane z udzielaniem informacji o zarejestrowanych zbiorach.

Do zadań Departamentu Informatyki (DIF) należy współdziałanie z innymi jednostkami Biura w zakresie analizy potrzeb informatycznych, zwłaszcza co do zapotrzebowania na określony sprzęt informatyczny czy oprogramowanie, udzielanie bieżącej pomocy informatycznej i serwisu sprzętu informatycznego, nadzoru eksploatacyjnego oraz administrowanie infrastrukturą informatyczną systemów informatycznych. Departament ten zajmuje się także realizacją zadań związanych z bezpieczeństwem systemów informatycznych Biura i wykonuje z upoważnienia Generalnego Inspektora czynności kontrolne wraz z pracownikami Departamentu Inspekcji.

Ostatnią jednostką merytoryczną Biura Generalnego Inspektora jest Zespół do Spraw Egzekucji Administracyjnej (ZEA). Departament ten powstał wraz z rozszerzeniem uprawnień Generalnego Inspektora o czynności egzekucyjne[884]. Spełnia wszelkie zadania związane z wszczynaniem i prowadzeniem postępowań egzekucyjnych obowiązków o charakterze niepieniężnym, a także wykonuje zadania związane z wszczynaniem i monitorowaniem postępowań egzekucyjnych obowiązków o charakterze pieniężnym i współpracuje w tym zakresie z naczelnikami urzędów skarbowych (§ 24 regulaminu).

[884] Nowelizacja ustawy o ochronie danych wprowadziła do wykazu zadań GIODO, zawartego w art. 12 u.o.d.o. nowe zadanie polegające na zapewnieniu wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z wydanych przez ten organ decyzji w sprawach ochrony danych osobowych. Zadanie to GIODO ma realizować stosując środki egzekucyjne określone w ustawie z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.). GIODO uzyskało zatem kompetencje do prowadzenia postępowania egzekucyjnego w przedmiotowych sprawach. Zob. P. Przybysz, *Kompetencje egzekucyjne Generalnego Inspektora Ochrony Danych Osobowych oraz postępowanie egzekucyjne prowadzone przez organ ochrony danych osobowych*, „Monitor Prawniczy" 2011, nr 3, s. 30-34.

Strukturę organizacyjną każdej komórki Biura GIODO tworzy: dyrektor departamentu, zastępca dyrektora departamentu, pracownicy departamentu oraz sekretariat departamentu podlegający bezpośrednio dyrektorowi departamentu.

Statutowymi jednostkami organizacyjnymi Biura GIODO kierują dyrektorzy tych jednostek, z wyjątkiem Działu Finansowego, którym kieruje Główny Księgowy, Samodzielnego Stanowiska do Spraw Ochrony Informacji Niejawnych, Samodzielnego Stanowiska do Spraw Pomocniczych oraz Samodzielnego Stanowiska do Spraw Audytu Wewnętrznego. Dyrektor departamentu kieruje podległym mu departamentem i odpowiada za wykonanie zadań określonych w regulaminie i zadań ustalonych przez Generalnego Inspektora lub jego zastępcę.

Wykonywanie czynności urzędowych wymaga zachowania drogi służbowej. Wszelkie pisma kierowane do Generalnego Inspektora wpływają do Kancelarii Ogólnej, zgodnie z Instrukcją Kancelaryjną Biura GIODO, a wszelkie dokumenty przygotowane na polecenie Generalnego Inspektora oraz jego zastępcy wymagają parafy dyrektora departamentu, w którym je sporządzono.

Zasady wykonywania czynności kancelaryjnych oraz tryb postępowania z dokumentami w jednostkach organizacyjnych Biura określa Instrukcja Kancelaryjna oraz inne akty wewnętrzne.

Poza ogólnymi aspektami organizacyjnymi, które są zawarte w ustawie oraz w statucie, brak jest szczegółowych regulacji, co do zasadniczych kwestii związanych z funkcjonowaniem Biura GIODO.

W skład Biura wchodzą upoważnieni przez Generalnego Inspektora pracownicy zwani, na mocy art. 14 u.o.d.o.[885], „inspektorami". Status pracowników-inspektorów, którzy są zatrudnieni w Biurze Generalnego Inspektora, regulowały pierwotnie przepisy o pracownikach urzędów państwowych, a ustawa o ochronie danych osobowych czyniła swoiste odesłanie do ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych[886]. Zgodnie z art. 48 wskazanej ustawy wszystkie kwestie związane ze statusem urzędników i organizacją urzędów powinny być regulowane przez Marszałka Sejmu w drodze zarządzenia. Tu jednak dochodzi do kolizji przepisów, gdyż na mocy art. 87 źródłami powszechnie obowiązującego prawa w RP są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe i rozporządzenia. W tym zamkniętym katalogu nie zostały zawarte

[885] Treść art. 14 u.o.d.o. została doprecyzowana w skutek nowelizacji ustawy z dnia 22 stycznia 2004 r.
[886] Dz. U. Nr 31, poz. 214, z późn. zm.

zarządzenia Marszałka Sejmu, zatem nie mogły one stanowić podstawy uprawnień i obowiązków pracowników urzędów państwowych[887]. Wraz jednak z wejściem w życie ustawy z dnia 21 listopada 2008 r. o służbie cywilnej[888], zmieniła się sytuacja prawna pracowników urzędów państwowych, w tym inspektorów Biura GIODO. Pracownicy Biura GIODO stanowią korpus służby cywilnej, stąd podlegają przepisom ustawy o służbie cywilnej.

Osoby zatrudnione na stanowiskach inspektorów nie posiadają własnych kompetencji, a działają wyłącznie z upoważnienia Generalnego Inspektora[889]. Posiadają od niego pisemne upoważnienie do wykonywania w jego imieniu czynności kontrolnych. Upoważnienie może mieć charakter jednorazowy, jako upoważnienie do wykonania czynności określonej w jego treści, lub stałe do wykonywania czynności, w określonym czasie, nie dłuższym jednak niż do końca kadencji Generalnego Inspektora.

Inspektorom nie przysługuje karnoprawna ochrona w zakresie wykonywania czynności kontrolnych zbliżona do przyznanej inspektorom pracy czy inspektorom ochrony środowiska[890]. Utrudnianie inspektorom czynności kontrolnych nie stanowi także wykroczenia. Na podstawie przepisów kodeksu karnego korzystają oni jednak z ochrony przysługującej funkcjonariuszom publicznym[891].

Zgodnie z § 3 ust. 3 statutu w Biurze Generalnego Inspektora może działać Rada Naukowa i Komisje Ekspertów**,** których skład określa Generalny Inspektor. Szczegółowe zasady działania Rady Naukowej określa III część Regulaminu Organizacyjnego Biura Generalnego Inspektora „Rada Naukowa i Komisje Ekspertów" (wprowadzona zarządzeniem nr 3/2012 Generalnego Inspektora Ochrony Danych Osobowych z dnia 18 lutego 2013 r. w sprawie zmiany Regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych[892]).

Rada Naukowa składa się z 10 do 15 członków. Członków Rady Naukowej powołuje Generalny Inspektor na okres swojej kadencji, spośród osób naukowo zajmujących się zagadnieniami objętymi działalnością Rady i wyróżniających się wiedzą w tym zakresie. Pracami rady kieruje jej przewodniczący. Generalny Inspektora powołuje też i odwołuje przewodniczącego i wiceprzewodniczącego Rady spośród jej członków.

---

[887] E. Kulesza, *Pozycja…,* s. 24.
[888] Dz. U. Nr 227, poz. 1505, z późn. zm.
[889] S. Sagan, *Prawo konstytucyjne Rzeczypospolitej Polskiej*, Warszawa 2001, s. 248.
[890] A. Drozd, *op. cit*., s. 103.
[891] *Ibidem*, s.103.
[892] Treść zarządzenia dostępna jest na stronie: http://www.giodo.gov.pl/1520187/j/pl/.

Do zadań Rady Naukowej należy w szczególności: zajmowanie stanowisk w sprawach przedstawionych przez Generalnego Inspektora biorąc pod uwagę dorobek i potrzeby nauki, analizowanie problemów ochrony danych osobowych i przedstawianie w tym zakresie Generalnemu Inspektorowi wyników swoich prac oraz inicjowanie działań na rzecz rozwoju ochrony danych osobowych, w tym prac naukowo-badawczych i wydawniczych[893]. Rada działa poprzez obrady na posiedzeniach, wymianę informacji lub pracę z wykorzystaniem systemów teleinformatycznych.

Zgodnie z § 31 Regulaminu Organizacyjnego Generalny Inspektor może powołać także Komisję Ekspertów, określając przedmiot jej badań i skład osobowy, w tym przewodniczącego oraz termin przekazania prac. Generalny Inspektor może utworzyć również więcej niż jedną komisję. Komisje pełnią rolę organów pomocniczych i opiniodawczo-doradczych i stanowią niejako merytoryczne wsparcie dla Generalnego Inspektora. Ich rola jest szczególnie ważna zwłaszcza w zakresie spraw, które stanowią istotne tło dla procesów ochrony i przetwarzania danych, jak chociażby zagadnienia z zakresu informatyki czy nowoczesnych technologii w kontekście ochrony prywatności jednostki[894].

---

[893] Na podstawie wspomnianych aktów w 2013 r. Generalny Inspektor powołał Radę Naukową, w skład której wchodzą: dr hab. P. Fajgielski, prof. KUL (Katolicki Uniwersytet Lubelski) – przewodniczący, dr G. Sibiga (Instytut Nauk Prawnych Polskiej Akademii Nauk) – wiceprzewodniczący, dr A. Mednis (Uniwersytet Warszawski), dr E. Perłakowska (Naczelna Dyrekcja Archiwów Państwowych), prof. dr hab. J. Stelina (Uniwersytet Gdański), prof. dr hab. G. Szpor (Uniwersytet Kardynała Stefana Wyszyńskiego), dr inż. J. Zawiła-Niedźwiecki (Politechnika Warszawska). Do śmierci (7 kwietnia 2013 r.) członkiem Rady Naukowej była prof. dr hab. T. Górzyńska z Instytutu Nauk Prawnych Polskiej Akademii Nauk. Źródło: http://www.giodo.gov.pl/1520187/j/pl/.

[894] Przykładem może być technologia RFID, wykorzystująca do komunikacji fale radiowe, która polega na zastosowaniu niewielkich mikroprocesorów komputerowych i anten wbudowanych w papierową lub plastikowa etykietę, zwana identyfikatorem produktu, skanowana za pomocą elektronicznego czytnika. Zob. dokument Grupy Roboczej nr 105 z 19 stycznia 2005 r. - *„Working dokument on data protection issues related to RFID technology”*, dostępny na: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm.

ROZDZIAŁ V
USTAWOWE ZADANIA
GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

1. Uwagi ogólne

Każdy akt prawny normujący materię w społecznym odczuciu nie do końca znaną i wciąż uważaną za niezbyt ważną, stwarza poważne niebezpieczeństwo, że bez ustanowienia środków gwarantujących jej przestrzeganie będzie kolejnym aktem prawnym, do istnienia którego nie przywiąże się zbytniej wagi. Z tego względu powołanie instytucji Generalnego Inspektora Ochrony Danych Osobowych, wskazanie określonych ustawą zadań do realizacji i wyposażenie tego organu w szereg kompetencji i środków działania, stało się niewątpliwie realną gwarancją zapewnienia ochrony prywatności jednostki w Polsce.

Generalnemu Inspektorowi Ochrony Danych Osobowych na mocy u.o.d.o. powierzono zadania, jakich nie wykonywał wcześniej żaden inny organ. Zasadniczą funkcją Generalnego Inspektora jest ochrona prywatności człowieka, którą GIODO realizuje poprzez czuwanie nad przestrzeganiem i stosowaniem przepisów u.o.d.o. W treści art. 8 ust. 1 u.o.d.o bardzo ogólnie został wskazany zakres działania tego organu, jako organu do spraw ochrony danych osobowych, a dopiero w art. 12 u.o.d.o[895]. enumeratywnie zostały wymienione jego zadania. Przedstawiony katalog nie jest zamknięty i znacznie wykracza poza standardowe uprawnienia przysługujące takiemu organowi na mocy dyrektywy 95/46/WE. Wymienione w ustawie jako podstawowe zadania Generalnego Inspektora wskazują, iż GIODO pełniąc rolę organu do spraw ochrony prywatności jednostki, w tym ochrony jej danych osobowych, w pewnym sensie także spełnia rolę rzecznika interesów poszczególnych osób oraz określonych interesów publicznych, a także wykonuje zadania jako organ rejestrowy i inspekcyjny. Jakiekolwiek jednak nie byłyby realizowane zadania przez Generalnego Inspektora, nie może to prowadzić do ingerowania w określone ustawowo kompetencje innych organów i prowadzone przez nie postępowania[896].

---

[895] Polski ustawodawca przyjął licencyjny model ochrony, zgodnie z którym przetwarzanie danych osobowych pozostaje pod nadzorem specjalnego organu. W literaturze wyróżnia się również akrobacyjny model ochrony danych osobowych, według którego przetwarzanie danych osobowych oparte jest na zgodzie osoby, której dane dotyczą. Zob. P. Bogdalski, *Ochrona Danych Osobowych w działalności Generalnego Inspektora Ochrony Danych Osobowych*, [w:] *Ochrona człowieka w świetle prawa Rzeczypospolitej Polskiej. Materiały II Międzynarodowej Konferencji Naukowej Mierki 18-19 października 2001*, red. S. Pikulski, Olsztyn 2002, s. 455.

[896] Zob. wyrok NSA w Warszawie z dnia 13 kwietnia 2007 r., II SA/Wa 2079/06, niepublikowany.

Art. 12 ustawy jest przepisem szczególnym, wyznaczającym właściwość rzeczową GIODO. Przyznaje Generalnemu Inspektorowi prawo rozpoznawania spraw w nim wymienionych, ale zarazem nakłada na ten organ obowiązek ich rozpoznania[897]. J. Barta, P. Fajgielski, R. Markiewicz trafnie wskazują, iż „niezależnie od wyliczenia podstawowych obowiązków, jakie znalazły się w art. 12 u.o.d.o., Generalny Inspektor […] ma do spełnienia bardzo ważną rolę także, jeśli chodzi o samo wdrożenie w życie rozwiązań ustawy, rozpoznanie istniejącej sytuacji faktycznej, kształtowanie polityki ochrony danych osobowych i wykładni odpowiednich, służących temu, postanowień, a także podniesienie świadomości prawnej w tym zakresie"[898].

W treści art. 12 u.o.d.o. zostało wskazane, iż GIODO zostały powierzone określone zadania, poprzez wprost użycie sformułowania „zadania" w treści artykułu. Z punktu widzenia niniejszej pracy należałoby zauważyć, iż GIODO realizując ustawowe zadania, dokonuje także pewnych czynności przy użyciu prawnie określonych środków, stąd w moim przekonaniu słuszne jest dla precyzyjnego określenia zakresu działań tego organu wyodrębnienie z przedstawionych w art. 12 u.o.d.o. *stricte* zadań tego organu oraz środków działania GIODO.

Środki działania GIODO stanowią uregulowane przez prawo działania władzy tego organu i zostaną szczegółowo omówione w rozdziale szóstym pracy.

Zadania zaś są pewnego rodzaju obowiązkiem, które GIODO musi spełnić zgodnie z założeniami ustawodawcy[899]. Zadania stanowią cel, który GIODO ma spełnić poprzez swoją ustawową działalność oraz kierunek działania, uwzględniający zakres spraw należących do właściwości tego organu.

Dokonując charakterystyki zadań organu często dla określenia statusu organu stosuje się także wymiennie określenie „kompetencje". W doktrynie przyjmuje się, iż „kompetencja" oznacza możność działania, pełnomocnictwo, upoważnienie, czy ogół praw i obowiązków[900]. Wskazuje się na trzy cechy, które odróżniają pojęcie zadań od kompetencji. Po pierwsze, kompetencje stanowią podstawę do wchodzenia w stosunki prawne, a zatem możliwość dokonywania czynności, które rodzą skutki prawne w postaci konkretnych obowiązków po stronie określonych podmiotów. Po drugie, pojęcie kompetencji zawiera w sobie element uprawnienia organu państwa do podejmowania konkretnych działań, ale i w pewnych

---

[897] Zob. wyrok WSA w Warszawie z dnia 13 czerwca 2006 r., II SA/Wa 2016/05, niepublikowany.
[898] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 431.
[899] K. Płonka-Bielenin, *Zakres pojęcia „zadania publiczne" i próba pokreślenia istoty ich realizacji przez organizacje pożytku publicznego*, „Administracja-Teoria-Dydaktyka-Praktyka" 2011, nr 2, s. 149.
[900] M. Matczak, *Kompetencje organu administracji publicznej*, Kraków 2004, s. 41-42.

sytuacjach normy prawne mogą zobowiązywać do korzystania z kompetencji (obowiązek). Po trzecie, kompetencje są jednym z elementów wykonywania zadań, co wskazuje na ich służebną rolę w stosunku do zadań[901]. W takim ujęciu zatem kompetencje to nie synonim zadań, a jedynie jeden z instrumentów wykonywania zadań, stanowiący konkretyzację celu.

Na tej podstawie, *stricte* do zadań GIODO, które zostały wskazane przez u.o.d.o. zaliczyć można: kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, prowadzenie rejestru zbiorów danych oraz udzielenie informacji o zarejestrowanych zbiorach, opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych, inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych oraz uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

2. Kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Do realizacji skutecznej ochrony prywatności i danych osobowych nie wystarczy tylko stworzenie odpowiednich praw osobom, których dane dotyczą ani obowiązków podmiotom przetwarzającym dane, potrzeba jeszcze zapewnić, by procesy przetwarzania danych i podmioty w tym uczestniczące zostały poddane kontroli, której celem ma być sprawdzenie, czy rzeczywiście normy w zakresie prawnej ochrony danych są realizowane w praktyce, czy tylko pozostają one statycznymi zapisami. Utworzenie i umożliwienie działania instytucji kontrolnych uznane zostało w literaturze przedmiotu, jak i w orzecznictwie, za jeden z podstawowych elementów szeroko ujmowanego prawa ochrony danych osobowych[902]. Potrzebę sprawowania kontroli wzmagają także coraz to nowe zagrożenia związane z procesami przetwarzania danych i nagminne naruszenia praw dysponentów danych i ich prywatności, dlatego właśnie kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych ma to wyeliminować lub chociaż ograniczyć. Kontrola służyć ma realizacji pewnych celów, w tym prewencyjnego wymiaru ochrony danych - jako sprawdzanie tego, jak przebiegają procesy przetwarzania danych i jakie są możliwości zapobiegania nieprawidłowościom. Powinna przyczyniać się do ciągłego ulepszania mechanizmów przetwarzania i ochrony danych poprzez wykrywanie zagrożeń i

[901] K. Płonka-Bielenin, *op. cit.*, s. 149.
[902] P. Fajgielski, *Kontrola…*, s. 50.

nieprawidłowości. Kontrola powinna spełniać także wymiar represyjny, gdyż w razie stwierdzenia uchybień może prowadzić do pociągnięcia osób winnych do odpowiedzialności.

Szeroko zakreślone działania kontrolne w zakresie zgodności przetwarzana danych osobowych z przepisami o ochronie danych osobowych na mocy art. 12 pkt 1 u.o.d.o. są niewątpliwie podstawowym zadaniem Generalnego Inspektora Danych Osobowych. Kontrola sprawowana przez GIODO jest określana mianem kontroli instytucjonalnej dla odróżnienia od innych rodzajów sprawowanej kontroli w zakresie przetwarzania danych. W literaturze przedmiotu kontrola dokonywana przez GIODO mieści się w zakresie kontroli administracji wykonywanej przez organy państwowe[903].

W doktrynie reprezentowane są różne modele kontroli, ale dla potrzeb niniejszej analizy kompetencji kontrolnych GIODO i biorąc pod uwagę kryterium podmiotu dokonującego kontroli, można wyróżnić: kontrolę indywidualną, kontrolę funkcjonalną kontrolę instytucjonalną oraz kontrolę uzupełniającą.

Kontrola indywidualna jest sprawowana przez osoby, których przetwarzane dane dotyczą, a więc przez podmiot danych. W ramach tej kontroli podmiotowi temu przysługują uprawnienia informacyjne, korekcyjne i szczególne, zatem na tej podstawie taki model kontroli jest przejawem realizacja prawa tej osoby do ochrony dotyczących jej danych osobowych, a osoba której dane dotyczą ponosi konsekwencje przetwarzania danych i reagowania na nieprawidłowości procesów pojawiające się w trakcie tych procesów[904].

Kontrola funkcjonalna jest sprawowana przez podmioty przetwarzające dane na bieżąco i w trakcie procesów przetwarzania danych osobowych, kiedy podejmowane są stosowne do tego decyzje. Ten rodzaj kontroli jest zwykle ściśle powiązany z pełnieniem funkcji kierowniczych lub wyodrębnionych funkcji kontrolnych: stąd nawet przyjęcie nazwy - kontrola funkcjonalna.

Kolejnym rodzajem kontroli jest kontrola uzupełniająca, realizowana przez podmioty takie jak: prokuratura, sądy powszechne, Trybunał Konstytucyjny czy Rzecznik Praw Obywatelskich. Jest to kontrola przeprowadzana przez specjalnie powołany w tym celu zespół lub osoby. Ma ustalony i formalnie istniejący tryb postępowania oraz jednolity dla wszystkich charakter[905]. Kontrola przetwarzania i ochrony danych osobowych nie jest jednak

---

[903] E. Ura, E. Ura, *Prawo administracyjne*, Warszawa 2009, s. 262-268.
[904] P. Fajgielski, *Kontrola…*, s. 59.
[905] B. Nowakowski, *Ochrona danych osobowych*, [w:] *System kontroli GIODO i ochrona informacji niejawnych. Praktyczne wskazówki ochrony i kontroli danych osobowych i informacji niejawnych,* red. A. Jędruszczak, B. Nowakowski, Warszawa 2011, s. 4.

podstawowym zadaniem podmiotów dokonujących kontrolę uzupełniającą, a jedynie konsekwencją szerokiego zakresu uprawnień kontrolnych w różnych dziedzinach[906].

Największe znaczenie spośród podmiotów dokonujących kontrolę przetwarzania i ochrony danych osobowych przypisuje się właśnie GIODO przeprowadzającemu ją jako wyspecjalizowana instytucja niezależna od rządu. Mianem wyspecjalizowanych organów kontroli państwowej i ochrony prawa określane są instytucje, których misją publiczną jest gromadzenie informacji dotyczących przestrzegania prawa, reagowanie w konkretnych przypadkach naruszenia prawa oraz sporządzanie analiz i ich przekazywanie właściwym organom władzy publicznej[907]. Z uwagi na to, że kontrola GIODO jest sprawowana przez podmiot powołany właśnie do realizacji uprawnień kontrolnych, z tego tytułu ten rodzaj kontroli można nazwać kontrolą instytucjonalną[908].

Uprawnienia kontrolne Generalnego Inspektora dotyczą sprawdzania zgodności działań nie tylko z przepisami u.o.d.o., ale i z przepisami innych aktów prawnych regulujących materię ochrony danych osobowych[909]. Użyte w ustawie sformułowanie „przepisy o ochronie danych osobowych" wskazuje, że Generalnemu Inspektorowi przysługują uprawnienia kontrolne do badania, czy przetwarzanie danych osobowych odbywa się zgodnie nie tylko z przepisami u.o.d.o., ale i wydanych do niej rozporządzeń wykonawczych i innych aktów prawnych (np. ustaw szczególnych) zawierających regulacje dotyczące ochrony danych osobowych[910]. Generalny Inspektor obejmuje kontrolą nie tylko przestrzeganie powszechnie obowiązujących przepisów o ochronie danych osobowych, lecz również przestrzeganie aktów o charakterze wewnętrznym, przejętych przez administratora danych, a dotyczących chociażby dokumentacji z zakresu bezpieczeństwa przetwarzania danych osobowych, tj. polityki bezpieczeństwa, instrukcji zarządzania systemem

---

[906] P. Fajgielski, *Kontrola…*, s. 62.

[907] G. Szpor, *Kontrola administracji*, [w:] *Prawo administracyjne*, red. Z. Cieślak, I. Lipowicz, Z. Niewiadomski, G. Szpor, Warszawa 2013, s. 282.

[908] Pojęcie „kontrola instytucjonalna" wykorzystywane jest często w dwojakim znaczeniu. Oprócz stanowiska, iż kontrola taka realizowana jest przez wyspecjalizowany organ kontroli (zob. A. Sylwestrzak, *Kontrola administracji publicznej w III Rzeczypospolitej Polskiej*, Gdańsk 2001, s. 8). Pojawia się też drugie rozumienie kontroli instytucjonalnej jako kontroli prawnej tzn. kontroli sprawowanej w formach przewidzianych w obowiązujących przepisach prawa (zob. J. Jagielski, *Kontrola administracji publicznej*, Warszawa 2012, s. 150). Bardziej trafne jest jednak określenie pierwsze, a używanie wskazanych określeń wymiennie może powodować niepotrzebne niezrozumienie.

[909] Zob. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024.).

[910] A. Krasuski, D. Skolimowska, *Dane osobowe w przedsiębiorstwie*, Warszawa 2007, s. 287.

informatycznym czy ustalonego przez administratora danych regulaminu udzielania informacji na podstawie art. 32 i art. 33 u.o.d.o.[911].

Realizowana przez Generalnego Inspektora funkcja kontrolna łączy się z możliwością władczego oddziaływania na podmioty kontrolowane, co polega w szczególności na wydawaniu decyzji administracyjnych nakazujących przywrócenie stanu zgodnego z prawem[912].

Zgodnie z wyrokiem NSA z 2 marca 2001 r. Generalny Inspektor Ochrony Danych Osobowych nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji lub w inny sposób określony odpowiednimi procedurami[913]. Na tej podstawie przedmiotem kontroli GIODO, zgodnie z art. 12 pkt 1 u.o.d.o., powinna być jedynie zgodność przetwarzania danych z przepisami o ochronie danych osobowych.

W zakresie ustalania uprawnień Generalnego Inspektora sprawowana przez niego kontrola traktowana jest w kategoriach funkcjonalnych i polega głównie (jak wskazuje definicja kontroli w zakresie funkcjonalnym) na sprawdzeniu stanu faktycznego oraz podejmowaniu czynności zmierzających do ustalenia faktycznego stanu rzeczy, połączonego z porównaniem stanu istniejącego z planowanym[914]. Kontrolę, do której sprawowania został ustawowo zobowiązany GIODO, można również określić jako ogół czynności zmierzających do ustalenia faktycznego stanu rzeczy, połączonego z porównaniem stanu istniejącego ze stanem planowanym[915]. Celem działań kontrolnych GIODO jest zbadanie istniejącego stanu rzeczy, zestawienie tego, co istnieje, z tym co być powinno, co przewidują odpowiednie wzorce czy normy postępowania, i sformułowanie na tej podstawie odpowiedniej oceny, w przypadku zaś rozbieżności między stanem faktycznym a stanem pożądanym - ustalenie przyczyn tych rozbieżności i sformułowanie zaleceń, mających na celu wskazanie sposobów usunięcia niepożądanych zjawisk ujawnionych przez kontrolę. Biorąc zatem pod uwagę funkcjonalny aspekt kontroli oraz potoczne znaczenie słowa „kontrola", można stwierdzić, że

---

[911] A. Drozd, *Ustawa…*, s. 95.
[912] B. Pilc, *Kontrola przestrzegania przepisów o ochronie danych osobowych po wprowadzeniu w OchrdanOsobU elementów treści protokołu kontroli*, „Dodatek do Monitora Prawniczego" 2011, nr 3, s. 42
[913] Wyrok NSA w Warszawie z dnia 2 marca 2001 r., II SA 401/00, LexPolonica nr 352750; „Wokanda" 2001, nr 9, s. 33.
[914] M. Jaroszyński, M. Zimmermann, W. Brzeziński, *Polskie prawo administracyjne. Część ogólna*, Warszawa 1956, s. 440.
[915] E. Iserzon, *Prawo administracyjne*, Warszawa 1968, s. 174.

kontrola jest funkcją, której istota tkwi w sprawdzaniu i ocenianiu określonej działalności[916]. Prawo tworzy instytucje kontroli, które mają uprawnienia do podejmowania działań kontrolnych wobec określonego kręgu podmiotów, a te podmioty zaś nie mogą się od kontroli uchylać.

Kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych prowadzona przez GIODO obejmuje przypadki przetwarzania danych osobowych w zbiorach danych, w zbiorach ewidencyjnych lub w celu utworzenia jednego z tych zbiorów, z wyjątkiem zbiorów danych sporządzonych doraźnie (tj. sporządzonych wyłącznie w celach technicznych, szkoleniowych lub w związku z dydaktyka w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych lub poddanych anonimizacji), oraz przetwarzania danych osobowych przez podmioty wskazane w art. 31a ust. 1 u.o.d.o.[917].

Wykonywanie uprawnień kontrolnych przez Generalnego Inspektora nie jest jednak możliwe w odniesieniu do zbiorów danych objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, zbiorów dotyczących osób należących do kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego, oraz zbiorów danych, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych prowadzonych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne (art. 43 ust. 2 u.o.d.o.). Wgląd do pozostałych zbiorów danych pochodzących z czynności operacyjno-rozpoznawczych przysługuje wyłącznie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej[918].

Kontroli GIODO zostały poddane wszystkie podmioty obowiązane stosować u.o.d.o., z wyjątkiem tych, które nie podlegają przepisom u.o.d.o., jak osoby fizyczne przetwarzające dane wyłącznie do celów domowych lub osobistych, a także podmioty mające siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujące środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych (art. 3a ust. 1 u.o.d.o.). Zakres podmiotowy uprawnień kontrolnych Generalnego Inspektora jest zatem bardzo szeroki. Kontroli są poddawane zarówno podmioty należące do sfery publicznej jak i prywatnej, dlatego że u.o.d.o. stosuje się także w zakresie postępowania kontrolnego do

[916] B. Nowakowski, *op. cit.*, s. 2.
[917] A. Drozd, *Ustawa…*, s. 95.
[918] T. Szewc, *Publicznoprawna…*, s. 90.

wszystkich podmiotów wymienionych w art. 3 u.o.d.o. Kontrola GIODO koncentruje się przede wszystkim na administratorach danych jako podmiotach, które na gruncie u.o.d.o. obciąża najwięcej obowiązków związanych z ochroną danych osobowych, ale poddane są jej również podmioty przetwarzające. Kontrola przetwarzania danych obejmuje zarówno administratorów danych podlegających obowiązkowi zgłoszenia zbioru do rejestracji, jak i administratorów, którzy z mocy u.o.d.o. są zwolnieni z obowiązku rejestracji[919]. Obowiązki związane z kontrolą ciążą nie tylko na administratorze danych, ale w trybie art. 31 u.o.d.o. także na podmiocie zajmującym się przetwarzaniem danych na podstawie umowy powierzenia (zleceniobiorca)[920].

Kontrola prowadzona przez GIODO w zakresie przetwarzania i ochrony danych osobowych, o której mowa w art. 12 pkt 1 u.o.d.o., może przybierać różne formy, tj. może być prowadzona z inicjatywy Generalnego Inspektora, ale także stanowić reakcję na wniesiony wniosek, uwagi lub zastrzeżenia. Kontrola z urzędu wykonywana jest z samej inicjatywy GIODO i stanowi konsekwencję obowiązku realizowania zadań kontrolnych nałożonych przez ustawę, w szczególności w toku postępowań rejestracyjnych prowadzonych przez Departament Rejestracji Zbiorów danych Osobowych oraz w toku rozpatrywania skarg przez Departament Legislacji, Orzecznictwa i Skarg Biura GIODO. Kontrola na wniosek pozostaje również w sferze wykonywania zadań kontrolnych GIODO, natomiast inspiracja do podjęcia i prowadzenia określonej kontroli pochodzi z zewnątrz i od innego podmiotu (np. Najwyższej Izby Kontroli, Państwowej Inspekcji Pracy, prokuratury, związków zawodowych, pracodawców, osoby fizycznej)[921].

Co więcej, kontrola prowadzona przez Generalnego Inspektora może przybierać formę kontroli kompleksowej, która dotyczy wszystkich zbiorów danych osobowych prowadzonych przez kontrolowany podmiot oraz obejmuje swoim zakresem wszystkie wymogi określone w przepisach o ochronie danych osobowych, mające zastosowanie w działalności danego podmiotu[922]. Generalny Inspektor może dokonywać także kontroli częściowej, która dotyczy poszczególnych zagadnień w procesie przetwarzania danych będących przedmiotem skargi (np. legalności pozyskiwania danych skarżącego), czy też problemów pojawiających się w toku postępowania rejestracyjnego (np. podstawy prawnej, zakresu danych, celu

---

[919] B. Pilc, *op. cit.*, s. 42.
[920] Gdy administrator danych sam nie przetwarza danych, a zleca na piśmie ich przetwarzanie innemu podmiotowi (zleceniobiorcy) w drodze umowy powierzenia zawartej na podstawie art. 31 u.o.d.o., wówczas kontroli podlega także zleceniobiorca.
[921] B. Pilc, *op. cit.*, s. 45.
[922] A. Krasuski, D. Skolimowska, *op. cit.*, s. 290.

przetwarzania - czyli zgodności informacji podanych w zgłoszeniu zbioru ze stanem faktycznym)[923].

Biorąc pod uwagę kryterium odnoszące się do trybu kontroli, kontrola w zakresie przetwarzania i ochrony danych osobowych może mieć charakter systematycznej, regularnej (periodycznej) kontroli, przeprowadzanej zgodnie z wcześniej ustalonym harmonogramem, jak i kontroli sporadycznej, incydentalnej (*ad hoc*)[924].

Z uwagi na przyjęty w polskim systemie prawnym model kontroli instytucjonalnej, kontrolę przetwarzania danych osobowych może wykonywać Generalny Inspektor, jego zastępca lub upoważnieni do tego inspektorzy wyposażeni w szerokie kompetencje do podejmowania określonych czynności kontrolnych (art. 14 u.o.d.o.o.). Uprawnienie do kontroli wynika bezpośrednio z przepisów u.o.d.o. Do środków kontrolnych, możliwych do użycia celem wykonywania uprawnień kontrolnych, ustawodawca zaliczył wstęp do pomieszczeń i przeprowadzenie niezbędnych działań lub czynności kontrolnych, żądanie złożenia pisemnych lub ustnych wyjaśnień oraz wzywanie i przesłuchiwanie osób w celu ustalenia stanu faktycznego, żądanie okazania dokumentów i danych mających bezpośredni związek z przedmiotem kontroli i sporządzania ich kopii, żądanie udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych oraz zlecenie sporządzenia ekspertyz i opinii (art. 14 u.o.d.o.). Uprawnienia kontrolne mogą być podejmowane wyłącznie w celu wykonania zadań określonych w art. 12 pkt 1 i 2 u.o.d.o., stąd są one wyłączone w stosunku do przetwarzania danych wymienionych w art. 43 ust. 2 u.o.d.o.[925]. Zakres zastosowania wskazanych uprawnień kontrolnych powinien być ustalany z uwzględnieniem art. 15 u.o.d.o., gdyż wskazanym w art. 14 u.o.d.o. uprawnieniom odpowiadają obowiązki istniejące po stronie kierownika kontrolowanej jednostki organizacyjnej oraz kontrolowanej osoby fizycznej będącej administratorem danych[926].

GIODO posiada zatem uprawnienia zarówno do kontroli warunków przetwarzania danych osobowych, jak i władczego nakazywania usunięcia nieprawidłowości wykazanych w toku kontroli, poprzez użycie tzw. środków pokontrolnych (w tym decyzji administracyjnych czy środków wskazanych w art. 17 u.o.d.o.). Środki te mają pośrednio charakter środków nadzoru i przysługują temu organowi w razie stwierdzenia w toku kontroli naruszenia wzorca

---

[923] B. Pilc, *op. cit.*, s. 45.
[924] P. Fajgielski, *Kontrola…*, s. 65.
[925] A. Drozd, *Ustawa…*, s. 101.
[926] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 415.

zgodności z prawem[927]. Wynikające z art. 12 pkt 1 u.o.d.o. uprawnienia Generalnego Inspektora obejmują więc kontrolę zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz po części nadzór.

W doktrynie spotyka się jednak stanowisko odmienne, według którego GIODO dokonuje tylko czynności kontrolnych bez możliwości władczej ingerencji względem podmiotu kontrolowanego[928]. Stąd Generalny Inspektor nie ponosi odpowiedzialności za niewłaściwe działania kontrolowanych podmiotów lub osób, gdyż nie sprawuje nadzoru, a jedynie je kontroluje. Przy ocenie kompetencji Generalnego Inspektora K. Wygoda posługuje się określeniem „nadzoru policyjnego", przez co rozumie zbliżony do nadzoru mechanizm działania, charakterystyczny dla państw typu policyjnego i działającego w sferze tzw. policji administracyjnej, który służy głównie ochronie życia, zdrowia, mienia, bezpieczeństwa czy porządku i spokoju publicznego[929]. W takim ujęciu zastosowanie owych kryteriów nie byłoby jednak adekwatne w odniesieniu do państwa demokratycznego, stąd wspomniany autor podnosi, iż „pozostać musimy przy stwierdzeniu, iż GIODO kontroluje podmioty przetwarzające dane osobowe ujęte w zbiory, a kontrola ta wykonywana jest w trybie «nadzoru» - z zastrzeżeniem, iż nie jest on typowy"[930].

W mojej ocenie Generalnego Inspektor Ochrony Danych Osobowych możemy uznać za specjalistyczny organ nadzorczy[931]. Poprzez nadzór rozumie się sprawdzanie i ocenianie (kontrolowanie) działalności (zachowań) danego podmiotu (organu, jednostki organizacyjnej czy podmiotu o innym charakterze prawnym, np. osoby prawnej) przez inny uprawniony podmiot (organ nadzorujący, jednostkę nadzorującą) z równoczesną możliwością władczego, wiążącego wkraczania w tę działalność w celu skorygowania jej w pożądanym, prawidłowym kierunku zgodnie z przyjętymi kryteriami oceny tej prawidłowości, jak np. legalność, celowość[932]. Cechą charakterystyczną nadzoru jest więc nie tylko możliwość sprawdzania i oceniania działalności podmiotu (nadzorowanego) przez inny podmiot (nadzorujący), lecz także prawo stosowania przez nadzorującego wiążącej ingerencji w działalność nadzorowanego[933]. W ten sposób kategoria nadzoru jawi się w stosunku do kontroli jako kategoria szersza, zawierająca w sobie działalność kontroli, ale ponadto dysponująca możliwością władczego wkraczania w działalność podmiotów nadzorowanych, w co

---

[927] T. A. J. Banyś, J. Łuczak, *op. cit.,* s. 173.
[928] B. Nowakowski, *op. cit.,* s. 2-4.
[929] K. Wygoda, *Ochrona…*, s. 414.
[930] *Ibidem,* s. 414.
[931] T. A. J. Banyś, J. Łuczak, *op. cit.,* s. 171.
[932] Odnośnie rozróżnienia nadzoru i kontroli patrz szerzej: J. Boć, *Prawo…*, s. 357-374.
[933] B. Nowakowski, *op. cit.,* s. 3-4.

niewątpliwie na mocy ustawy został wyposażony Generalny Inspektor. W ramach działań nadzorczych mieści się ponadto podejmowanie względem podmiotów nadzorowanych czynności o charakterze niewładczym, organizatorskim, opiekuńczym czy wspierającym, jak udzielanie pomocy, doradzanie, instruktarz. Zadania Generalnego Inspektora wskazane głównie w art. 12 pkt 5 i 6 jak najbardziej wpisują się w całokształt uprawnień o charakterze wspierającym *stricte* z zakresu ochrony danych osobowych, które GIODO realizuje w ramach swojej aktywnej działalności. W doktrynie proponuje się również, by uprawnienia kontrolno-nadzorcze GIODO zaklasyfikować do nadzoru, wskazując dodatkowo na podobieństwo do uprawnień inspekcji państwowych, które podobnie jak GIODO mają możliwość przeprowadzania kontroli przestrzegania zagwarantowanych ustawowo zasad i władczej ingerencji w przypadku stwierdzenia ich naruszenia, gdzie nie ma generalnie znaczenia status prawny czy przynależność do określonych struktur podmiotu naruszającego te zasady[934].

Konsekwencją przeprowadzanych przez GIODO kontroli, w przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych, oprócz prawa do wydawania decyzji administracyjnych może być też inne władcze wyeliminowanie nieprawidłowości[935]. Zgodnie z art. 17 ust. 2 u.o.d.o. istnieje możliwość na podstawie ustaleń kontroli pociągnięcia do odpowiedzialności osób winnych dopuszczenia tych uchybień poprzez żądanie wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia tych uchybień[936]. Ponadto, w przypadku naruszenia przepisów o ochronie danych osobowych w wyniku działania lub zaniechania konkretnej osoby, które spełniają jednocześnie znamiona przestępstwa określonego w u.o.d.o., Generalny Inspektor zawiadamia właściwe ograny ścigania, dołączając dowody dokumentujące podejrzenia (art. 19 u.o.d.o.)[937]. Można zatem wskazać, iż w ramach wykonywania zadań kontroli zgodności przetwarzania danych osobowych z przepisami prawa Generalny Inspektor korzysta z kompetencji na trzech płaszczyznach: administracyjnej (wydawanie decyzji administracyjnej), karnej (zawiadomienie organów ścigania o popełnieniu przestępstwa

[934] K. Wygoda, *Ochrona*…, s. 414; G. Sibiga, *Postępowanie…,* s. 120.
[935] M. Sakowska, *Pozycja…*, s. 89.
[936] GIODO może na podstawie wyników kontroli np. zażądać od pracodawcy wszczęcia postępowania dyscyplinarnego lub innego postępowania przewidzianego prawem przeciwko pracownikowi, który naruszył przepisy u.o.d.o.
[937] B. Konieczna, *Decyzje GIODO w sprawach ochrony danych osobowych*, [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009, s. 248.

przeciwko ochronie danych osobowych) i odpowiedzialności dyscyplinarnej (kierowanie do pracodawcy wniosków o wszczęcie postępowania w sprawach o ukaranie pracownika)[938].

Celem kontroli jest ustalenie stanu faktycznego w zakresie przestrzegania przez kontrolowany podmiot przepisów o ochronie danych osobowych oraz udokumentowanie dokonanych w trakcie kontroli ustaleń. Uczestnikami procesu kontroli są: organ kontrolny (tj. Generalny Inspektor Ochrony Danych Osobowych) oraz podmiot kontrolowany. Ustawa wskazuje prawa i obowiązki przysługujące uczestnikom, by zapewnić osiągnięcie celu kontroli.

Inspektor przeprowadzający kontrolę ma prawo wstępu do pomieszczenia, w którym zlokalizowany jest zbiór danych oraz do pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, w godzinach od 6 do 22 za okazaniem imiennego upoważnienia i legitymacji służbowej[939] (art. 14 pkt 1 u.o.d.o.). Imienne upoważnienie wydawane jest przez Generalnego Inspektora musi być opatrzone jego pieczęcią urzędową oraz podpisem i jest ważne jedynie przy równoczesnym okazaniu legitymacji służbowej. Taka sformalizowana procedura ma być gwarancją tego, że kontroli dokonuje właściwy inspektor Biura GIODO, rzeczywiście działający z upoważnienia Generalnego Inspektora za jego wiedzą i zgodą.

Inspektor nie może przekroczyć zakresu upoważnienia udzielonego mu przez Generalnego Inspektora. Jest zobowiązany do przestrzegania uprawnień, które przysługują kontrolowanemu podmiotowi, w szczególności ma obowiązek poinformować w jaki sposób kontrolowany podmiot może domagać się np. wniesienia uwag, zastrzeżeń, poprawek czy sprostowań do protokołu kontroli. Nie może przekroczyć zakresu przedmiotowego kontroli, a więc żądać dokumentów lub informacji niezwiązanych bezpośrednio z celem i zakresem kontroli. W swoim działaniu inspektor powinien wykazać się obiektywizmem, profesjonalizmem i zachować w tajemnicy wszelkie informacje uzyskane w toku kontroli i w związku z wykonywaniem obowiązków służbowych[940]. Kontrolowany ma natomiast obowiązek umożliwić inspektorowi sprawne i rzetelne przeprowadzenie kontroli i realizację uprawnień kontrolnych przewidzianych przez ustawę, w szczególności udostępnić na żądanie

---

[938] G. Sibiga, *Postępowanie…*, s. 121. Autor zaznacza, że wspomniane kompetencje mają charakter niezależny od siebie, a Generalny Inspektor nie ma wyboru pomiędzy wydawaniem decyzji administracyjnej a zawiadomieniem o popełnieniu przestępstwa. Zawiadomienie o popełnieniu przestępstwa „nie zwalnia" inspektora od obowiązku wszczęcia postępowania administracyjnego i wydania decyzji administracyjnej nakazującej przywrócenie staniu zgodnego z prawem.

[939] Wzór upoważnienia i legitymacji zawiera rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 94, poz. 923) wydane na podstawie art. 22a u.o.d.o.

[940] B. Pilc, *op. cit.*, s. 46.

inspektora konieczną dokumentację, nośniki danych czy wstęp do wskazanych i kontrolowanych pomieszczeń. Powinien czynnie uczestniczyć w prowadzonej kontroli i nie uchylać się od udzielania wyjaśnień, przedkładania żądanych danych czy wykonywania innych przewidzianych prawem czynności.

Obecnie na skutek nowelizacji z 2010 r. u.o.d.o. w art. 54a przewidziane są sankcje karne za udaremnianie lub utrudnianie wykonywania kontroli. Przyjęte w 1997 r. w u.o.d.o. rozwiązania prawne w zakresie odpowiedzialności karnej okazały się mało efektywne, zatem w uzasadnieniu projektu ustawy o zmianie ustawy o ochronie danych osobowych z 2007 r. wskazana została potrzeba wzmocnienia skuteczności ochrony danych osobowych[941]. W uzasadnieniu podniesiono, iż dotychczasowa u.o.d.o. nie przyznaje GIODO żadnych skutecznych instrumentów służących egzekwowaniu prawa i mogących stanowić gwarancję tego, że administratorzy danych, którzy uporczywie naruszają przepisy ustawy o ochronie danych osobowych poniosą określone konsekwencje swoich działań[942]. Wprowadzenie art. 54a u.o.d.o. pozostało zatem w zgodzie z założeniami projektów zmian i stało się formalną gwarancją wykonywania ustawowych uprawnień kontrolnych Generalnego Inspektora[943].

Poszczególne czynności kontrolne są dokumentowane w celu włączenia ich do materiału dowodowego, na podstawie którego ustalany jest stan faktyczny. Z dokonywanych czynności kontrolnych inspektorzy sporządzają protokoły: protokół przyjęcia ustnych wyjaśnień, protokół przesłuchania świadka i protokół oględzin, które następnie stanowią załączniki do głównego protokołu kontroli[944]. Całe postępowanie kontrolne kończy się sformułowaniem wyników kontroli w postaci sporządzenia protokołu kontroli, który podpisuje inspektor i kontrolowany administrator (lub jego przedstawiciel). Protokół kontroli jest sporządzony w dwóch jednobrzmiących egzemplarzach, z których jeden doręcza się kontrolowanemu podmiotowi lub osobie przez niego upoważnionej, a drugi egzemplarz pozostaje w aktach kontroli. Kontrolowany administrator ma prawo wnieść na piśmie umotywowane zastrzeżenia i uwagi do protokołu, zarówno do jego treści jak i ustaleń

---

[941] Wdrożone zmiany w zakresie stosowania sankcji karnych były także realizacją wymogów dyrektywy 95/46/WE parlamentu Europejskiego i Rady, której art. 24 obliguje państwa członkowskie do podjęcia działań zmierzających do zapewnienia pełnej realizacji określonych w niej praw i obowiązków. Zob. uzasadnienie projektu ustawy o zmianie ustawy o ochronie danych osobowych, druk sejmowy nr 488 z dnia 21 grudnia 2007 r., dostępne na stronie: ww.sejm.gov.pl.

[942] Uzasadnienie projektu ustawy o zmianie ustawy o ochronie danych osobowych, druk sejmowy nr 488 z 21.12.2007 r., s. 1.

[943] Szerzej na ten temat: A. Błachnio-Parzych, *Prawnokarna ochrona inspektora ochrony danych osobowych-przestępstwo udaremnienia lub utrudnienia kontroli przestrzegania przepisów o ochronie danych osobowych*, „Dodatek do Monitora Prawniczego" 2011, nr 3, s. 35-41.

[944] B. Pilc, *op. cit.*, s. 46.

zawartych w protokole. Inspektor zobowiązany jest rozpatrzeć złożone zastrzeżenia i uwagi i ustosunkować się do nich, a o sposobie ich rozpatrzenia powinien zawiadomić kontrolowanego administratora na piśmie. W razie odmowy podpisania protokołu przez kontrolowanego inspektor czyni wzmiankę w protokole, a odmawiający podpisu może w terminie 7 dni przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi. Na podstawie zebranego w toku kontroli materiału dowodowego inspektor przedstawia wnioski z kontroli i jeżeli na podstawie wniosków z kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do GIODO o zastosowanie środków przewidzianych w art. 18 ustawy (art. 17 u.o.d.o.).

Na podstawie wyników kontroli następuje wszczęcie postępowania administracyjnego (art. 41§ 4 k.p.a.). Postępowanie administracyjne w sprawie stwierdzenia naruszenia przepisów o ochronie danych osobowych (tzw. postępowanie nakazowe) jest wszczynane z urzędu, w wyniku wniosku skierowanego do Generalnego Inspektora przez inspektora ochrony danych osobowych przeprowadzającego kontrolę (art. 17 ust. 1 u.o.d.o.), przy czym wniosek ten występuje tylko w sferze wewnętrznej Biura GIODO. Po zakończeniu kontroli przeprowadzający ją inspektor ochrony danych osobowych w przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych występuje do Generalnego Inspektora o wydanie decyzji administracyjnej[945]. W następstwie przeprowadzonej kontroli Generalny Inspektor wydaje następujące rodzaje decyzji: nakazującą przywrócenie stanu zgodnego z prawem, jeżeli zostały naruszone przepisy o ochronie danych osobowych (treść nakazu wynika z treści art. 18 u.o.d.o.) lub umarzającą postępowanie jako bezprzedmiotowe, jeżeli postępowanie administracyjne zostało wszczęte w wyniku stwierdzonych w toku kontroli uchybień, a w trakcie postępowania kontrolowany podmiot je usunął i przywrócił tym samym stan zgodny z prawem.

Charakteryzując działalność Generalnego Inspektora Ochrony Danych Osobowych w obszarze związanym z kontrolą zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych należy stwierdzić, że w latach 2007-2014 liczba kontroli utrzymywała się pomiędzy 165 a 220 rocznie, z czego najwięcej kontroli zostało przeprowadzonych w Warszawie (58% wszystkich kontroli). Najwięcej kontroli przeprowadzono z urzędu, a czynnościom kontrolnym poddane zostały m. in. obszary bankowe, administracji publicznej, służby zdrowia, oświaty, zatrudnienia, dostawcy usług

[945] Przez pojecie „zakończenia kontroli" rozumieć należy podpisanie protokołu przez inspektora i kontrolowanego administratora danych, z wyjątkiem sytuacji przewidzianej w art. 16 ust. 3 u.o.d.o., tj. odmowy podpisania protokołu przez kontrolowanego. Zob. G. Sibiga, *Postępowanie…*, s. 138.

telekomunikacyjnych, podmioty mające dostęp do danych przetwarzanych w systemie informacji o szkolnictwie wyższym czy sądy[946]. Na tej podstawie można wnioskować, że z uwagi na fakt, iż siedziba Biura GIODO mieści się w Warszawie, tam w większości były przeprowadzane kontrole. Co więcej, podobny obszar i charakter kontroli w ubiegłych latach wskazuje, że ostatnie kontrole GIODO odznaczają się taką samą specyfiką i w większości dotyczą podobnego zakresu tematycznego. Stwierdzone uchybienia dotyczyły głównie niewłaściwie spełnionego (lub wcale) obowiązku informacyjnego poprzez niezawarcie w nim wszystkich informacji wymaganych przez u.o.d.o. lub też „ukrycie" tych informacji wśród postanowień umowy lub regulaminu, co czyniło je w konsekwencji trudno dostępnymi i mało czytelnymi. Jednostki kontrolowane nie do końca spełniały także ustawowo wymagane warunki organizacyjne i techniczne w celu zabezpieczenia danych osobowych przed ich udostępnianiem czy zbieraniem przez nieupoważnione osoby, utratą, uszkodzeniem czy zniszczeniem. Kontrole uwidoczniły także notoryczne błędy w zakresie tworzenia i wdrażania dokumentacji z zakresu ochrony danych osobowych w instytucjach publicznych i prywatnych. Zwykle nie była to dokumentacja adekwatnie opracowana i dostosowana do charakteru i rodzaju przetwarzania danych.

Obecnie pocieszający jest jednak fakt, że z uwagi na coraz to wyższą świadomość w zakresie ochrony danych osobowych oraz znaczną poprawę w praktycznym stosowaniu regulacji w zakresie ochrony danych osobowych, liczba kontroli w ostatnich latach zmalała[947]. Sytuacja ta dowodzi, że działalność GIODO chociażby w sferze kontrolnej jest jak najbardziej efektywna, a tym samym całokształt polityki informacyjnej GIODO zmierzającej do popularyzacji wiedzy z zakresu ochrony danych osobowych przynosi pożądane efekty.

3. Prowadzenie rejestru zbiorów danych osobowych i administratorów bezpieczeństwa informacji oraz udzielenie informacji o zarejestrowanych zbiorach

Uprawnienie GIODO do kontroli przebiegu rejestracji zbiorów danych odgrywa istotną rolę dla rzeczywistego przestrzegania zasad przetwarzania danych osobowych. Ogólna zasada objęcia zbiorów danych osobowych kontrolą Generalnego Inspektora (art. 12 ust. 4 u.o.d.o) dotyczy uprawnień w zakresie rejestrowania zbiorów danych. Zadaniem GIODO jest głównie prowadzenie ogólnokrajowego, jawnego rejestru zbioru danych osobowych

[946] *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, s. 22-26.
[947] Zob. http://www.giodo.gov.pl/1520252/j/pl/.

zgłoszonych do rejestracji oraz ogólnokrajowego rejestru administratorów bezpieczeństwa informacji, udzielanie informacji o zarejestrowanych zbiorach, a także wydawanie, na żądanie osoby uprawnionej, zaświadczeń o zarejestrowaniu wskazanego zbioru danych lub o zarejestrowaniu administratora bezpieczeństwa informacji (rozdział 6 u.o.d.o.).

Prowadzenie jawnego rejestru zbioru danych osobowych zgłoszonych do rejestracji i rejestru administratorów bezpieczeństwa informacji opiera się na zasadzie jawności tych rejestrów, a każdy z obywateli ma możliwość skorzystania z uprawnień w zakresie dostępu do informacji. Każdy ma więc prawo przeglądać wskazane rejestry w ramach tzw. jawności formalnej rejestru, która nie wymaga istnienia interesu prawnego, zarówno w biurze GIODO jak i na oficjalnych stronach Generalnego Inspektora[948], oraz uzyskać zaświadczenie o wpisie określonego zbioru do rejestru (w trybie art. 217 k.p.a.).

Rejestr prowadzony jest w formie ksiąg rejestrowych (każdy ze zbiorów posiada odrębną księgę), dla których prowadzi się osobne akta rejestrowe i umieszcza się w nich całość dokumentacji stanowiącą podstawę wpisów dokonywanych w rejestrze[949]. Wpisów do rejestru jak i zmian w ich treści dokonują uprawnieni pracownicy Biura GIODO odpowiednio do informacji wynikających ze zgłoszenia lub jego uzupełnienia, sporządzonych zgodnie z wymogami art. 41 u.o.d.o. oraz art. 46b u.o.d.o.

Kompetencje Generalnego Inspektora w zakresie rejestracji zbiorów danych bezpośrednio związane są z praktyką przetwarzania danych osobowych, co stanowi realizację funkcji ewidencyjnej GIODO[950]. Dostęp do jawnego rejestru jest to z kolei jeden z aspektów realizacji uprawnień informacyjnych jednostki[951], zgodnie z którym każdy ma prawo dostępu do swoich danych oraz prawo do kontroli swoich danych, w jakich zbiorach są przetwarzane, przez jakiego administratora, w jakim celu, w jakim zakresie i w jaki sposób są one przetwarzane (art. 32 u.o.d.o.). Zgłoszenie zbioru danych do rejestracji powinno zawierać m. in.: wszystkie informacje identyfikujące podmiot prowadzący zbiór, tj. administratora danych osobowych, określać cel i zakres przetwarzania danych, sposób zbierania i udostępniania danych, opis środków technicznych i organizacyjnych służących do zabezpieczenia danych oraz opis kategorii osób, których dane dotyczą, informacje o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane i informacje dotyczące ewentualnego

[948] www.giodo.gov.pl/index.dhtml.
[949] K. Wygoda, *Ochrona…*, s. 416.
[950] R. Szałowski, *op. cit.*, , s. 44-45.
[951] A. Mrózek, *Ustawowe prawo ochrony danych. Analiza porównawcza*, Toruń 1981, s. 100.

przekazywania danych do państwa trzeciego (art. 41 ust. 1 u.o.d.o.)[952]. Jawność rejestru, w połączeniu z obowiązkiem zgłaszania zbiorów danych do rejestracji, uważać można za swego rodzaju „wstępną gwarancję" korzystania przez jednostkę ze swoich uprawnień określonych w art. 51 ust. 3 i ust. 4 Konstytucji, które ponadto uszczegółowione zostały w rozdziale 4 u.o.d.o.[953]. W ten sposób zapewnia się jej „niezbędną wiedzę o podmiotach przetwarzających dane oraz sposobach i warunkach, w jakich się to odbywa"[954].

Realizacja uprawnień rejestrowych GIODO jest także pewną formą wstępnej kontroli przetwarzania i zabezpieczenia danych[955]. Celem rejestracji jest „stworzenie możliwości kontroli przez Generalnego Inspektora, kto i jakie dane zbiera, aby w konsekwencji zapewnić autentyczną ochronę dóbr osobistych obywateli"[956].

Efektywność realizacji przedstawionych funkcji zapewnia przede wszystkim szeroki krąg podmiotów zobowiązanych na mocy ustawy o ochronie danych osobowych do spełnienia obowiązku rejestracyjnego. Na mocy art. 40 u.o.d.o. obowiązek ten ciąży na każdym administratorze danych, z wyjątkiem enumeratywnie wskazanych podmiotów w art. 43 ust. 1 i ust. 1a u.o.d.o. Wyłączeń od obowiązku rejestracji dokonano wskazując wprost określonych administratorów danych, którzy nie muszą rejestrować zbiorów lub wskazując kategorię zbiorów (art. 43 ust. 1 i ust. 1a u.o.d.o.) [957].

Kompetencje rejestrowe GIODO, na mocy art. 43 u.o.d.o., nie obejmują np. zbiorów danych objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia lub zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, a także zbiorów dotyczących członków kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej, zbiorów danych powszechnie dostępnych, zbiorów danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, zbiorów danych przetwarzanych dla potrzeb postępowania sądowego i przetwarzanych na podstawie przepisów o Krajowym Rejestrze Karnym oraz przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły

---

[952] Zob. M. Kluska, K. Koszewicz, G. Leśniewski, G. Wanio, *Ochrona danych osobowych w działach kadr. Odpowiedzi na 370 najtrudniejszych pytań*, Wrocław 2014, s. 105 i n.
[953] M. Sakowska, *Pozycja…*, s. 92.
[954] K. Wygoda, *Ochrona…*, s. 416.
[955] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 407.
[956] Uzasadnienie do projektu ustawy o ochronie danych osobowych z 11 sierpnia 1992 r., s. 4, niepublikowane. Za: G. Sibiga, *Zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych*, „Monitor Prawniczy" 1999, nr 8, s. 17.
[957] Np. Generalny Inspektor Informacji Finansowej na podstawie art. 43 ust. 1 pkt 2a u.o.d.o. oraz na podstawie ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (Dz. U. z 2003 r. Nr 153, poz.1505 z późn. zm.)

wyższej lub stopnia naukowego, zbiorów danych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego, czy zbiorów danych powszechnie dostępnych[958].

Od 1 stycznia 2015 r. znowelizowane przepisy u.o.d.o. przewidują również zwolnienie z obowiązku rejestracji u Generalnego Inspektora tych zbiorów danych, które nie są prowadzone z wykorzystaniem systemów informatycznych (zbiory danych prowadzone wyłącznie w formie papierowej), z wyjątkiem, gdy w zbiorze przetwarzane są tzw. dane szczególnie chronione, o których mowa w art. 27 ust. 1 ustawy (art. 43 ust.1 pkt 12 u.o.d.o.)[959]. Tak prowadzonych zbiorów nie trzeba zgłaszać do rejestracji u Generalnego Inspektora ani dokonywać aktualizacji takich zgłoszeń również wówczas, gdy administrator danych powoła administratora bezpieczeństwa informacji (ABI) i zgłosi go Generalnemu Inspektorowi do rejestracji.

Zgłoszenie zbioru do rejestracji jest także warunkiem koniecznym do rozpoczęcia przetwarzania danych w zbiorze, a w przypadku zbioru zawierającego dane wrażliwe, przetwarzanie może nastąpić dopiero po jego zarejestrowaniu (art. 46 ust. 1 i ust. 2 u.o.d.o.). Obowiązek rejestracji jest niezależny od faktycznego wykorzystywania zbioru[960], a także od ilości danych wchodzących w skład zbioru[961]. Nie dotyczy zbiorów danych, do których postanowienia u.o.d.o. nie mają zastosowania, a także w sposób oczywisty zbiorów wyłączonych na mocy ustawy z obowiązku rejestracji.

Niewykonanie obowiązku notyfikacji wiąże się z sankcjami karnymi, które przewiduje art. 53 u.o.d.o., takimi jak: kara grzywny, kara ograniczenia wolności albo pozbawienia wolności do roku.

Generalny Inspektor Ochrony Danych Osobowych realizując ustawowy obowiązek rejestracji stwierdziwszy, że nie zachodzą żadne przeszkody do rejestracji zbioru, tj. zostały spełnione przesłanki rejestracji zbioru oraz wymogi formalne zgłoszenia zbioru, w efekcie wpisuje zbiór do rejestru i wystawia administratorowi stosowne zaświadczenie z urzędu - jeżeli jest to zbiór danych wrażliwych, lub na jego wniosek, gdy doszło do rejestracji zbioru danych zwykłych.

---

[958] Tj. „sprawy drugorzędne, niemające zasadniczego znaczenia dla administratora danych. Jednocześnie jednak ta drugorzędność powinna mieć charakter obiektywny, w przeciwnym wypadku zbiór zawierający określone dane i służący określonym celom, prowadzony w «drobnych bieżących sprawach życia codziennego» może nie być uznany za taki przez innego dysponenta zbioru". Zob. http://www.giodo.gov.pl/323/id_art/993/j/pl/.
[959] http://www.giodo.gov.pl/1520001/id_art/8306/j/pl; Dz. U. z 2014 r., poz. 1662.
[960] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 683.
[961] A. Drozd, *Ustawa…*, s. 264.

Wpis do rejestru i całe postępowanie rejestrowe jest czynnością materialno-techniczną[962], chociaż w literaturze przedmiotu prezentowane są stanowiska, iż rejestracja ma charakter decyzji administracyjnej[963]. W u.o.d.o. nie określono wprost prawnej formy wpisu do rejestru zbioru danych. Ustawodawca w sposób wyczerpujący określił uprawnienia GIODO do wydawania decyzji (np. art. 18 ust. 1, art. 32 ust. 2, art. 44 ust. 1 u.o.d.o.) czy przynajmniej wyraził takie kompetencje organu w formie czasownikowej (np. art. 35 ust. 2, art. 48 u.o.d.o.), dlatego nie powinno się domniemywać podstawy prawnej wydawania decyzji administracyjnych, gdy przepisy materialne nie zawierają takiej podstawy[964].

Trudno także uznać postępowanie rejestrowe prowadzone przez Generalnego Inspektora za typowe postępowanie administracyjne (pomimo iż w art. 22 u.o.d.o. wyraźnie wskazane jest, że stosuje się przepisy k.p.a. w przypadku wszystkich postępowań, które zostały określone w niniejszej ustawie), stąd jego materialnotechniczny charakter (na wzór chociażby wpisu do ewidencji działalności gospodarczej). Co więcej, ten typ postępowania prowadzony przez Generalnego Inspektora jest odmienny od typowych procedur administracyjnych z uwagi na fakt, iż braki formalne wniosku zobowiązują GIODO w trybie art. 44 ust. 1 u.o.d.o. do wydania wspomnianego nakazu (decyzji o odmowie rejestracji), a nie jak wskazuje art. 64 §2 k.p.a., do pozostawienia go bez rozpatrzenia (w sytuacji bezskutecznego wezwania administratora danych do usunięcia tych braków)[965]. Za K. Wygodą warto więc powtórzyć, iż „takie ukształtowanie procedury rejestracji sprzyja zabezpieczeniu praw osób, których dane dotyczą"[966]. Można na tej podstawie zatem próbować wysunąć wniosek, iż realizacja uprawnień przez Generalnego Inspektora i przez to jego pozycja wśród innych organów w państwie nie ogranicza się do jednoznacznego umiejscowienia GIODO tylko wśród organów administracyjnych, a więc „innych organów państwowych […] zaliczanych do organów administracji publicznej w znaczeniu funkcjonalnym"[967], a nakazuje potraktowanie donioślej ten organ z uwagi na jego działalność w zakresie ochrony praw i wolności jednostki, jako organu ochrony prawa opierającego swoje istnienie na normach Konstytucji.

---

[962] Za takim stanowiskiem opowiedzieli się m. in: A. Szewc, *Z problematyki ochrony danych osobowych, cz. III*, „Radca Prawny" 1999, nr 5, s. 19; E. Kulesza, G. Sibiga, *Wykonanie obowiązku rejestracji zbiorów danych osobowych przez kasy chorych*, „Prawo i Medycyna" 2000, nr 6-7, s. 127; K. Wygoda, *Ochrona…*, s. 416.
[963] G. Szpor, *Ustawa…*, s. 143.
[964] G. Sibiga, *Postępowanie…,* s. 176.
[965] K. Wygoda, *Ochrona…*, s. 417.
[966] *Ibidem*, s. 417.
[967] W. Chróścielewski, *Organ…*, s. 52-53.

W przypadku jednak niedopełnienia wskazanych przez ustawę warunków GIODO ma obowiązek na mocy art. 44 u.o.d.o. wydać decyzję o odmowie rejestracji zbioru danych i zgodnie z ust. 2 tego artykułu nakazać „wstrzymanie dalszego przetwarzania danych w tym zbiorze lub ich usunięcie", co podlega natychmiastowemu wykonaniu. Takie skutki są przewidziane w przypadku, gdy „nie zostały spełnione wymogi określone w art. 41 ust. 1, co do prawidłowości sporządzenia wniosku rejestrowego, jeśli „przetwarzanie danych naruszałoby zasady" dotyczące przetwarzania danych, określone w art. 20-30 u.o.d.o., lub jeśli „urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w przepisach" wykonawczych do ustawy. Jeżeli zaś zgłoszony przez administratora wniosek dotyczył zbioru zwolnionego od rejestracji na mocy art. 43 ust. 1 u.o.d.o., wówczas Generalny Inspektor umarza postępowanie jako bezprzedmiotowe.

Udzielanie informacji o zarejestrowanych zbiorach następuje w wyniku przeglądania akt rejestrowych w biurze GIODO, a także w wyniku wydawania zaświadczeń, głównie administratorom danych[968]. Na czynność polegającą na dokonaniu wpisu do rejestru, w związku z tym, że nie jest ona decyzją administracyjną, nie przysługuje odwołanie[969].

Nie tylko zbiór danych, ale i każdą zmianę informacji podanych w zgłoszeniu administrator danych ma obowiązek zgłosić do organu rejestrowego, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych (art. 41 ust. 2 u.o.d.o.). Jest to bardzo istotny obowiązek, gdyż w razie kontroli GIODO może nakazać przywrócenie stanu zgodnego z prawem, tj. stanu uwidocznionego w rejestrze zbiorów[970]. Rejestr zbiorów danych, aby spełniał swoje funkcje, powinien zawierać informacje aktualne o zgłoszonych zbiorach. W obecnym stanie prawnym należy przyjąć, iż Generalny Inspektor nie jest uprawniony do odmowy wpisu zgłoszonych zmian do rejestru zbioru danych[971].

Z prowadzeniem ogólnokrajowego jawnego rejestru zbiorów danych osobowych przez GIODO skorelowany jest obowiązek zgłaszania do rejestracji zbiorów danych osobowych przez administratorów danych. Na tej podstawie administratorzy danych, wypełniając nałożony przepisami u.o.d.o. obowiązek, w latach 2007- 2014 zgłosili do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych od 4850 zbiorów w roku 2007 do

---

[968] A. Drozd, *Ustawa…*, s. 96.
[969] G. Sibiga, *Postępowanie…,* s. 177.
[970] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 696.
[971] A. Siostrzonek, *Dane osobowe gromadzone w bazach danych i ich ochrona w prawie polskim*, „Rejent" 1999, nr 9, s. 275; E. Kulesza, *Rejestr musi być aktualny*, „Rzeczpospolita" z 31.08.2000 r.

28264 w 2014 roku, z czego podmioty z sektora administracji publicznej zgłosiły średnio około 54 % ogólnej liczby zgłoszeń dokonanych w tym okresie, zaś podmioty z sektora prywatnego 46 % ogólniej liczby zgłoszonych zbiorów[972]. Obserwuje się więc tendencję zwyżkową w zakresie realizacji obowiązku rejestracyjnego praktycznie w takim samym zakresie w sektorze publicznym jak i prywatnym, co stanowi o stale rosnącej świadomości obywateli w zakresie ochrony danych osobowych.

W dniu 1 stycznia 2015 r. weszły w życie, wprowadzone na mocy art. 9 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[973], zmiany przepisów ustawy o ochronie danych osobowych dotyczące m.in. funkcjonowania administratora bezpieczeństwa informacji. Zgodnie z treścią art. 46b u.o.d.o. administrator danych jest obowiązany zgłosić do rejestracji GIODO także powołanie i odwołanie administratora bezpieczeństwa informacji (ABI)[974]. Prowadzenie przez GIODO ogólnopolskiego jawnego rejestru administratorów bezpieczeństwa informacji (dalej: rejestr ABI) przewiduje art. 46c u.o.d.o. Rejestr ten zawiera informacje o powołanych przez administratorów danych i zarejestrowanych u Generalnego Inspektora administratorach bezpieczeństwa informacji.

Na wykonanie obowiązku rejestracji ABI administrator danych ma 30 dni licząc od dnia jego powołania lub odwołania. Zgłoszenie powołania ABI do rejestru powinno spełniać wymogi formalne, zgodnie z treścią art. 46b ust. 2 u.o.d.o., zaś zgłoszenie odwołania ABI powinno zawierać wymagane informacje zgodnie z treścią art. 46b ust. 3 u.o.d.o. Zgłoszenia powołania ABI do rejestracji Generalnemu Inspektorowi oraz zgłoszenia odwołania ABI należy dokonać przy użyciu wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, które stanowią załączniki do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji [975]. Wzór zgłoszenia powołania może być także wykorzystany do zgłoszenia zmian w tym rejestrze.

Nowością wprowadzoną w zakresie prowadzenia rejestru danych przez Generalnego Inspektora Ochrony Danych Osobowych jest również uruchomienie systemu informatycznego

---

[972] *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych w roku 2013,* s. 127.
[973] Dz. U. z 2014, poz. 1662.
[974] Zob. K. Wygoda, *Powoływanie Administratora Bezpieczeństwa Informacji jako zasada bezpiecznego przetwarzania danych na gruncie ustawy o ochronie danych osobowych*, „Przegląd Prawa i Administracji" 2015;. C/2, No 3661, s. 337 i n.; A. Mednis , *Administrator bezpieczeństwa informacji po nowelizacji ustawy o ochronie d*anych osobowych z 7.11.2014 r. – ocena rozwiązań, [w:] Aktualne problemy ochrony danych osobowych, dodatek do Monitora Prawniczego, 2015, nr 6.
[975] Dz. U. z 2014 r., poz. 1934.

zapewniającego publiczny dostęp do rejestru ABI[976]. Publiczny dostęp do rejestru ABI udostępniony został w ramach rozbudowy funkcjonującej od 2006 r. elektronicznej platformy komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych zwanej e-GIODO[977]. Platforma ta służy nie tylko do udostępniania informacji zawartych w prowadzonych przez GIODO ogólnopolskim jawnym rejestrze zbiorów danych osobowych i ogólnopolskim, jawnym rejestrze administratorów bezpieczeństwa informacji, ale również do wspomagania operacji przesyłania drogą elektroniczna wniosków do GIODO o wpis lub aktualizację zawartych w nich informacji. Uruchomiony 26 stycznia 2015 r. moduł systemu e-GIODO umożliwiający dostęp do Rejestru ABI jest jednym z pierwszych etapów prac nad tym rejestrem. Kolejnymi etapami jego rozbudowy jest wdrażanie mechanizmów, które pozwolą przekazywać m. in.: wnioski o wpis, aktualizację lub wykreślenie ABI drogą elektroniczną z wykorzystaniem platformy ePUAP (elektronicznej Platformy Usług Administracji Publicznej).

Skutkiem zmian w zakresie wprowadzenia rejestrów ABI jest także fakt, iż w przypadku zgłoszenia ABI do rejestru ABI prowadzonego przez GIODO, nie istnieje obowiązek zgłaszania do GIODO zbiorów danych osobowych nie zawierających danych wrażliwych. Zgłoszony do rejestracji u GIODO ABI ma obowiązek wówczas prowadzić aktualny jawny rejestr zbiorów danych osobowych[978].

W przypadku zbiorów tzw. danych wrażliwych (art. 27 ust. 1 u.o.d.o.), nadal istnieje obowiązek zgłoszenia takich zbiorów danych do rejestracji GIODO przed rozpoczęciem przetwarzania (art. 40 u.o.d.o.).

4. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych

Eliminowaniu nieprawidłowości dotyczących przetwarzania danych osobowych już na etapie tworzenia prawa pozwala uprawnienie GIODO nadane mu przez ustawodawcę w zakresie opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych

---

[976] System e-GIODO umożliwiający publiczny dostęp do prowadzonych przez GIODO rejestru zbiorów danych osobowych oraz rejestru administratorów bezpieczeństwa informacji dostępny jest pod adresem: http://egiodo.giodo.gov.pl.

[977] http://www.giodo.gov.pl/560/id_art/8366/j/pl/.

[978] Od 1 stycznia 2015 r. informacje umieszczone w jawnym rejestrze zbiorów prowadzonym przez ABI nie muszą być aktualizowane w rejestrze GIODO, z wyjątkiem zbiorów zawierających tzw. dane wrażliwe. ABI nie są także zobowiązani do wnioskowania o wykreślenie z rejestru GIODO prowadzonych u siebie zbiorów z danymi zwykłymi.

osobowych (art. 12 pkt 5 u.o.d.o.o). W praktyce jednak działalność opiniodawcza jest przez GIODO rzadko wykorzystywana, gdyż cały czas jest zbyt mała liczba projektów ustaw i rozporządzeń odnoszących się do ochrony danych osobowych[979].

Niewątpliwie uprawnienie Generalnego Inspektora w zakresie opiniowania projektów aktów normatywnych z punktu widzenia ich zgodności z zasadami ochrony danych osobowych jest bardzo ważne[980]. Wiele przygotowywanych projektów ustaw nie uwzględnia istoty postanowień zawartych w u.o.d.o. (np. w projektach ustaw nie ma poprawnie sformułowanej delegacji do wydawania przepisów wykonawczych albo przepisy wykonawcze upoważniają do przetwarzania danych sensytywnych, gdy może na to zezwalać tylko przepis ustawowy)[981]. W praktyce zdarza się, iż znaczna część aktów prawnych jest wydawanych z naruszeniem ustawy o ochronie danych osobowych, a wiele aktów prawnych przedstawionych do konsultacji i opinii Generalnego Inspektora w finalnej opinii GIODO zawiera naruszenia konstytucyjnych praw i wolności jednostki właśnie w zakresie ochrony danych osobowych. Zdarza się również, iż projekty aktów nie zostały w ogóle przedstawione GIODO do opinii lub treść opinii GIODO nie została uwzględniona przy przygotowywaniu projektu.

Taki stan rzeczy jest konsekwencją braku w ustawie obligatoryjnego wymogu konsultacji i uzyskania opinii od Generalnego Inspektora, co do zakresu postanowień dotyczących ochrony danych osobowych. Z tego względu opinie GIODO na chwilę obecną nie mają i nie mogą mieć charakteru wiążącego. Wyjątkiem jest tylko sytuacja, gdy przepisy szczególne mogą przewidywać, iż organy wydające akty o charakterze wewnętrznie obowiązującym mają obowiązek zasięgania opinii GIODO przed ich wydaniem[982].

GIODO dokonując opinii w zakresie projektów aktów prawnych niejednokrotnie zwracał uwagę, iż wiele przepisów resortowych zawiera niewłaściwe sformułowania dotyczące istotnych instytucji oraz zagadnień z zakresu ochrony prywatności jednostki i ochrony danych osobowych, w następstwie czego jest szereg błędów interpretacyjnych w

---

[979] Przykładowo w roku 2008 do Biura GIODO wpłynęło do zaopiniowania 511 projektów aktów prawnych, w roku 2009 - 625 projektów aktów prawnych, w roku 2010- 617 projektów aktów prawnych, w roku 2011 - 603 projektów aktów prawnych, w 2012 - 598 projektów aktów prawnych, a w roku 2013 było to 617 projektów aktów prawnych. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, s. 138.
[980] Zob. http://www.giodo.gov.pl/1520254/j/pl/.
[981] E. Kulesza, *Pozycja…,* s. 20.
[982] A. Drozd, *Ustawa…*, s. 97

zakresie przetwarzania danych przez podmioty publiczne, prywatne czy osoby fizyczne[983]. Zgłaszając uwagi do projektów aktów normatywnych celem GIODO jest wyeliminowanie błędnych rozwiązań dotyczących ochrony danych osobowych, jak również wskazanie jak najwłaściwszych narzędzi prawnych, technicznych i organizacyjnych, które można lub trzeba zastosować w procesie ochrony prywatności człowieka. GIODO stając na straży ochrony prywatności jednostki niejednokrotnie wskazywał również, iż realizacji określonych założeń i celów nie może odbywać się w oderwaniu od poszanowania prawa do prywatności jednostki i w konsekwencji przy użyciu środków nadmiernych i zbędnych z punktu widzenia realizacji celów, które dotkliwie ingerują w to konstytucyjnie gwarantowane prawo[984].

W zakresie realizacji przedmiotowego zadania organ do spraw ochrony danych osobowych został zaliczony do organów uczestniczących w uzgodnieniach międzyresortowych, o których mowa w uchwale nr 13 Rady Ministrów z dnia 25 lutego 1997 r. Regulamin pracy Rady Ministrów[985], w sytuacji gdy projekt aktu prawnego jest przygotowywany przez rząd. Nie ma on natomiast możliwości wyrażania opinii na temat projektu aktu normatywnego stanowiącego wynik inicjatywy poselskiej[986].

Generalny Inspektor nie został wyposażony w prawo skutecznego żądania zmiany aktu prawnego niezgodnego z art. 51 Konstytucji oraz z u.o.d.o. GIODO nie przysługuje również kompetencja do wystąpienia do Trybunału Konstytucyjnego z wnioskiem o zbadanie zgodności aktu normatywnego (projektu) z Konstytucją. W przypadku naruszenia Konstytucji poprzez niezgodność treści aktu prawnego z Konstytucją, GIODO ma jedynie możliwość skierowania prośby do organu, który wydał taki akt, o rozważenie jego zmiany lub może zwrócić uwagę podmiotu uprawnionego na mocy art. 191 Konstytucji do składania wniosków do Trybunału Konstytucyjnego (np. Rzecznika Praw Obywatelskich, Prezesa Najwyższej Izby Kontroli, Prokuratora Generalnego) na potrzebę uruchomienia stosownej procedury przed TK[987].

Co więcej, Generalny Inspektor nie uzyskał także prawa do występowania do Sądu Najwyższego z wnioskami o podjęcie uchwały mającej na celu wyjaśnienie przepisów

---

[983] Zob. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, s. 138-211*; Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2012*, s. 114-176.
[984] *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, s. 156.
[985] M. P. Nr 15, poz. 144, z późn. zm.
[986] E. Kulesza, *Pozycja…,* s. 19.
[987] M. Sakowska, *Pozycja…*, s. 88.

prawnych budzących wątpliwości w praktyce, lub których stosowanie wywołało rozbieżności w orzecznictwie[988].

Pominięcie GIODO wśród podmiotów mających prawo do inicjowania postępowania przez TK oraz składania wniosków do Sądu Najwyższego stanowi o ograniczeniu wpływu tego organu na proces kontroli konstytucyjności prawa. Brak nawet możliwości przedstawienia TK zakwestionowanego aktu prawnego czy zakwestionowanej normy prawnej w zakresie ochrony danych osobowych jest niewspółmierne do roli, jaką w całym procesie ochrony prawa ma spełniać ten organ. Ustanowienie i tak dość szerokiego kręgu podmiotów uprawnionych do inicjowania abstrakcyjnej kontroli norm przez TK w obecnej rzeczywistości stało się jednak niewystarczającym, skoro pominięty został organ do spraw ochrony danych osobowych, ze swej istoty powołany jako organ do sprawowania kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Pozbawienie GIODO prawa inicjatywy do TK czy możliwości składania wniosków do Sądu Najwyższego nie powinno być jednak równoznaczne z brakiem jego zainteresowania ochroną praworządności w stanowieniu prawa, a wręcz przeciwnie. Organ ten wyposażony został m. in. w kompetencje opiniodawcze, których efektem jest konkretne stwierdzenie, iż istnieje lub nie istnieje niezgodność z zasadami ochrony danych osobowych, a tym samym i potencjalny interes prawny do dokonania wnikliwej kontroli norm przez TK.

W świetle powyższego zasadnym byłoby wyposażenie Generalnego Inspektora w szersze kompetencje, tak by mógł on w najwyższym możliwie stopniu wykonywać powierzone zadania i w pełni samodzielnie oddziaływać na kształt obowiązujących regulacji prawnych w zakresie ochrony danych osobowych. Postulaty *de lege ferenda* kierowane do ustawodawcy dotyczyłyby zatem wyposażenia GIODO w prawo zwracania się do Sądu Najwyższego z wnioskiem o podjęcie uchwały mającej na celu wyjaśnienie przepisów prawnych budzących wątpliwości w praktyce lub których stosowanie wywołało rozbieżności w orzecznictwie; składania do TK wniosku o ustalenie zgodności aktu normatywnego z Konstytucją RP i zgłaszania udziału w postępowaniu przez TK w sprawach skarg konstytucyjnych dotyczących ochrony danych osobowych i uczestniczenia w tych postępowaniach; zwracania się do Sejmu o zlecenie Najwyższej Izbie Kontroli przeprowadzenia kontroli dla zbadania określonej sprawy.

---

[988] Prawo takie ma np. Rzecznik Praw Obywatelskich, zgodnie z art. 16 ust. 2 pkt 4 ustawy o Rzeczniku Praw Obywatelskich.

W moim przekonaniu także umiejscowienie GIODO wśród podmiotów z art. 191 Konstytucji wpłynęłoby znacząco na okazanie ważności zagadnieniom z zakresu ochrony prywatności i ochrony danych osobowych człowieka. Ten fakt przyczyniłby się również do wskazania, iż Generalny Inspektor jest organem, na równi z innymi podmioty wymienionymi w tym artykule, powołanym do czuwania nad konstytucyjnością i legalnością unormowań prawnych w Polsce.

5. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

Zadanie przyznane GIODO na mocy art. 12 pkt 6 u.o.d.o. dotyczące inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych, to szeroko zakrojone działania informacyjne i edukacyjne, których różnorodna forma i dynamika ma wpływ na podnoszenie świadomości społecznej w sprawach dotyczących ochrony prywatności i ochrony danych osobowych. To zadanie obejmuje propagowanie idei ochrony danych osobowych, ale przede wszystkim ma dotyczyć podejmowania inicjatyw w zakresie ochrony danych osobowych zarówno pod względem prawa obowiązującego, jak i przyszłych norm prawnych.

Jednym z elementów działalności edukacyjnej i informacyjnej GIODO jest udzielanie odpowiedzi na pytania dotyczących legalności przetwarzania danych osobowych bądź sygnalizujących różnego rodzaju problemy interpretacyjne związane z ich przestrzeganiem, co dotyczy różnych sektorów i branż[989]. Pytania prawne kierowane do GIODO w znacznej większości dotyczą działalności różnych instytucji publicznych, banków i innych instytucji finansowych, firm windykacyjnych, szkół wyższych, zakładów opieki zdrowotnej, podmiotów świadczących usługi w sieci, a także zagadnień związanych z rejestracją zbiorów danych.

W praktyce inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych ma także formę wystąpień Generalnego Inspektora do parlamentu oraz centralnych organów administracji państwowej z wnioskami o zmianę prawa

[989] Np. w 2013 r. do Biura GIODO wpłynęło 4911 pytań prawnych odnoszących się do legalności przetwarzania danych osobowych i problemów w zakresie interpretacji przepisów u.o.d.o., a jeszcze np. w 2010 r. było to 3448 zapytań. To jednoznacznie wskazuje na większe zainteresowanie różnych podmiotów prawną ochroną danych osobowych oraz wzrostem świadomości społeczeństwa co do konieczności legalnego przetwarzania danych osobowych. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, s. 211.

w razie stwierdzonej sprzeczności obowiązujących przepisów z art. 51 Konstytucji oraz przepisami u.o.d.o.[990] Wystąpienia stanowią pewne uzupełnienie prawa opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych (wskazane w art. 12 pkt 5 u.o.d.o.), gdyż celem w tych obu przypadkach jest dostosowanie systemu prawa do wymogów ochrony danych osobowych[991]. Co więcej, realizacji tego uprawnienia GIODO służy także obowiązek wspomnianego już w pracy składania corocznych sprawozdań ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych (art. 20 u.o.d.o.). Przy okazji prezentowania Sejmowi wniosków co do aktualnego stanu Generalny Inspektor ma możliwość także wysuwania wniosków *de lege ferenda.*

W celu realizacji zadań, o których mowa w art. 12 pkt 6 u.o.d.o., Generalny Inspektor może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. Generalny Inspektor może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej lub o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Nowe kompetencje GIODO zawarte w treści art. 19a u.o.d.o. dotyczą przede wszystkim prawa do wystąpienia zmierzającego do zapewnienia skutecznej ochrony danych osobowych oraz prawa do złożenia wniosku o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Przed wprowadzeniem nowelizacji z 2010 r. instytucja wystąpienia nie była znana na gruncie ustawy o ochronie danych osobowych. W praktyce GIODO zdarzały się wystąpienia o charakterze wewnętrznym Biura GIODO, będące etapem wydawania decyzji administracyjnej (art. 17 ust. 1 u.o.d.o.) lub wystąpienia (sygnalizacje) GIODO kierowane do innych podmiotów (zindywidualizowanych administratorów danych) w zakresie konkretnych naruszeń praw i obowiązków wynikających z ustawy[992]. Uprawnienie do wystąpienia posiadał Rzecznik Praw Obywatelskich[993] czy

---

[990] E. Kulesza, *Pozycja…,* s. 21.
[991] *Ibidem,* s. 21.
[992] W przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych przysługuje możliwość „występowania do administratorów danych o zmianę niewłaściwych praktyk (tzw. sygnalizacje)". M. Krasińska, S. Mizerek, *ABC wybranych zagadnień z ustawy o ochronie danych osobowych (Biuro GIODO)*, Warszawa 2007, s. 9-10.
[993] Art. 16 ustawy o Rzeczniku Praw Obywatelskich.

Rzecznik Praw Dziecka[994], zaś nie posiadał ich dotąd Generalny Inspektor, dlatego istotnym stało się wyposażenie także tego organu w analogiczne kompetencje[995].

Generalny Inspektor zyskał zatem nowe uprawnienie do przedstawiania właściwym organom, organizacjom czy instytucjom ocen i wniosków, których celem jest zapewnienie skutecznej ochrony danych osobowych, obok realizowanych odrębnie zadań ustawowych w zakresie kontroli przestrzegania przepisów prawa czy wydawania decyzji (art. 12 pkt 1-2 u.o.d.o.). Wystąpienie nie jest zatem środkiem w sprawie indywidualnej naruszenia przepisów o ochronie danych osobowych i nie może poprzedzać lub zastępować decyzji nakazowej Generalnego Inspektora (art. 18 ust. 1 u.o.d.o.)[996]. Wydanie decyzji nakazowej GIODO jest poprzedzone właściwym postępowaniem w trybie k.p.a. (art. 22 u.o.d.o.). Nie może również mieć miejsce sytuacja, że w tej samej sprawie organ jednocześnie wystosował wystąpienie i wydał nakaz[997].

Wprawdzie u.o.d.o. nie ogranicza przedmiotu wystąpienia, jednak na pewno nie może ono służyć przywracaniu stanu zgodnego z prawem w indywidualnej sprawie[998]. GIODO kieruje swoje wystąpienie do konkretnego adresata, zatem musi dokonać oceny stanu faktycznego w zakresie ochrony danych osobowych i wyciągnąć wnioski. Następnym etapem jest skierowanie uwag, rekomendacji, postulatów czy zaleceń adekwatnych w konkretnym przypadku mających na celu zapewnienie skutecznej ochrony danych osobowych. GIODO może wskazać konkretne działania czy dobre praktyki dla osiągnięcia przedmiotowego celu, jednak wystąpienie nigdy nie będzie źródłem obowiązków ochrony danych dla jego adresata. Wystąpienie może stanowić konsekwencję ustaleń dokonanych w trakcie kontroli, np. gdy zostanie stwierdzona powtarzalna a nieprawidłowa praktyka w działalności podmiotu; wówczas wystąpienie może mieć charakter sygnalizacji do organu nadrzędnego. Wystąpienie może mieć zatem charakter indywidualny, gdy jego celem będzie zwrócenie uwagi oraz sygnalizacja co do udoskonalenia zasad ochrony danych osobowych względem konkretnego adresata oraz generalny, którego celem będzie powszechna rekomendacja dobrych praktyk ochrony danych osobowych. Adresatem wystąpienia może być każdy, gdyż u.o.d.o. nie wskazała ani określonych rodzajów podmiotów ani określonych kategorii podmiotów do których może zostać skierowane wystąpienie, a to z uwagi na użyte w treści art. 19a ust. 1

---

[994] Art. 11 ustawy z 6 stycznia 2000 r. o Rzeczniku Praw Dziecka (Dz. U. Nr 6, poz. 69 z późn.zm.).
[995] Uzasadnienie projektu ustawy o zmianie ustawy o ochronie danych osobowych, druk sejmowy nr 488 z 21.12.2007 r., s. 3, dostępne na: www.sejm.gov.pl.
[996] G. Sibiga, *Wystąpienie- nowa kompetencja Generalnego Inspektora ochrony Danych Osobowych*, „Dodatek do Monitora Prawniczego" 2011, nr 3, s. 27.
[997] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 436.
[998] G. Sibiga, *Wystąpienie…,* s. 27.

określenie „inny podmiot". Adresatem wystąpienia więc mogą być nie tylko podmioty bezpośrednio odpowiedzialne za przestrzeganie przepisów o ochronie danych osobowych (np. administrator danych, przetwarzający), ale i inne podmioty mające wpływ na prawidłową realizację wymogów ustawy.

Kompetencja określona w art. 19a ust. 2 u.o.d.o. jest wzorowana na analogicznych uprawnieniach, które posiada Rzecznik Praw Obywatelskich, określanych jako pośrednia inicjatywa prawodawcza. Przyznaje się ją organom, które same nie posiadają inicjatywy ustawodawczej lub podstawy do wydawania aktów powszechnie obowiązujących.

Nowelizacją u.o.d.o. z dnia 29 października 2010 r.[999] została wprowadzona również konstrukcja wniosków, które Generalny Inspektor może kierować do właściwych organów. Jednym z podstawowych celów tej nowelizacji było wzmocnienie kompetencyjne organu do spraw ochrony danych osobowych, poprzez wyposażenie go w kolejne niewładcze uprawnienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. Nowelizacja przyczyniła się do połączenia w rękach GIODO uprawnień inspektorskich - władczych (tj. do wydawania decyzji administracyjnych) z uprawnieniami niewładczymi (tj. do kierowania wystąpień), typowymi dla rzeczników[1000].

Zgodnie z treścią art. 19a ust. 2 Generalny Inspektor może także występować do właściwych organów z wnioskami w przedmiocie: podjęcia inicjatywy ustawodawczej oraz wydania lub zmiany aktów prawnych[1001]. Inaczej niż w przypadku wystąpienia, o którym mowa w art. 19a ust. 1 u.o.d.o., wniosek może być kierowany jedynie do określonych kategorii odbiorców: w zakresie podjęcia inicjatywy ustawodawczej - do organów uprawnionych do wnoszenia projektów ustaw na podstawie art. 118 Konstytucji (posłowie, Senat, Prezydent RP, Rada Ministrów), a w zakresie wydania lub zmiany aktu prawnego - do organów uprawnionych do wydawania rozporządzeń na podstawie stosownych upoważnień ustawowych, jak również do organów samorządu terytorialnego oraz terenowych organów administracji rządowej - w przypadku wniosku dotyczącego prawa miejscowego[1002]. Z uwagi na to, iż Generalny Inspektor nie posiada prawa inicjatywy ustawodawczej, przyznanie mu możliwość zwrócenia się do podmiotów, które takie uprawnienia mają, ułatwia organowi

---

[999] Dz. U. Nr 229, poz. 1497.
[1000] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 435.
[1001] Kompetencja określone w art. 19a ust. 2 u.o.d.o. jest wzorowana na analogicznych uprawnieniach, które posiada Rzecznik Praw Obywatelskich, określane jako pośrednia inicjatywa prawodawcza. Przyznaje się je organom, które same nie posiadają inicjatywy ustawodawczej lub podstawy do wydawania aktów powszechnie obowiązujących.
[1002] G. Sibiga, *Wystąpienie…,* s. 28-29.

ochrony danych działania w zakresie doskonalenia przepisów w dziedzinie ochrony danych osobowych.

Przyznane Generalnemu Inspektorowi kompetencje, o których mowa w art. 12 pkt 6 u.o.d.o., jak i nowe uprawnienia, na podstawie art. 19a u.o.d.o. zapewniają mu prawną formę działania, której celem ma być przede wszystkim jeszcze skuteczniejsza ochrona danych osobowych. Jako specjalistyczny organ do spraw ochrony danych osobowych może on przedstawiać swoje wnioski, analizy oraz postulaty, które w znaczący sposób mają szansę wpłynąć na późniejszy proces stanowienia jak i stosowania prawa. Przyznanie wyraźnych podstaw prawnych w ustawie we wskazanym zakresie powinno wzbudzić jeszcze większą aktywność i powagę działań Generalnego Inspektora.

Aktywność Generalnego Inspektora zgodnie z art. 12 pkt 6 u.o.d.o. wymaga przede wszystkim działalności informacyjnej, do której wykorzystywane są różne kanały komunikacyjne. Publikowanie informacji na oficjalnej stronie internetowej GIODO oraz *newsletter* jest także w praktyce doskonałą formą rozpowszechniania wiedzy z dziedziny ochrony danych, a zamieszczane tam i ogólnie dostępne opinie, porady, odpowiedzi na pytania dotyczące tematyki ochrony danych, zbiory aktów prawnych z zakresu prawnej ochrony prywatności czy wszelkie aktualności dotyczące tych zagadnień także są realizacją przedstawianego zadania.

Nie bez znaczenia jest fakt organizacji z ramienia Generalnego Inspektora Ochrony Danych Osobowych konferencji i spotkań dających możliwość wymiany informacji z zakresu ochrony danych osobowych wszystkim podmiotom zainteresowanym ową tematyką. Na forum krajowym aktywność i działalność GIODO w zakresie doskonalenia ochrony danych osobowych widoczna jest także poprzez szereg podejmowanych przedsięwzięć, w których aktywnie uczestniczą różne podmioty. Organizowane kampanie edukacyjne i informacyjne (np. Dzień Ochrony Danych Osobowych, Dni Otwarte GIODO), szkolenia i warsztaty dla różnych grup docelowych (firmy i instytucje prywatne i publiczne z różnych sektorów działalności, organizacje krajowe, dzieci i młodzież) mają na celu upowszechnianie podstawowych zasad ochrony prywatności. Uświadamianie o konieczności prowadzenia szkoleń i podnoszenia kwalifikacji jest także ważnym aspektem realizacji przedmiotowego zadania GIODO.

Także obecność GIODO i jego przedstawicieli w mediach, poprzez udział w konferencjach prasowych, programach radiowych i telewizyjnych, jest skuteczną formą

upowszechniania wiedzy z zakresu prawnej ochrony danych szerokiemu gronu odbiorców[1003]. Opracowane przez GIODO materiały edukacyjno-informacyjne publikowane były w prasie codziennej o zasięgu ogólnopolskim („Rzeczpospolita", „Dziennik Gazeta Prawna", „Puls Biznesu"), jak również w ogólnopolskich pismach branżowych („Serwis Prawno-Pracowniczy", „Computerworld", „IT w Administracji") czy na portalach internetowych (lex.pl, Dziennik Internautów).

GIODO aktywnie współpracuje również z wieloma krajowymi firmami i instytucjami, jak chociażby z: Najwyższą Izbą Kontroli, Związkiem Banków Polskich, Państwową Inspekcją Pracy, Polskim Autokefalicznym Kościołem Prawosławnym czy Sekretariatem Konferencji Episkopatu Polski. Celem tej współpracy jest przede wszystkim wymiana doświadczeń w zakresie stosowania przepisów o ochronie danych osobowych, przekazywanie informacji na odnośnie praw i obowiązków tych podmiotów w zakresie ochrony danych osobowych, stosowanie wymaganych zabezpieczeń danych, istnienie ewentualnych zagrożeń w procesach przetwarzania różnych kategorii danych i sposoby im przeciwdziałania, a także popularyzacja stałej konieczności podnoszenia wiedzy z ochrony danych osobowych.

Informacje do pojedynczych odbiorców trafiają zaś zarówno w formie pism jak i ustnych wyjaśnień, udzielanych za pośrednictwem infolinii GIODO czy indywidualnych spotkań interesantów z pracownikami Biura GIODO, w tym zastępcą GIODO, w ramach dyżurów. Dotyczą zwykle udzielania wyjaśnień i wskazówek w zakresie tworzenia i wdrażania przez administratorów danych regulacji i dokumentacji z zakresu danych osobowych. Duży krąg odbiorców informacji z zakresu ochrony danych osobowych zapewniły także publikacje prasowe i książkowe dotyczące ochrony prywatności.

Generalny Inspektor obejmuje też często patronat nad ważniejszymi przedsięwzięciami w zakresie bezpieczeństwa i ochrony informacji, jak konferencje naukowe, konwenty czy kongresy, w których uczestniczy propagując istotę i konieczność ochrony danych osobowych. W zakresie nauki GIODO nawiązuje także coraz prężniej współpracę ze szkołami wyższymi. Taka współpraca jest realizowana w obszarach działalności: naukowo-badawczej, edukacyjnej, promocyjnej i wydawniczej. Instytucje mają możliwość wymiany materiałów o charakterze analitycznym i informacyjnym, dokumentacji prawnej czy innych danych dotyczących form i metod pracy z zachowaniem danych prawnie chronionych.

[1003] Np. w 2012 r. w prasie, radiu, telewizji i Internecie zostało opublikowanych ogółem około 160 materiałów poświeconych zagadnieniom ochrony danych osobowych. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2012*, s. 228.

Wspólnie są organizowane seminaria, konferencje, szkolenia, praktyki studenckie oraz prace naukowe i badawcze z zakresu ochrony danych osobowych.

6. Uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych

Działalność organów ochrony danych osobowych, niezależnie od właściwości przypisanych im przez ustawy krajowe, nie może i nie mieści się już dzisiaj w granicach państwa, stąd konieczne jest dostosowanie reguł ochrony danych osobowych do potrzeb związanych z integracją europejską oraz ze wspólnymi interesami wynikającymi ze współistnienia[1004]. Na tej podstawie zadanie GIODO określone w art. 12 pkt 7 u.o.d.o. jako uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych nabiera coraz nowego znaczenia. Wszystkie aspekty związane z rozwojem technologii, z transgraniczym przepływem danych oraz koniecznością wprowadzania nowych rozwiązań prawnych na tle rozwijającej się rzeczywistości przyczyniają się do konieczności aktywnego działania organu ochrony danych osobowych nie tylko w granicach państwa. Zadanie to jest przede wszystkim realizowane poprzez udział GIODO oraz jego przedstawicieli w pracach grup roboczych, konferencjach, seminariach czy spotkaniach organizowanych w kraju i za granicą, a także w różnych formach współpracy z innymi organami ochrony danych osobowych na forum Unii Europejskiej. W spotkaniach tego typu biorą udział rzecznicy ochrony danych osobowych z Europy, na czele z Europejskim Inspektorem Ochrony Danych, jak i rzecznicy z całego świata, przedstawiciele instytucji UE, rządów państw, eksperci zajmujący się tą problematyką, przedstawiciele świata akademickiego, organizacje pozarządowe i międzynarodowe działające na rzecz praw człowieka, jak i przedstawiciele biznesu[1005].

Zgadzam się z poglądem J. Barty, P. Fajgielskiego i R. Markiewicza, iż „literalna wykładnia tego przepisu może sugerować, iż GIODO jest uprawniony do współdziałania jedynie z organizacjami i instytucjami międzynarodowymi, podczas gdy organy do spraw ochrony danych osobowych innych państw nie mają statusu międzynarodowego, a jedynie narodowy. […] należy jednak w tym zakresie dopuścić wykładnię funkcjonalną i uznać, iż chodzi o szeroko rozumianą współpracę międzynarodową, w tym również współdziałanie z

[1004] Zob. T. Górzyńska, *Kto strzeże prywatności*, „Rzeczpospolita" z 26 maja 1997 r.
[1005] Zob. http://www.giodo.gov.pl/153/j/pl/, https://www.privacyconference2015.org/.

«narodowymi organami ochrony danych osobowych» innych państw”[1006]. W praktyce oznacza to zatem uczestnictwo Generalnego Inspektora w większości najważniejszych przedsięwzięć i spotkań zrzeszających podmioty i organizacje odpowiedzialne za system ochrony danych osobowych na świecie. Taka możliwość wymiany informacji na szczeblu regionalnym lub międzynarodowym jest niezwykle cenną platformą informacyjną w zakresie wszelkich stosowanych rozwiązań i procedur co do ochrony danych.

Zgodnie z brzmieniem art. 12 pkt 7 u.o.d.o. Generalny Inspektor Ochrony Danych Osobowych uczestniczy w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych. Głównym celem takich spotkań są debaty i wspólne propozycje wdrażania rozwiązań proponowanych przez ekspertów w dziedzinie ochrony danych osobowych i prywatności, mających zapewnić jak najlepszy stopień ochrony danych osobowych i prywatności człowieka na świecie.

Do najważniejszych działań w tym zakresie należy udział GIODO w posiedzeniach Grupy Roboczej Art. 29 ds. ochrony danych osobowych (w tym w pracach podgrup tematycznych, np. Podgrupy ds. Międzynarodowych Transferów Danych, ds. Technologii, ds. Kluczowych Postanowień Dyrektywy, ds. E-administracji i Biometrii, ds. Przyszłości Prywatności oraz Podgrupy ds. Granic, Podróży i Egzekwowania Prawa - BTLE), współpraca z rzecznikami ochrony danych innych krajów (w szczególności w ramach Grupy Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, której jest założycielem i w której pełni rolę Sekretariatu) i związany z tym udział w organizowanych cyklicznie Międzynarodowych Konferencjach Rzeczników Ochrony Danych i Prywatności, Wiosennych Konferencjach Europejskich Organów Ochrony Danych oraz w Warsztatach Rozpatrywania Spraw. Z ramienia Rzeczypospolitej Polskiej Generalny Inspektor Ochrony Danych Osobowych jest członkiem Komitetu Konsultacyjnego ds. Konwencji Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (T-PD) i aktywnie uczestniczy w pracach tego podmiotu.

Inne ważne zadania stojące przed polskim organem ds. ochrony danych w ramach współpracy międzynarodowej, związane są z jego udziałem w pracach grup koordynujących nadzór nad SIS II, VIS, CIS oraz IMI, grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac, Systemem Informacji Celnej, a także Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji (tzw. Grupa Berlińska). Ponadto Generalny Inspektor bierze aktywny udział w pracach Wspólnego Organu Nadzorczego nad Europolem (*Joint*

[1006] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 408-409.

Supervisory Body of Europol), a także Wspólnego Organu Nadzorczego właściwego w sprawach ochrony danych osobowych w związku z wykorzystaniem systemu informacyjnego dla odpraw celnych (*Joint Supervisory Authority Customs* - JSA Customs)[1007].

W działalności międzynarodowej Generalnego Inspektora należy również wyróżnić udzielanie przez niego odpowiedzi na napływające z zagranicy pytania dotyczące interpretacji i stosowania przepisów polskiego prawa o ochronie danych osobowych.

[1007] *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013,* s. 347.

ROZDZIAŁ VI
ŚRODKI DZIAŁANIA
GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

1. Uwagi ogólne

Środki działania GIODO można określić jako prawną formę działania tego organu i narzędzia prawne, które ma prawo używać, by skutecznie realizować swoje uprawnienia i zadania zlecone przez u.o.d.o. To prawne kroki i określone formalne procedury i metody, które zostają podjęte przez GIODO w celu ochrony prywatności człowieka.

Do środków działania należy zatem zaliczyć: wydawanie decyzji administracyjnych w sprawach wykonania przepisów o ochronie danych osobowych, rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych oraz uprawnienia egzekucyjne GIODO.

2. Wydawanie decyzji administracyjnych w sprawach wykonania przepisów o ochronie danych osobowych

Przejawem władczych kompetencji Generalnego Inspektora jest przyznanie mu prawa do wydawania decyzji administracyjnych oraz rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych zgodnie z treścią art. 12 pkt 2 u.o.d.o. oraz przepisów innych aktów normatywnych regulujących ochronę danych osobowych[1008]. Wymienione zadania bezpośrednio związane są z praktyką przetwarzania danych osobowych i polegają na realizacji przez Generalnego Inspektora funkcji orzeczniczej[1009]. Zgodnie z wyrokiem NSA z 20 lutego 2003 r., jedynym organem do spraw ochrony danych osobowych jest, w świetle przepisów u.o.d.o., Generalny Inspektor Ochrony Danych Osobowych, który wydaje decyzje w razie stwierdzenia naruszenia przepisów o ochronie tych danych[1010]. W innym wyroku NSA przyjął, zgodnie z treścią rozdziału 2 u.o.d.o., iż jedynym organem

---

[1008] Art. 12 pkt 2 u.o.d.o. jest równocześnie przepisem szczególnym wyznaczającym właściwość GIODO, jeśli chodzi o rozpatrywanie skarg określonego rodzaju, przepisem wyprzedzającym w tej mierze postanowienia art. 229 i art. 230 k.p.a. Por. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 400.

[1009] Jak wskazuje R. Szałowski (*Ochrona…*, s. 43-44), wydawanie decyzji administracyjnych nie jest zadaniem, a stanowi formę realizacji uprawnień i obowiązków GIODO w sytuacjach przewidzianych przez przepisy.

[1010] Wyrok NSA w Gdańsku z dnia 20 lutego 2003 r., II SA/Gd 597/00, niepublikowany.

ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych i że jedynie ten podmiot może się posługiwać środkami administracyjnymi - podejmować decyzje w sprawach dotyczących przetwarzania danych osobowych[1011].

Decyzje wydawane przez Generalnego Inspektora są konsekwencją przeprowadzonego postępowania w sprawie naruszenia przepisów o ochronie danych osobowych (tzw. postępowania nakazowego), które zostało uregulowane aż w pięciu różnych przepisach znajdujących się w rozdziałach 2 i 5 u.o.d.o. (art. 17 ust. 1, art. 18 ust. 1, art. 32 ust. 2 i ust. 3a, art. 35 ust. 2 u.o.d.o.). Decyzje administracyjne wydawane przez GIODO dotyczą zatem: przywrócenia staniu zgodnego z prawem (art. 18 ust. 1 u.o.d.o.), realizacji uprawnień osoby, której dane dotyczą (art. 32 ust. 2 i ust. 3a, art. 35 ust. 2 u.o.d.o.), rejestracji zbiorów danych i wykreślenia zbiorów danych z rejestru (art. 44 ust. 1 i ust. 2, art. 44a u.o.d.o.) oraz zgody na przekazywanie danych do państwa trzeciego (art. 48 u.o.d.o.)[1012].

Władcza kompetencja GIODO do wydawania decyzji administracyjnych nie zawsze jest jednak prawnie dopuszczalna. Ograniczenia zostały sformułowane w u.o.d.o. poprzez wskazanie określonych kategorii danych i celu ich przetwarzania, a także z uwagi na konieczność stosowania w pierwszej kolejności przepisów innych ustaw. Prawo do wydawania decyzji administracyjnych jest uchylone wówczas, gdy chodzi o znajdujące się w zbiorze informacje niejawne (art. 43 ust. 1 pkt. 1 u.o.d.o.), tj. dane, które zostały uzyskane w wyniku prowadzenia czynności operacyjno-rozpoznawczych przez uprawnionych funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego (art. 43 ust. 1 pkt. 1a w zw. z art. 43 ust. 2 u.o.d.o.). Analogicznie ustawodawca odnosi się na mocy art. 43 u.o.d.o. do zbiorów danych dotyczących osób należących do kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego (art. 43 ust. 1 pkt 3 u.o.d.o.). Nie wyłącza to jednak możliwości sprawowania kontroli co do zgodności przetwarzania danych osobowych przez każdy ze wskazanych powyżej podmiotów. Uprawnienie Generalnego Inspektora do wydawania decyzji administracyjnych jest również

[1011] Wyrok NSA z dnia 19 kwietnia 2000 r., II SA 2619/99, „Wokanda”2000, nr 7, s. 43.

[1012] Jak wynika np. ze *Sprawozdania z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013 r*., w 2013 r. Generalny Inspektor wydał 1358 decyzji administracyjnych, tj. o 61 więcej w stosunku do roku 2012, w którym wydanych było 1297 decyzji. Spośród 1358 decyzji wydanych w 2013 r. 504 dotyczyło postępowań rejestrowych, 74 zostało wydanych w związku z przeprowadzonymi kontrolami, 646 wydano na skutek postępowania zainicjowanego skargą, zaś 134 dotyczyło zgody na przekazanie danych do państwa trzeciego. Pośród 1358 decyzji 109 z nich dotyczyło egzekucji administracyjnej.

wyłączone, jeżeli przepisy innych ustaw regulują odrębnie wykonywanie czynności na danych. Wówczas stosuje się przepisy tych ustaw[1013].

Z uwzględnieniem jednak konstytucyjnych gwarancji niezależności przyznanej poszczególnym organom, GIODO nie jest władny wydawać decyzje administracyjne adresowane do sądów i trybunałów w związku z prowadzoną przez nie działalnością orzeczniczą; jego działalność obejmuje tylko tę sferę funkcjonowania sądów i trybunałów, która nie dotyczy niezależności tych organów[1014]. W szczególności chodzi tu o przetwarzanie danych osobowych w związku z działalnością prywatnoprawną sądów i trybunałów, np. zawierania umów prawa cywilnego czy zatrudniania pracowników. GIODO może także wydawać decyzje w sprawach regulowanych prawem publicznym, które wykraczają poza działalność orzeczniczą, jak np. nakazywać udostępnienie listy biegłych sądowych[1015].

W myśl art. 43 ust. 2 Generalny Inspektor nie może wydawać decyzji administracyjnych adresowanych do kościołów czy związków wyznaniowych o uregulowanej sytuacji prawnej w zakresie, w jakim przetwarzają one dane dotyczące osób należących do kościoła lub związku wyznaniowego na własne potrzeby[1016].

Generalny Inspektor nie może wydawać także decyzji administracyjnych adresowanych do podmiotów zgłaszających kandydatów lub listy kandydatów w wyborach na urząd Prezydenta RP, do Sejmu, Senatu i organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, w okresie między dniem zarządzenia wyborów a dniem głosowania, jeżeli decyzje ograniczałyby swobodę działania w tym zakresie (art. 18 ust. 2 u.o.d.o.). Analogicznie jednak, poza wspomnianymi przypadkami, GIODO może w tym okresie wydawać decyzje administracyjne, jeśli działania podmiotu zgłaszającego kandydatów lub listy kandydatów nie mogą być uznane w żadnym wypadku za korzystanie z wolności, np. stanowią przestępstwo[1017].

[1013] W wyroku NSA z dnia 9 listopada 1999 r. (II SAB 153/ 99, niepublikowany) sąd stwierdził, że przepisów u.o.d.o. nie stosuje się, gdy przepisy innych ustaw regulują wykonywanie takich czynności jak usuwanie uchybień lub dokonywanie sprostowań. Wszelkich sprostowań w postępowaniu karnym, w tym także w postępowaniu przygotowawczym, dokonuje organ, który popełnił omyłkę. Ponadto generalny Inspektor uprawniony jest tylko do ochrony danych osobowych wymienianych w tej ustawie, a nienależących do właściwości innych organów. Skarga na bezczynność GIODO w sprawach nienależących do jego właściwości podlega odrzuceniu.

[1014] A. Drozd, *Ustawa…*, s. 108.

[1015] *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2003*, s. 84.

[1016] Generalny Inspektor uznał, że nie jest kompetentny w sprawie wykorzystania przez proboszcza danych osobowych ze zbioru danych dotyczących członków kościoła katolickiego do rozesłania ulotek wyborczych. Zob. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2002*, s. 146-147.

[1017] A. Drozd, *Ustawa….*, s. 109.

Zakres kompetencji władczych Generalnego Inspektora, zgodnie z art. 18 ust. 3 u.o.d.o., obejmuje również przepisy szczególne regulujące odrębnie wykonywanie czynności przez GIODO w razie naruszenia przepisów o ochronie danych osobowych. Przykładem takich regulacji są postanowienia obecne w: ustawie z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych[1018], w ustawie Kodeks postępowania cywilnego, czy w części Kodeksu postępowania cywilnego regulującej zasady prowadzenia postępowania egzekucyjnego[1019]. Takie kompetencje mogą wówczas zostać przyznane organom innym niż Generalny Inspektor.

Jeżeli wyniki kontroli doprowadzą do stwierdzenia naruszenia przepisów o ochronie danych osobowych, na mocy ustawy inspektor jest zobowiązany wystąpić do Generalnego Inspektora o zastosowanie środków z art. 18 u.o.d.o., tj. wydania decyzji nakazującej przywrócenie stanu zgodnego z prawem (nakaz). Zgadzam się z J. Bartą, P. Fajgielskim, R. Markiewiczem, iż przez pojęcie „naruszenia przepisów o ochronie danych osobowych" zawarte w treści art. 18 ust. 1 u.o.d.o., rozumieć należy nie tylko jako naruszenie treści ustawy o ochronie danych osobowych, ale i przepisów dotyczących przetwarzania i ochrony danych zawartych w innych aktach normatywnych"[1020].

Jeżeli organ ochrony danych osobowych wniosku nie odrzuci, zostanie wszczęte postępowanie administracyjne, o czym zostaje poinformowany kontrolowany administrator danych. Uprawnienia GIODO do wydania decyzji administracyjnej są ściśle związane z uprawnieniami kontrolnymi[1021]. W zależności od wyników postępowania Generalny Inspektor może wydać decyzję administracyjną (stosowanie do postanowień art. 18 ust. 1 u.o.d.o.) najdalej idącą w skutkach, tj. nakazującą przywrócenie stanu zgodnego z prawem poprzez usunięcie uchybień (np. przez udzielenie odpowiednich informacji tym, których dane osobowe są przetwarzane), uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych oraz zabezpieczenie danych lub przekazanie ich innym podmiotom (w tym zwrot danych pozyskanych przez podmiot nieuprawniony)[1022]. Generalny Inspektor może nakazać też zastosowanie środków zabezpieczających dane osobowe, wstrzymanie ich transferu za granicę czy usunięcie ich trwale ze zbioru. Oznacza to, że treść

[1018] Dz. U. Nr 98, poz. 1070 z późn. zm.
[1019] GIODO nie jest, co do zasady, właściwy w sprawach przetwarzania danych osobowych przez komorników. Zob. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2000*, s. 56 i 81.
[1020] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 400.
[1021] G. Sibiga, *Postępowanie…*, s. 119.
[1022] Zgodnie z treścią art. 17 ust. 1 u.o.d.o., jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do Generalnego Inspektora o zastosowanie środków, o których mowa w art. 18 u.o.d.o.

decyzji stanowi nakaz przywrócenia stanu zgodnego z prawem, który może dotyczyć konkretnego działania lub zaniechania[1023]. Stosownie do wyroku WSA z 22 stycznia 2004 r.[1024], „orzeczenia wydane w trybie art. 18 ust. 1 ustawy o ochronie danych osobowych powinny spełniać wszystkie wymogi decyzji administracyjnej zgodnie z art. 107 k.p.a. Jednym z tych wymogów jest podane w decyzji elementu rozstrzygnięcia, które powinno być określone w taki sposób, by strona wiedziała, jakie ją obciążają obowiązki lub jakie jej przyznano uprawnienia"[1025].

W sytuacji gdy kontrolowany podmiot kwestionowałby skierowaną do niego decyzję GIODO, ma prawo zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o ponowne rozpatrzenie sprawy (art. 21 ust. 1 u.o.d.o.). Na decyzje wydaną w przedmiocie wniosku o ponowne rozpatrzenie sprawy kontrolowanemu przysługuje następnie skarga do sądu administracyjnego (art. 21 ust. 2 u.o.d.o.).

Adresatem wydanych decyzji administracyjnych, których wykonanie prowadzi do przywrócenia stanu poprzedniego, może być nie tylko administrator danych, lecz także - w trybie art. 31 u.o.d.o. - przetwarzający oraz inny podmiot, jeżeli naruszają oni przepisy o ochronie danych osobowych[1026].

Wszędzie tam, gdzie konieczne jest wykonanie przepisów o ochronie danych osobowych, Generalny Inspektor jest uprawniony do wkroczenia z władczymi uprawnieniami w postaci możliwości wydania decyzji administracyjnej. Wszystkie decyzje wydane przez Generalnego Inspektora na skutek naruszenia przepisów o ochronie danych osobowych powinny spełniać wszelkie formalne wymogi zgodnie z treścią art. 107 k.p.a., który to określa składniki decyzji[1027]. W toku postępowania zmierzającego do wydania decyzji Generalny Inspektor może, na zasadach ogólnych, wydawać postanowienia (art. 123 i n. k.p.a.)[1028].

[1023] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.,* s. 431.
[1024] Wyrok WSA w Warszawie z dnia 22 stycznia 2004 r., II SA/Wa 3498/02, niepublikowany.
[1025] *Ibidem.*
[1026] Nowelizacją u.o.d.o. z dnia 22 stycznia 2004 r. usunięto z art. 18 ust. 1 u.o.d.o. określenie „administratorowi danych". Bez względu jednak na to, czy administrator danych jest podmiotem publicznym czy prywatnym nie ma on żadnych uprawnień władczych, w tym prawa do wydawania decyzji administracyjnych w zakresie ochrony danych osobowych. Zob. Wyrok NSA z 19 kwietnia 2000 r., II SA 2619/99, „Wokanda" 2000, nr 7, s. 43.
[1027] Decyzja administracyjna jest aktem o określonej treści i formie i zgodnie z art. 107 k.p.a. powinna zawierać: oznaczenie organu który ja wydał, datę wydania, oznaczenie strony lub stron, powołanie podstawy prawnej, rozstrzygniecie, uzasadnienie faktyczne i prawne, pouczenie, czy i w jakim trybie służy odwołanie od decyzji, podpis z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do wydania decyzji. Jeżeli od decyzji służy powództwo do sądu powszechnego lub skarga do sądu administracyjnego, to decyzja winna zawierać stosowane pouczenie. Zob. G. Łaszczyca, Cz. Marzysz, A. Matan, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2007, s. 56.
[1028] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 404.

Drugą grupą decyzji administracyjnych, które jest władny wydawać Generalny Inspektor, są decyzje administracyjne wydawane w ramach szczególnych trybów załatwiania żądań osoby fizycznej związanych z przetwarzaniem jej danych osobowych. Ten tryb wydawania decyzji administracyjnych związany jest z przeprowadzeniem postępowania nakazowego na wniosek (na wniosek osoby zainteresowanej - art. 18 ust. 1 u.o.d.o., na wniosek osoby, której dane dotyczą - art. 35 ust. 2 u.o.d.o. i na wniosek administratora danych - art. 35 ust. 2 i ust. 3a u.o.d.o.). Ustawa o ochronie danych osobowych przyjmuje konstrukcję dwuetapowego postępowania w sprawie naruszenia ochrony danych osobowych[1029].

Gdy na wniosek osoby, której dane dotyczą, zostanie wskazane, iż dane są niekompletne, nieprawdziwe, nieaktualne lub zostały zebrane z naruszeniem ustawy, lub są zbędne do realizacji celu, w jakim zostały zebrane, osoba fizyczna kieruje do administratora danych wniosek. Jeśli administrator danych nie uwzględnił jej żądania i nie dopełnił obowiązku ich uzupełnienia, uaktualnienia, sprostowania lub czasowego czy stałego wstrzymania się od przetwarzania tych danych lub ich usunięcia ze zbioru, Generalny Inspektor jest zobowiązany podjąć adekwatne kroki przewidziane przez ustawę. Generalny Inspektor podejmuje działania jednak dopiero wówczas, gdy osoba, której dane dotyczą, wniesie do administratora danych żądanie zaprzestania przetwarzania jej danych w sytuacjach określonych w art. 23 ust. 1 pkt 4 i 5 u.o.d.o. z uwagi na szczególną sytuację tej osoby, a administrator nie zaprzestanie przetwarzania danych, ale przekaże żądanie Generalnemu Inspektorowi w celu wydania rozstrzygnięcia. Z chwilą otrzymania sprawy przez GIODO następuje wszczęcie postępowania administracyjnego na wniosek, które kończy się wydaniem decyzji w indywidualnej sprawie, a z uwagi na rolę organu do spraw ochrony danych osobowych w „sporze" pomiędzy podmiotem danych a administratorem danych używana jest nazwa „postępowanie arbitrażowe"[1030]. Wydana decyzja przez Generalnego Inspektora zawiera jego stanowisko w sprawach zasadności żądania osoby, której dane dotyczą, co do zaprzestania przetwarzania tych danych ze względu na jej szczególną sytuację (art. 32 ust. 2 u.o.d.o.). Wydając stosowaną decyzję, Generalny Inspektor korzysta z nakazów przewidzianych w art. 18 u.o.d.o. Możliwość wydania decyzji administracyjnej zgodnie z treścią art. 18 ust. 1 u.o.d.o przez Generalnego Inspektora, służy ochronie danych osobowych i ma istotne znaczenie dla ochrony interesów osób, których dane dotyczą, jak i interesu

---

[1029] G. Sibiga, *Postępowanie…*, s. 139.
[1030] Zob. W. Zimny, *Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z dnia 25 sierpnia 2001 r.*, „ODO Biuletyn ABI" 2001, nr 21, s. 12.

powszechnego. Podzielam stanowisko M. Sakowskiej, zgodnie z którym środki naprawcze, o których wspomina art. 18 ust. 1 u.o.d.o., korespondują z treścią art. 51 Konstytucji w ten sposób, że działania, które nakazuje podjąć GIODO, niezależnie od ich specyfiki i charakteru służą ochronie prawa do ochrony danych osobowych[1031].

Gdy przeprowadzone zostało postępowanie w przedmiocie wykonania żądania zaprzestania przetwarzania danych osobowych ze względu na szczególną sytuację podmiotu danych (art. 32 ust. 1 pkt 7 w zw. z art. 2 u.o.d.o.)[1032], GIODO wydaje decyzję administracyjną nakazującą zaprzestanie przetwarzania danych (usunięcie danych lub wstrzymanie ich przetwarzania) lub wydaje decyzję stwierdzającą, że żądanie podmiotu danych było bezzasadne.

W przypadku przeprowadzania postępowania w przedmiocie naruszenia zakazu automatyzacji rozstrzygnięć indywidualnych (art. 32 ust. 1 pkt 9 w zw. z art. 3a u.o.d.o.), GIODO wydaje decyzję administracyjną nakazującą ponowne rozpatrzenie sprawy rozstrzygniętej z przekroczeniem zakazu automatyzacji rozstrzygnięć indywidualnych lub niestwierdzającej naruszenia art. 26 u.o.d.o.

Gdy zaś zostało przeprowadzone postępowanie w przedmiocie naruszenia poprawności, kompletności lub legalności przetwarzania danych osobowych (art. 32 ust. 1 pkt 5 w zw. z art. 35 ust. 1 i 2 u.o.d.o.), GIODO wydaje decyzję administracyjną nakazującą przywrócenie stanu zgodnego z prawem lub decyzję administracyjną, na mocy której nakazuje administratorowi danych, na wniosek osoby, której dane dotyczą, dopełnienie obowiązku uzupełnienia, uaktualnienia, sprostowania danych, wstrzymania ich przetwarzania lub usunięcia ze zbioru (art. 35 ust. 2 u.o.d.o.). GIODO może wydać także decyzję stwierdzając, iż nie doszło do naruszenia art. 35 ust. 1 oraz art. 26 ust. 1 u.o.d.o.

W dwóch ostatnich sytuacjach nakazy Generalnego Inspektora będą oczywiście związane z naruszeniem przepisów o ochronie danych osobowych, jednak w przypadku wydania przez Generalnego Inspektora decyzji nakazującej zaprzestanie przetwarzania danych (usunięcie danych lub wstrzymanie ich przetwarzania) lub decyzji stwierdzającej, że żądanie podmiotu danych było bezzasadne, nie musi zachodzić taka przyczyna. Generalny Inspektor może nakazać zaprzestanie przetwarzania danych osobowych nawet w sytuacji, gdyby nie doszło do naruszenia przepisów o ochronie danych osobowych. Jego rola w ramach tego postępowania sprowadza się do oceny, czy zachodzą przesłanki dopuszczalności

---

[1031] M. Sakowska, *Pozycja…*, s. 90.

[1032] Rozróżnienie trzech procedur w zakresie prowadzonych postępowań administracyjnych przez GIODO przyjmuje: G. Sibiga, *Postępowanie…*, s. 159-164.

żądania, a następnie czy podnoszone przez podmiot przyczyny przemawiają za zaprzestaniem przetwarzania danych osobowych[1033].

Także odmowa rejestracji zbioru danych następuje w drodze decyzji administracyjnej i ma ona charakter obligatoryjny (art. 44 ust. 1 u.o.d.o.). Organ rejestracyjny (GIODO) jest zobowiązany do wydania przedmiotowej decyzji w sytuacji, gdy dojdzie do spełnienia chociażby jednej z trzech przesłanek, tj.:

a) nie zostały spełnione wymogi formalne określone w art. 41 ust. 1 u.o.d.o.,

b) przetwarzanie danych narusza podstawowe zasady przetwarzania danych określone w art. 23 - art. 30 u.o.d.o.,

c) urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych wskazanych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Decyzja administracyjna Generalnego Inspektora w przedmiocie odmowy rejestracji zbioru danych osobowych zawiera rozstrzygnięcie dwuelementowe. Pierwszym elementem decyzji jest odmową rejestracji zbioru danych, zaś drugim elementem jest jeden z dwóch wskazanych w art. 44 u.o.d.o. nakazów rejestracyjnych, tj. ograniczenie przetwarzania wszystkich lub niektórych tylko kategorii danych wyłącznie do ich przechowywania albo nakaz zastosowania innych środków, o których mowa w art. 18 u.o.d.o.[1034]. Jest to więc decyzja o dość swobodnym uznaniu ze strony GIODO, dlatego też istota stosowania tego środka przez Generalnego Inspektora powinna odpowiadać zasadzie adekwatności do zaistniałego zagrożenia. Generalny Inspektor jest zobowiązany przestrzegać zasady proporcjonalności działań władczych[1035].

Do momentu uprawomocnienia się decyzji w przedmiocie odmowy rejestracji zbioru (lub nadania jej rygoru natychmiastowej wykonalności) administrator może swobodnie przetwarzać dane zwykłe na podstawie zgłoszenia (korzysta więc ze swoistego „kredytu zaufania"). Wydawany jednocześnie z odmową rejestracji nakaz wstrzymania przetwarzania danych lub ich usunięcia ze zbioru podlega natychmiastowemu wykonaniu. Jest to jeden z wyjątków od zasady, iż decyzja nieostateczna nie ulega wykonaniu przed upływem terminu

---

[1033] *Ibidem,* s. 162.
[1034] B. Konieczna, *Decyzje*…, s. 250.
[1035] X. Konarski, G. Sibiga, *Zmiany…, s. 554.*

do wniesienia odwołania, a jego wniesienie wstrzymuje wykonanie tej decyzji (art. 130 § 1 i 2 k.p.a.). Z takimi wyjątkami mamy do czynienia, jeśli organ nadaje decyzji rygor natychmiastowej wykonalności na podstawie art. 108 k.p.a. oraz gdy z mocy odrębnej ustawy podlega ona natychmiastowemu wykonaniu[1036]. Takim przykładem szczególnego rozwiązania jest właśnie art. 44 ust. 3 u.o.d.o., który zobowiązuje Generalnego Inspektora do zawarcia w decyzji klauzuli natychmiastowej wykonalności, która jest obligatoryjnym elementem decyzji, a GIODO nie może badać potrzeby jej zastosowania. Niedopuszczalne jest po wydaniu decyzji nadanie jej klauzuli wykonalności w drodze postanowienia na podstawie art. 108 § 2 k.p.a.

Wydanie przez GIODO decyzji odmownej rejestracji zbioru nie wyklucza jego ponownego zgłoszenia do rejestracji. Warunkiem zarejestrowania zbioru jest jednak usunięcie przez administratora danych wszystkich wcześniejszych uchybień, które poprzednio były podstawą odmowy rejestracji. W razie ponownego zgłoszenia zbioru danych do rejestracji, ich przetwarzanie zgodnie z art. 44 ust. 5 u.o.d.o. może mieć miejsce dopiero po zarejestrowaniu. Zarówno złożenie wniosku o ponowne rozpatrzenie sprawy, jak i ponowne zgłoszenie zbioru danych do rejestracji nie wstrzymuje wykonalności nakazu Generalnego Inspektora, o którym mowa w art. 44 ust. 3 u.o.d.o. Oznacza on również zakaz prowadzenia zbioru danych do czasu ewentualnego uchylenia decyzji przez organ rejestracyjny, zarejestrowania zbioru po jego ponownym zgłoszeniu lub wydania odpowiedniego orzeczenia NSA[1037].

Także wykreślenie zbioru danych z rejestru następuje w formie decyzji administracyjnej wydanej przez Generalnego Inspektora Ochrony Danych Osobowych, w przypadku gdy zaprzestano przetwarzania danych w zarejestrowanym zbiorze lub rejestracji dokonano z naruszeniem prawa (art. 44a u.o.d.o.)[1038]. Przez zaprzestanie przetwarzania danych w zbiorze należy rozumieć usunięcie danych ze zbioru lub zniszczenie danych wraz zawartością, co powinno mieć charakter faktycznego i trwałego zakończenia dokonywania jakichkolwiek czynności na danych osobowych[1039].

Sformułowanie przesłanek będących podstawą do wykreślenia zbioru danych z rejestru prowadzi do wniosku, że Generalny Inspektor może wykreślić zbiór z rejestru na

---

[1036] G. Sibiga, *Postępowanie…*, s. 190.
[1037] E. Kulesza, G. Sibiga, *Wykonanie…,* s. 124.
[1038] Uprawnienie to zostało nadane GIODO nowelizacją u.o.d.o. z 2004 r. Zob. Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych.
[1039] Samo przechowywanie jednak danych jest ich przetwarzaniem.

wniosek administratora, ale i z urzędu[1040]. Wykreślenie zbioru danych z rejestru w przypadku zaprzestania przetwarzania danych osobowych, uzależnione jest od faktu poinformowania o tym Generalnego Inspektora. W przypadku gdy rejestracji zbioru dokonano z naruszeniem prawa, nie ma podstawy do wznowienia postępowania, ani stwierdzenia nieważności decyzji[1041].

Postępowanie w sprawie wydania zgody na przekazywanie danych do państwa trzeciego[1042] zakończone jest także wydaniem decyzji przez Generalnego Inspektora zezwalającej na przekazywanie danych osobowych do państwa trzeciego lub decyzji odmawiającą ich przekazywanie, po uprzednim złożeniu wniosku przez administratora danych[1043]. Decyzja zezwalająca na przekazywanie danych do państwa trzeciego ma charakter uznaniowy i powinna zawierać wszystkie okoliczności sprawy. W przypadku wydania przez GIODO decyzji odmownej co do przekazania danych do państwa trzeciego, administratorowi danych przysługuje prawo złożenia wniosku o ponowne rozpatrzenie sprawy, a w przypadku otrzymania ponownie negatywnej decyzji, zaskarżyć ją może do sądu administracyjnego (art. 21 ust. 1 i ust. 2 u.o.d.o.).

3. Rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych

Kolejnym przysługującym Generalnemu Inspektorowi uprawnieniem jest rozpatrywanie skarg[1044]. Proces ten opiera się, zgodnie z ogólną wskazówką zawartą w art. 22 u.o.d.o., na zastosowaniu przepisów kodeksu postępowania administracyjnego, co odnieść należy również do stosowania przepisów wykonawczych rozporządzenia Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków[1045].

[1040] T. Szewc, *Publicznoprawna…*, s. 100.
[1041] G. Sibiga, *Postępowanie…*, s. 179.
[1042] Na mocy art. 47 ust. 1 u.o.d.o. może nastąpić przekazanie danych osobowych do państwa trzeciego (stosownie do definicji ustawowej - art. 7 pkt 7 u.o.d.o., państwo trzecie to państwo nienależące do Europejskiego Obszaru Gospodarczego - EOG, które tworzą państwa członkowskie UE oraz Norwegia, Islandia i Lichtenstein), jeżeli docelowe państwo zapewnia gwarancje ochrony danych osobowych na swoim terytorium, przynajmniej takie, jakie obowiązuje na terytorium RP.
[1043] Gdy przesyłanie danych wynikać będzie z obowiązku nałożonego na administratora danych na mocy przepisów prawa lub na mocy postanowień ratyfikowanej umowy międzynarodowej, wówczas zostaje wyłączone obowiązywanie art. 47 ust. 1 u.o.d.o. (art. 47 ust. 2 u.o.d.o.).
[1044] W 2013 r. do Biura GIODO wpłynęło 1879 skarg dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2013, liczba ta uległa zwiększeniu o 286. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013, s. 71.*
[1045] Dz. U. Nr 5, poz. 46 z późn. zm.

Skargę do Generalnego Inspektora może złożyć każdy, nie tylko osoba, której dane dotyczą[1046]. Złożenie skargi nie ogranicza w żadnej mierze korzystania z innych uprawnień przewidzianych ustawą, w tym z art. 32 u.o.d.o. Przedmiotem skargi może być w szczególności zaniedbanie lub nienależyte wykonywanie zadań przez właściwe organy albo przez ich pracowników, naruszenie praworządności lub słusznych interesów obywateli, a także przewlekłe lub biurokratyczne załatwianie spraw (art. 227 k.p.a.)[1047]. Skarga złożona do Generalnego Inspektora dotyczyć więc może np. niedopełnienia przez organ przetwarzający dane obowiązków informacyjnych wskazanych w art. 24 i art. 25 u.o.d.o., braku dbałości administratora o merytoryczną poprawność przetwarzanych danych, przetwarzania danych w innym celu niż ten, dla którego zostały zebrane, bezpodstawnego nieudostępniania danych, jak i bezprawnego udostępniania danych ze zbioru innym osobom, utrudnianie sprawowania kontroli (art. 32 u.o.d.o.) czy niewłaściwego zabezpieczenia danych[1048].

Skargi mogą być wnoszone pisemnie, za pośrednictwem telefaksu, poczty elektronicznej, a także ustnie do protokołu. Przyjmowanie skarg powierza się Departamentowi Orzecznictwa Legislacji i Skarg Biura GIODO (DOLiS).

Każda ze skarg analizowana jest na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego i ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej[1049]. W sytuacji gdy skarga nie spełnia warunków wymaganych przez ww. przepisy prawa, organ ochrony danych osobowych wzywa wnioskodawcę do uzupełnienia braków formalnych[1050]. W przypadku tych, które je spełniały, Generalny Inspektor Ochrony Danych Osobowych wszczyna postępowania administracyjne. Jeżeli w jego toku stwierdza naruszenie przepisów ustawy o ochronie danych osobowych, wydaje decyzje administracyjne i zgodnie z art. 18 u.o.d.o. nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności: 1) usunięcie uchybień; 2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych; 3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane

---

[1046] Np. skargę na udostępnienie danych osobowych może złożyć spółka w razie udostępniania danych osobowych członka zarządu tej spółki.

[1047] Wszystkie wspomniane wcześniej w pracy wyłączenia dotyczące wydawania decyzji administracyjnych przez Generalnego Inspektora odnoszą się także do rozpatrywania skarg.

[1048] Zob. zarządzenie nr 2/2012 Generalnego Inspektora Ochrony Danych Osobowych z dnia 4 stycznia 2012 r. w sprawie przyjmowania i rozpatrywania skarg i wniosków w Biurze Generalnego Inspektora Ochrony Danych Osobowych; dostępne na str. http://www.giodo.gov.pl/1520133/j/pl/

[1049] Dz. U. Nr 225, poz. 1635 z późn. zm.

[1050] W związku z nieuzupełnieniem braków formalnych, w 2013 r. 129 skarg zostało zwróconych do wnioskodawców. Wiele skarg zostało również pozostawionych bez rozpoznania. Zob. *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013,* s. 72.

osobowe; 4) wstrzymanie przekazywania danych osobowych do państwa trzeciego; 5) zabezpieczenie danych lub przekazanie ich innym podmiotom; 6) usunięcie danych osobowych.

W sytuacji gdy GIODO nie stwierdza naruszenia prawa, wydaje decyzje administracyjne odmawiające uwzględnienia wniosku.

Biorąc pod uwagę treść skarg kierowanych do Generalnego Inspektora wskazać można, że dotyczyły one 11 kategorii zagadnień: administracji publicznej, bezpieczeństwa publicznego, sądów, prokuratury i komorników, organizacji społecznych, banków i innych instytucje finansowe, zagadnień związanych z Internetem, marketingiem, mieszkalnictwem, oświatą i szkolnictwem wyższym, służbą zdrowia, ubezpieczeniami społecznymi, majątkowymi i osobowymi, telekomunikacją, zatrudnieniem, windykacją i spraw innych[1051]. Jak wynika z działalności sprawozdawczej GIODO, w porównaniu z poprzednimi latami można zauważyć stopniowy wzrost liczby kierowanych skarg (w 2008 wpłynęło 986 skarg, w 2009 r. – 1049, w 2010 r. – 1114 , w 2011 – 1271, a w 2012 r. – 1593)[1052]. Taki stan rzeczy najprawdopodobniej jest spowodowany zwiększeniem świadomości społeczeństwa w zakresie ochrony danych osobowych i aktywności w dochodzeniu praw przez dysponentów danych. Także fakt zaskarżania decyzji administracyjnych obrazuje, że strony poinformowane są o przysługujących im narzędziach prawnych, wykorzystując je do weryfikacji zasadności rozstrzygnięć Generalnego Inspektora[1053].

4. Uprawnienia egzekucyjne GIODO

Na skutek noweli z 29 października 2010 r. wprowadzonej do ustawy o ochronie danych osobowych włączono w zakres działań Generalnego Inspektora prowadzenie egzekucji administracyjnej. Zgodnie z nowym brzmieniem art. 12 ust. 3 u.o.d.o. GIODO ma możliwość stosowania środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (w skrócie u.p.e.a.)[1054] jako

[1051] *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013,* s. 71.
[1052] *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2012,* s. 300.
[1053] *Ibidem*, s. 302.
[1054] Dz. U. z 2005 r. Nr 229, poz.1954 z późn. zm. W projekcie ustawy nowelizującej przewidziano nawet wyposażenie GIODO w uprawnienia do nakładania kar pieniężnych w wysokości do 100 tys. euro za niewykonanie jego decyzji, jednak proponowane rozwiązanie zostało poddane powszechnej krytyce i nie uzyskało ostatecznie aprobaty wśród członków Sejmu. Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 405.

zapewnienie wykonywania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji, o których mowa w art. 12 pkt 2 u.o.d.o.

Uprawnienie Generalnego Inspektora do prowadzenia postępowania egzekucyjnego nie były do tej pory przedmiotem pogłębionych analiz, gdyż wydawało się oczywiste, że wydawane przez GIODO decyzje administracyjne podlegają egzekucji administracyjnej. Uznawano milcząco, że jest to właściwy tryb do prowadzenia egzekucji obowiązków wynikających z wszelkich decyzji administracyjnych[1055]. Pogląd taki był prezentowany w wielu opiniach oraz podzielały go sądy administracyjne[1056]. W wyroku z 3 czerwca 2004 r. WSA w Warszawie stwierdził, że „w przypadku decyzji wydawanych przez Generalnego Inspektora Ochrony Danych osobowych nakaz usunięcia danych osobowych nie może budzić żadnych wątpliwości, zwłaszcza w aspekcie wykonalności. Osnowa decyzji musi być zatem sformułowana w taki sposób, aby następnie możliwe było dobrowolne wykonanie decyzji lub wykonanie jej z zastosowaniem środków egzekucji administracyjnej” [1057].

Odmienne stanowisko reprezentował jednak Generalny Inspektor, który nie podejmował postępowania egzekucyjnego w przypadku niewykonywania obowiązków nałożonych decyzją GIODO, a ograniczał się jedynie do składania w prokuraturze zawiadomienia o popełnieniu przestępstwa. GIODO stwierdzał, iż jest to jedyna prawnie dopuszczalna sankcja w przypadku naruszenia ustawy o ochronie danych osobowych.

Przez kilkanaście lat obowiązywania przepisów opisywanej ustawy GIODO nie posiadał wprost wyrażonych w ustawie uprawnień egzekucyjnych, dlatego nie mógł doprowadzać do przymusowego wykonania obowiązków (nakazów) nałożonych w wydanych przez niego decyzjach. Taki stan prawny nie wpływał korzystnie na skuteczność i całokształt uprawnień GIODO co do wykonalności wydawanych przez niego decyzji.

Art. 2 § 1 pkt 10 u.p.e.a. przewiduje egzekucję obowiązków o charakterze niepieniężnym pozostających we właściwości organów administracji rządowej i samorządu terytorialnego lub przekazanych do egzekucji administracyjnej na podstawie przepisu szczególnego. Generalny Inspektor nie należy jednak do organów administracji rządowej ani do organów samorządu terytorialnego, a jest organem państwowym wykonującym zadania z

---

[1055] P. Przybysz, *Kompetencje egzekucyjne Generalnego Inspektora Ochrony Danych Osobowych oraz postępowanie egzekucyjne prowadzone przez organ ochrony danych osobowych*, „Monitor Prawniczy” 2011, nr 3, s. 30.

[1056] Zob. X. Konarski w opinii prawnej dołączonej do stanowiska Polskiej Izby Informatyki i Komunikacji z 18 lutego 2008 r. do przedłożonego Sejmowi prezydenckiego projektu ustawy o zmianie ustawy o ochronie danych osobowych z 21 grudnia 2007 r., druk sejmowy nr 488 z 21 grudnia 2007 r., s. 90, dostępny na stronie: http://ww.sejm.gov.pl.

[1057] Zob. Wyrok WSA w Warszawie z dnia 3 czerwca 2004 r. , II SA/Wa 225/04, niepublikowany.

zakresu administracji publicznej w sposób niezależny od Rady Ministrów[1058]. Z tego względu niezbędne było uchwalenie szczegółowego przepisu, by Generalny Inspektor mógł zostać wyposażony w kompetencje egzekucyjne i by mógł egzekwować wykonanie obowiązków nakładanych decyzjami GIODO. Generalny Inspektor wyposażony więc został w nowe uprawnienie, polegające na zapewnieniu wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji wydanych przez GIODO w sprawach ochrony danych osobowych. W związku z tym GIODO ma możliwość użycia środków egzekucyjnych określonych w u.p.e.a. i prowadzenia postępowania egzekucyjnego w przedmiotowych sprawach.

Na skutek wspomnianej nowelizacji ustawy o ochronie danych osobowych GIODO uzyskał uprawnienia organu egzekucyjnego w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym. W u.p.e.a. postanowiono dokonać zmiany dodając do zawartego w art. 2 § 1 wyliczenia obowiązków poddanych egzekucji w pkt 12 nową kategorię obowiązków o charakterze niepieniężnym, tj. obowiązki z zakresu ochrony danych osobowych nakładanych w drodze z decyzji GIODO. Co więcej, w art. 20 § 2 Generalny Inspektor został dodany do kręgu podmiotów uprawnionych do działania jako organ egzekucyjny w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym[1059].

Na drogę egzekucji administracyjnej zostały przekazane obowiązki wynikające z decyzji wydawanych przez Generalnego Inspektora, jednak nie wszystkie decyzje wydawane przez ten organ mogą stać się przedmiotem egzekucji. Egzekucja może być prowadzona, gdy z decyzji wynika obowiązek, tj. na adresacie decyzji ciąży konieczność zachowania się w określony sposób. Egzekucja nie może być prowadzona, jeśli decyzja wywołuje określone skutki z chwilą jej wydania, bez potrzeby dokonywania dalszych czynności przez adresata tej decyzji[1060]. Dla przykładu decyzja odmawiająca rejestracji zbioru danych nie wymaga egzekucji, gdyż wywiera skutki prawne niezależnie od zachowania się adresata takiej

---

[1058] P. Przybysz, *Kompetencje…,* s. 30.

[1059] Art. 20 §2 u.p.e.a. otrzymał brzmienie: „Ponadto w przypadkach określonych szczególnymi przepisami jako organ egzekucyjny w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym działa każdy organ Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu lub Straży Granicznej, Generalny Inspektor Ochrony Danych Osobowych, organ Państwowej Inspekcji Pracy wydający decyzję w pierwszej instancji, organ straży pożarnej kierujący akcją ratowniczą, a także inne organy powołane do ochrony spokoju, bezpieczeństwa, porządku, zdrowia publicznego lub mienia społecznego”.

[1060] P. Przybysz, *Kompetencje…,* s. 33.

decyzji[1061]. Przedmiotem egzekucji może być jednak nakaz przywrócenia stanu zgodnego z prawem czy nakaz zaprzestania przetwarzania danych.

Obowiązkiem Generalnego Inspektora jest czuwanie nad tym, by wydawane przez niego decyzje były wykonywane dobrowolnie, a wszczynanie postępowania egzekucyjnego w administracji odbywało się tylko wobec tych, którzy nie wykonują dobrowolnie obowiązków zawartych w tytule egzekucyjnym. Zagadnienia kontroli wykonywania obowiązków nie zostały unormowane na gruncie u.p.e.a., z wyjątkiem upominania zobowiązanego (art. 15 u.p.e.a.). Celem zatem GIODO działającego w charakterze wierzyciela jest doprowadzenie do zastosowania środków egzekucyjnych wobec adresata decyzji uchylającego się do dobrowolnego wykonywania nałożonych obowiązków (art. 6 § 1 u.p.e.a.)[1062]. W przypadku niedopełnienie tego obowiązku przez GIODO istnieje możliwość wniesienia skargi na bezczynność tego organu przez każdego, czyj interes prawny lub faktyczny został naruszony w wyniku niewykonania obowiązku. Skargę taką może też wnieść organ zainteresowany wykonaniem obowiązku (art. 6 § 1a u.p.e.a.).

Istotne znaczenie z punktu widzenia skuteczności egzekucji ma także obowiązek Generalnego Inspektora jako organu egzekucyjnego, by doprowadził on do wyegzekwowania obowiązku. Sankcją za niewykonanie tego obowiązku jest ewentualna odpowiedzialność odszkodowawcza GIODO wobec każdego, kto poniósł szkodę wskutek prowadzenia postępowanie egzekucyjnego w administracji w opieszały i nieskuteczny sposób[1063]. Ten, kogo dane były przetwarzane w sposób niezgodny z prawem i kto poniósł szkodę w wyniku niewyegzekwowania przez GIODO obowiązków wynikających z decyzji nakazującej usuniecie naruszenia prawa, może wnieść do sądu powszechnego pozew przeciwko Generalnemu Inspektorowi o odszkodowanie[1064].

Obowiązkiem Generalnego Inspektora prowadzącego postępowanie egzekucyjne w administracji na zasadach ogólnych jest pisemne upomnienie zobowiązanego. Po upływie 7 dni od doręczenia zobowiązanemu upomnienia wierzyciel powinien wystawić tytuł

[1061] *Ibidem, s. 32.*

[1062] Równoczesne wykonywanie przez GIODO funkcji wierzyciela i organu egzekucyjnego nie stanowi *novum* w postępowaniu egzekucyjnym w administracji, a rozwiązanie takie jest typowe dla większości prowadzonych postępowań egzekucyjnych. Tym bardziej zatem wprowadzenie tego uprawnienia w zakres kompetencji GIODO nie powinno budzić żadnych wątpliwości.

[1063] Zob. Wyrok SN z dnia 2 czerwca 1972 r., I CR 42/72, OSPiKA 1973, nr 7-8, poz. 152 z glosą M. Nestorowicza.

[1064] Jeżeli przyjąć, że obowiązki nakładane przez GIODO mogły być egzekwowane na drodze decyzji administracyjnej przed wejściem w życie nowelizacji ustawy o ochronie danych osobowych z 2010 r., to GIODO ponosi też odpowiedzialność odszkodowawczą za szkody spowodowane niewyegzekwowaniem decyzji wydanych przed tą datą. Zob. P. Przybysz, *Kompetencje…,* s. 33.

wykonawczy oraz wniosek do organu egzekucyjnego o wszczęcie postępowania egzekucyjnego. Jeśli organ egzekucyjny jest jednocześnie wierzycielem, to wystawia tytuł wykonawczy i z urzędu kieruje go do egzekucji. Obowiązek zawarty w tytule wykonawczym musi być taki sam jak w treści decyzji wydanej przez Generalnego Inspektora, która jest podstawą do wydania owego tytułu wykonawczego. Organ, który wydał decyzję, może wydając postanowienie wyjaśnić treść tej decyzji na żądanie organu egzekucyjnego lub strony (art. 113 § 3 k.p.a). W związku z tym jeśli GIODO wystawiając tytuł wykonawczy uzna za celowe doprecyzowanie jej treści i obowiązku, to powinien wydać postanowienie w sprawie wyjaśnienia treści decyzji[1065].

U.p.e.a. przewiduje również uproszczony tryb egzekucji, który może być stosowany przez organy egzekucyjne z art. 20 § 2 u.p.e.a., w tym przez Generalnego Inspektora. W przypadkach określonych w przepisach szczególnych istnieje możliwość wydania ustnie polecenia określonego działania i przystąpienia do jego egzekwowania z pominięciem wystawiania pisemnego tytułu wykonawczego i bez doręczenia zobowiązanemu postanowienia o zastosowaniu środka egzekucyjnego. Zgodnie z treścią art. 117 u.p.e.a. przesłania zastosowania trybu uproszczonego egzekucji jest stwierdzenie, że zwłoka w wykonaniu obowiązku groziłaby niebezpieczeństwem dla życia lub zdrowia ludzkiego albo ciężkimi szkodami dla gospodarstwa narodowego lub jeżeli wymaga tego szczególny interes społeczny. Rozwiązanie takie wprowadzono na potrzeby organów powołanych do ochrony spokoju, bezpieczeństwa, porządku, zdrowia publicznego lub mienia społecznego, które w toku prowadzonej akcji zmuszone są działać w niestandardowy sposób, by zachować skuteczność działania. Do specyfiki sytuacji dostosowano również rodzaj środków egzekucyjnych, które mogą być stosowane w uproszczonej egzekucji, ograniczając je do wykonania zastępczego, odebrania rzeczy ruchomej i przymusu bezpośredniego. W literaturze wskazuje się także, że w przypadku prowadzenia postępowania egzekucyjnego w trybie uproszczonym, należy odstąpić od pisemnego upomnienia zobowiązanego, ponieważ tylko w takim przypadku możliwa będzie realizacja celu tej regulacji prawnej, tj. szybka egzekucja nałożonego obowiązku[1066].

Pomimo wyposażenia Generalnego Inspektora w kompetencje egzekucyjne, prowadzenie przez niego uproszczonego postępowania egzekucyjnego budzi wątpliwości. W treści art. 12 ust. 3 u.o.d.o. brak jest wskazania przypadków, w których GIODO mógłby

---

[1065] *Ibidem,* s. 32.
[1066] R. Hauser, Z. Leoński, A. Skoczylas, *Komentarz do ustawy o postępowaniu egzekucyjnym w administracji,* Warszawa 2008, s. 527.

prowadzić ten rodzaj postępowania egzekucyjnego. Dodatkowo art. 20 2 u.p.e.a. nie stanowi samodzielnej podstawy prawnej do prowadzenia postępowania egzekucyjnego, lecz odsyła do przepisów szczególnych, które określają przypadki, kiedy możliwe jest prowadzenie uproszczonej egzekucji. Jak słusznie zauważył P. Przybysz, „najprawdopodobniej istnieje albo luka w prawie i nie ma normy określającej przypadki, w których GIODO może prowadzić uproszczone postępowanie egzekucyjne, albo GIODO może we wszystkich przypadkach prowadzić takie postępowanie"[1067].

Analizując uprawnienia Generalnego Inspektora w zakresie postępowania egzekucyjnego należałoby zwrócić uwagę także na rodzaj środków egzekucyjnych, które może on stosować realizując przedmiotowe uprawnienia. Użycie środków egzekucyjnych jest możliwe wraz z rozpoczęciem pierwszej czynności egzekucyjnej, co następuje po doręczeniu zobowiązanemu odpisu tytułu wykonawczego oraz udzieleniu mu stosownych pouczeń.

Spośród przewidzianych przez u.p.e.a. środków egzekucyjnych dotyczących obowiązków o charakterze niepieniężnym typowym środkiem, który może zastosować GIODO, jest grzywna w celu przymuszenia[1068]. Jak słusznie wskazują J. Barta, P. Fajgielski i R. Markiewicz, „uwzględniając specyfikę obowiązków wynikających z decyzji GIODO, raczej […] trudno sobie wyobrazić stosowanie innych środków egzekucyjnych takich jak np. wykonanie zastępcze czy przymus bezpośredni"[1069]. W literaturze przedmiotu prezentowane jest także stanowisko odrębne, zgodnie z którym środek egzekucyjny jak wykonanie zastępcze można wykorzystywać we wszystkich postępowaniach egzekucyjnych prowadzonych przez GIODO[1070]. W moim przekonaniu specyfika wykonania zastępczego[1071] czy przymusu bezpośredniego[1072] wskazuje, iż utrudnione byłoby określenie konkretnych

---

[1067] P. Przybysz, *Kompetencje…,* s. 32

[1068] Ustawa o postępowaniu egzekucyjnym w administracji przewiduje następujące sposoby egzekucji tego typu obowiązków: grzywnę w celu przymuszenia, wykonanie zastępcze, odebranie rzeczy ruchomej, odebranie nieruchomości, opróżnienie lokali i innych pomieszczeń, przymus bezpośredni. Szerzej na ten temat: R. Hauser, Z. Leoński, A. Skoczylas, *Komentarz…*, s. 527 i n.

[1069] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 406.

[1070] P. Przybysz, *Kompetencje…,* s. 33. Autor stoi na stanowisku, iż w przypadku uznania za dopuszczalne prowadzenia przez GIODO uproszczonej egzekucji, mógłby stosować on z mocy art. 17 u.p.e.a. wyłącznie trzy środki egzekucyjne: wykonanie zastępcze, odebranie rzeczy ruchomej i przymus bezpośredni. GIODO prowadzić postępowanie egzekucyjne na zasadach ogólnych mógłby stosować także inne środki, tj. grzywnę w celu przymuszenia i odebranie rzeczy ruchomej. Charakter nakładanych przez GIODO obowiązków nie stoi na przeszkodzie zastosowaniu środka egzekucyjnego w postaci wykonania zastępczego i to we wszystkich postępowaniach egzekucyjnych prowadzonych na zasadach ogólnych oraz w trybie uproszczonym. Co więcej wskazuje, iż GIODO prowadząc egzekucję w trybie uproszczonym powinien najpierw zastosować wykonanie zastępcze, a następnie - w razie potrzeby - przymus bezpośredni.

[1071] Prowadzi bezpośrednio do wykonania obowiązku, jednak można go stosować wyłącznie wówczas, gdy przedmiotem egzekucji są czynności, które może dokonać każdy, a nie wyłącznie zobowiązany.

[1072] To specyficzny środek egzekucyjny, który polega albo na użyciu siły fizycznej albo groźby jej użycia tak, by w zobowiązanym przełamać opór przeszkadzający mu w wykonaniu nałożonego na niego obowiązku. Jest

działań, które mógłby podjąć Generalny Inspektor w celu wykonania przez zobowiązanych treści jego decyzji. Środki te w mojej opinii nie są adekwatne do egzekwowania wykonalności decyzji GIODO, a to głównie z uwagi na charakter obowiązków wynikających z tych decyzji.

Decyzją Generalnego Inspektor mogą być nakładane kary pieniężne na podmioty niewykonujące decyzji GIODO. Zakres zastosowania tego środka egzekucyjnego jest szeroki, gdyż może być on stosowany w celu przymuszenia do wykonania obowiązku znoszenia lub zaniechania albo obowiązku wykonania określonej czynności. Grzywna jest to pewnego rodzaju środek motywujący do dobrowolnego wykonania ciążącego na podmiotach obowiązku wykonania decyzji administracyjnej GIODO, a może być zastosowana w stosunku do wszystkich obowiązków nakładanych przez Generalnego Inspektora. Z punktu widzenia organu egzekucyjnego, jest to środek łatwy do zastosowania, gdyż jego stosowanie sprowadza się do wystawienia przez organ egzekucyjny postanowienia o zastosowaniu grzywny w celu przymuszenia, a w przypadku nieziszczenia grzywny sporządzenia tytułu wykonawczego i skierowania go do właściwego urzędu skarbowego wraz z wnioskiem o wszczęcie egzekucji[1073].

Wysokość takiej grzywny w stosunku do osoby fizycznej wynosi maksymalnie 10 000 zł, zaś w stosunku do osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej 50 000 zł, jednak w przypadku wielokrotnego nakładania grzywien w jednym postępowaniu egzekucyjnym ich łączna kwota nie może przekraczać: 50 000 zł w odniesieniu do osób fizycznych oraz 200 000 zł w odniesieniu do osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej[1074]. Grzywnę można nakładać kilkakrotnie, dlatego tytuł wykonawczy powinien obejmować wszystkie nałożone grzywny[1075].

W razie wykonania jednak obowiązku określonego w tytule wykonawczym nałożone, a nieziszczone lub nieściągnięte grzywny w celu przymuszenia podlegają na wniosek zobowiązanego umorzeniu (art. 125 u.p.e.a.), natomiast na wniosek zobowiązanego, który wykonał obowiązek, grzywny uiszczone lub ściągnięte w celu przymuszenia mogą być w uzasadnionych przypadkach zwrócone w wysokości 75% lub w całości (art. 126 u.p.e.a.).

---

zwykle używany jako samoistny środek egzekucyjny, gdy jest egzekwowany obowiązek opuszczenia nieruchomości (lokalu, pomieszczenia), wydania rzeczy czy zaniechania czynności.

[1073] P. Przybysz, *Kompetencje…,* s. 33.

[1074] http://www.giodo.gov.pl/560/id_art/3973/j/pl/.

[1075] P. Przybysz, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2010, s. 136.

Wyposażenie Generalnego Inspektora w nowe kompetencje o charakterze egzekucyjnym powinno przyczynić się do lepszej wykonalności wydawanych przez niego decyzji. GIODO nareszcie uzyskał środek sprawczy do egzekwowania wykonalności swoich decyzji. Oznacza to, że istnieje realna szansa na faktyczne wykonywanie przez zobowiązane podmioty obowiązków wskazanych w treści decyzji, a nie tylko statyczne formułowanie przedmiotowych decyzji bez istnienia jakichkolwiek mechanizmów i środków monitorowania i przymuszania do ich wykonalności.

ZAKOŃCZENIE

Ochrona prywatności człowieka jest w Polsce przedmiotem wielu regulacji prawnych, a jedną z najważniejszych na przestrzeni lat stała się ustawa o ochronie danych osobowych. Trudno jest przecenić, z punktu widzenia ochrony praw i wolności jednostki, wartość i znacznie tej ustawy. W stylizacji jej postanowień dostrzec można starania ustawodawcy uczynienia wszystkiego, aby rodzime regulacje czyniły zadość standardom międzynarodowym i europejskim oraz założeniu racjonalnego prawodawcy w kształtowaniu dobrego prawa. Ustawa ta po raz pierwszy skonkretyzowała prawa obywateli do ochrony dotyczących ich danych osobowych oraz ustanowiła instrumenty umożliwiające realizację ich prawa do prywatności.

Analizując rozwiązania wprowadzone ustawą o ochronie danych osobowych należałoby stwierdzić, iż na szczególne uznanie zasługują instytucjonalne rozwiązania stworzone w celu ochrony prywatności jednostki, stanowiące *novum* w krajowym systemie prawnym. Powołanie instytucji Generalnego Inspektora Ochrony Danych Osobowych w Polsce stało się niewątpliwie realną gwarancją przestrzegania i realizowania praw i obowiązków związanych z ochroną prywatności jednostki oraz dało w praktyce możliwość zapewnienia należytej ochrony jej prywatności. Realizacja postulatu stworzenia zinstytucjonalizowanego mechanizmu ochrony wymusiła kreację organu, którego głównym celem jest ochrona praw i wolności jednostki w zakresie jej autonomii informacyjnej.

Rola GIODO w systemie polskich organów państwowych jest niezwykle ważna z uwagi na istotę i znaczenie działań, które on realizuje. W obliczu współczesnego postępu i rozwoju technologii oraz informacji konieczne staje się funkcjonowanie organu, który stoi na straży wzmacniania prewencyjnej ochrony prywatności i danych osobowych człowieka. Różne rodzaje informacji o człowieku powinny być chronione na gruncie prawa i przez specjalnie powołane do tego instytucje, gdyż niejednokrotnie niewystarczająca jest dbałość o swoją prywatność dokonywana tylko przez dysponenta danych - przez jednostkę. Powierzenie ochrony wyspecjalizowanemu podmiotowi gwarantuje pewność prawną, że dane, które są przetwarzane w różnych okolicznościach i przez różne podmioty, są należycie przetwarzane, a także właściwie chronione.

GIODO w Polsce jest jedynym tego typu organem, wyspecjalizowanym i powołanym do ochrony prawa do prywatności człowieka. Żaden inny organ w skali kraju nie realizuje w ramach swojej działalności zadań, które odnoszą się szczegółowo do ochrony danych osobowych osób fizycznych.

GIODO, na podstawie ustawy o ochronie danych osobowych, został umocowany, by realizować główne cele państwa związane z ochroną prywatności człowieka, co widoczne jest poprzez podejmowane przez niego działania. Generalny Inspektora sprawuje ochronę nad prawidłowością procesów przetwarzania danych osobowych przez podmioty prywatne i publiczne, realizując tym samym podstawowe wytyczne ustawowe odnoszące się do procesu kontroli przetwarzania danych osobowych. To nie tylko zatem organ kontrolujący procesy przetwarzania danych przez podmioty posiadające dostęp do różnych informacji o charakterze osobowym, ale także organ stojący na straży prywatności, powołany by chronić autonomię informacyjną jednostki i strzec ją przed nielegalnymi korzystaniem z jej danych osobowych. Jest to niezwykle doniosła funkcja GIODO na tle innych organów państwowych, gdyż odnosi się wprost do ochrony podstawowych praw i wolności człowieka. Swoimi działaniami GIODO realizuje ochronę na gruncie prawa do prywatności, kontrolując procesy przetwarzania danych osobowych oraz zapobiegając naruszeniu prywatności człowieka na różnych polach.

Działalność notyfikacyjna GIODO, która odnosi się do prowadzenia rejestru zbiorów danych osobowych i administratorów bezpieczeństwa informacji oraz udzielania informacji o zarejestrowanych zbiorach, zapewnia z kolei GIODO posiadanie wiedzy i możliwości kontroli nad tym, kto i jakie dane zbiera oraz w jakich warunkach są one wykorzystywane. Dysponowanie takimi informacjami przez ten organ umożliwia autentyczne i adekwatne zapewnienie ochrony prywatności człowieka, a w praktyce przyczynia się do rzeczywistej realizacji przez GIODO funkcji rzecznika ochrony interesów jednostki.

Z punktu widzenia rzeczywistej i skutecznej ochrony przetwarzania danych osobowych istotne są także uprawnienia egzekucyjne GIODO oraz kompetencje do rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych. Gdy wydawane przez GIODO decyzje nie są wykonywane dobrowolnie, ma on uprawnienia, aby wobec tych, którzy dobrowolnie nie wykonują obowiązków zawartych w tytule egzekucyjnym, wszcząć postępowanie egzekucyjne. Posiadanie uprawnień organu egzekucyjnego w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym pozwala GIODO aktywnie wpływać na zapewnienie prawidłowego procesu przetwarzania danych osobowych we wszystkich jego stadiach i faktycznie realizować wszelkie nakazy odnoszące się do wdrażania prawidłowego procesu ochrony danych.

Działalność GIODO jako organu ochrony prawa do prywatności to także jego prawo i zarazem obowiązek rozpatrywania skarg i wniosków. Już sam fakt, iż wnioskodawca może skierować do takiego organu zarzuty lub informuje o wszelkich nieprawidłowościach i

nadużyciach w zakresie przetwarzania danych osobowych, jest formą wykonywania ochrony w stosunku do danych osobowych. To również kształtuje właściwe postawy w społeczeństwie, które wykazuje się dbałością o ochronę prywatności swojej lub drugiego człowieka. Daje to pewność, iż kierowanie skarg i uwag co do niezgodnego z prawem korzystania z cudzych danych spotka się z reakcją właściwego organu, który w następstwie podejmie stosowne kroki prawne w celu szczegółowego zbadania sprawy i zastosuje adekwatne środki zaradcze.

GIODO posiada także możliwość wydawania decyzji administracyjnych w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych. Jest to jego typowo władcze uprawnienie, na mocy którego może kierować do określonych podmiotów sformułowane wprost żądanie nakazujące określone zachowanie się w zakresie przetwarzania danych osobowych. Poprzez wydanie decyzji administracyjnej może nakazać przywrócenie stanu przetwarzania lub ochrony danych osobowych zgodnego z prawem czy uwzględnić żądania osoby fizycznej związane z przetwarzaniem jej danych osobowych. GIODO wydaje również decyzje administracyjne w procesie notyfikacyjnym, w przedmiocie rejestracji lub wykreślenia określonych zbiorów danych z rejestru oraz co do zgody na przekazywanie danych do państwa trzeciego.

Podsumowując działalność Generalnego Inspektora odnoszącą się do ochrony prywatności informacyjnej jednostki warto także zwrócić uwagę na przyznane mu kompetencje w zakresie opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych. W założeniu służyć one mają eliminowaniu nieprawidłowości dotyczących przetwarzania danych osobowych już na etapie tworzenia prawa. Niestety jednak uprawnienia GIODO w tym zakresie zostały określone zbyt wąsko. Działalność opiniodawcza GIODO w stosunku do projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych z punktu widzenia ich zgodności z zasadami ochrony danych osobowych, chociaż niezwykle ważna, jest mało efektywna i ograniczona z uwagi na zbyt małą liczbę aktów prawnych odnoszących się *stricte* do ochrony danych osobowych. Wiele przygotowywanych projektów ustaw nie uwzględnia istoty postanowień zawartych w u.o.d.o., a znaczna część aktów prawnych jest wydawana z naruszeniem ustawy o ochronie danych osobowych. W praktyce często zdarza się także, że akty prawne przedstawione do konsultacji i opinii Generalnego Inspektora zawierają rozwiązania naruszające konstytucyjne prawa i wolności jednostki właśnie w zakresie ochrony danych osobowych. Zdarza się również, iż projekty aktów nie są w ogóle przedstawiane GIODO do opinii lub treść opinii GIODO nie jest uwzględniona przy przygotowywaniu projektu. Praktyka wskazuje, iż opinie czy sygnalizacje,

które z własnej inicjatywy podejmuje ten organ, eliminują nieprawidłowości w zakresie ochrony danych na etapie tworzenia prawa w różnych sektorach działalności państwa, jednak cały czas w niewystarczającym stopniu ta działalność GIODO przyczynia się to do zwrócenia uwagi prawodawcy na problem ochrony prywatności jednostki.

W moim przekonaniu konieczne jest, przy okazji przyszłych nowelizacji ustawy o ochronie danych osobowych, wprowadzenie zapisu co do obligatoryjnego wymogu konsultacji z GIODO w zakresie postanowień odnoszących się do ochrony prywatności i ochrony danych osobowych. Co więcej, potrzebne byłoby również wyposażenie tego organu w prawo wyrażania opinii na temat projektu ustawy stanowiącego wynik inicjatywy poselskiej, czego GIODO obecnie nie może dokonywać. By zapewnić skuteczne i efektywne działanie GIODO w zakresie ochrony prywatności konieczne jest także dalsze rozszerzenie zakresu jego działania o nowe uprawnienia.

W obecnym stanie prawnym GIODO nie ma prawa żądać zmiany aktu prawnego niezgodnego z art. 51 Konstytucji ani z ustawą o ochronie danych osobowych. Został także pominięty wśród podmiotów mających prawo do inicjowania postępowania przez TK oraz składania wniosków do Sądu Najwyższego, co stanowić może o ograniczeniu wpływu takiego organu na proces kontroli konstytucyjności prawa. Brak wskazanych uprawnień jest niewspółmierny do całej roli jaką GIODO odgrywa wśród organów ochrony prawa. Potrzebne jest poszerzenie jego uprawnień o powyżej wskazane, tak by ten organ w jak najefektywniejszy sposób mógł realizować funkcję ochrony prawa do prywatności. Także poszerzenie zakresu podmiotowego w art. 191 Konstytucji RP o organ, jakim jest Generalny Inspektor, wpłynęłoby znacząco na okazanie ważności zagadnieniom ochrony prywatności i ochrony danych osobowych człowieka. Ten fakt przyczyniłby się do podniesienia rangi GIODO i zrównania go przynajmniej w tym zakresie z innymi podmioty wymienionymi w tym artykule (np. Rzecznik Praw Obywatelskich, Prezes Najwyższej Izby Kontroli, Prezes Naczelnego Sądu Administracyjnego czy Prokurator Generalny).

Koncentrując się w dalszej kolejności na działaniach GIODO wart uwagi jest także fakt, iż dla ochrony prywatności człowieka nieocenione jest zaangażowanie Generalnego Inspektora na polu edukacyjno–informacyjnym i w zakresie uczestnictwa w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych. Dzięki jego funkcjonowaniu na płaszczyźnie krajowej, a także na forum międzynarodowym stale pojawia się potrzeba wprowadzania i przestrzegania regulacji w zakresie prywatności informacyjnej człowieka. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenie ochrony danych osobowych przez GIODO pozwala na większe

zrozumienie problematyki i konieczności ochrony prywatności. Szereg podmiotów zobowiązanych do ochrony danych osobowych korzysta z rozwiązań, które zapewnia GIODO (np. zapytania prawne kierowane do GIODO, interpretacja przepisów dokonywanych przez GIODO czy uczestnictwo w wielu przedsięwzięciach o charakterze edukacyjno-naukowym dotyczących ochrony problematyki prywatności jednostki), co ujawnia rosnące zainteresowanie społeczne tą problematyką i aktywnie kształtuje świadomość społeczną w zakresie potrzeby ochrony prywatności człowieka.

Należałoby jednako sobie życzyć, by wszelkie działania naukowo–edukacyjne, którym patronuje i podejmuje GIODO, objęły swoim zasięgiem jeszcze większa liczbę podmiotów. Oczywiście związane jest to z poszerzeniem zakresu działania GIODO oraz jego Biura, którego pracownicy z ramienia GIODO realizują ustawowe zadania tego organu. W takim wypadku konieczna byłaby reorganizacja jednostki pomocniczej, tj. urzędu GIODO. Wiązałoby się to z powołaniem chociażby większej liczby Jednostek Zamiejscowych Biura GIODO, niż dwóch obecnie działających w Gdańsku i w Katowicach. Zatrudnienie także większej liczby inspektorów w Biurze GIODO pozwoli na istnienie szeregu specjalistów jako stałego wsparcia GIODO, którzy wspólnie z nim działać będą na rzecz ochrony prywatności człowieka i zapewnią tym samym efektywniejszą i szybszą realizację zadań w urzędzie GIODO.

W zakresie realizacji przez GIODO swoich działań na rzecz ochrony prywatności na forum międzynarodowym koniecznym byłoby także wprowadzenie w ustawie wymogu dla kandydata na stanowisko GIODO, by znał co najmniej jeden język obcy, spośród języków roboczych Unii Europejskiej. Współcześnie nie wydaje się to oczekiwaniem wybiegającym znacząco ponad standardy stanowiskowe związane z zatrudnianiem osób pełniących funkcje kierownicze. Znacząco jednak wpłynąć może na profil i doniosłość organu, który w obliczu podejmowanych zadań równie swobodnie poradzi sobie ze zrozumieniem ich istoty i celu na forum krajowym jak i zagranicznym.

Pojawienie się GIODO w systemie organów państwowych niewątpliwie podniosło rangę problematyki ochrony prywatności i ochrony danych osobowych człowieka w Polsce. Pozycja tego organu oraz zakres przyznanych mu kompetencji upoważniają do stwierdzenia, iż GIODO zapewnia właściwą realizację praw podmiotowych w zakresie ochrony prywatności jednostki. Podsumowanie zadań, które realizuje GIODO i środków działania, które wykorzystuje w swojej działalności wyraźnie obrazuje, iż organ ten zapewnia ochronę prywatności człowieka na wszelkich etapach i możliwych polach przetwarzania danych.

Warto podkreślić, iż pozycja prawno–ustrojowa GIODO na tle innych organów państwowych jest znacząca lecz konieczne byłyby jeszcze do wprowadzenia następujące zmiany.

Jednym z postulatów skierowanych do prawodawcy jest potrzeba wskazania wprost w ramach przyszłej nowelizacji ustawy o ochronie danych osobowych, iż GIODO należy do organów centralnych, za czym przemawia jego pozycja prawna. Byłby to punkt wyjścia do stopniowej redukcji wszystkich wątpliwości, które dotychczas związane są z miejscem i pozycją tego organu wśród innych organów państwowych w Polsce.

Kluczowy wniosek *de lege ferenda* dotyczy jednak uzyskania przez GIODO statusu organu konstytucyjnego. Z punktu widzenia świadomości społecznej oraz *wskazania powagi i istoty tego organu* umiejscowienie GIODO w Konstytucji RP byłoby znaczące. GIODO realizując swoje działania jako rzecznik obywateli do spraw ochrony prywatności człowieka i ochrony danych osobowych bez wątpienia należy do grupy organów ochrony prawa. Jego kompetencje koncentrują się w istocie na ochronie podstawowego prawa człowieka, tj. prawa do ochrony prywatności jednostki, w tym jej danych osobowych, jednak jak dotąd GIODO nie znalazł miejsca wśród organów konstytucyjnych. Pozycja GIODO i przede wszystkim zakres przyznanych zadań do realizacji jak najbardziej upoważnia do stwierdzenia, iż stanowi on istotną gwarancję realizacji praw podmiotowych wynikających z ustawy, w tym prawa jednostki do informacji osobowych przetwarzanych przez administratora. W tym względzie, póki co, pozycja GIODO została umniejszona i to niesłusznie, chociażby w stosunku do Rzecznika Praw Obywatelskich (do którego Generalny Inspektor jest często porównywany), którego pozycja jest silniejsza z uwagi na uzyskanie statusu konstytucyjnego organu ochrony prawa, przez umiejscowienie go wprost w Konstytucji. Zdaniem chociażby W. Sokolewicza taki stan rzeczy, jest „rezultatem decyzji ustrojodawcy o powstrzymaniu się - być może czasowym - od nadania przymiotu organu konstytucyjnego instytucji wciąż jeszcze nieco eksperymentalnej”[1076]. Upłynął już jednak wystarczająco długi czas od wejścia w życie ustawy o ochronie danych osobowych i momentu powołania tego organu, by na gruncie jego dotychczasowych osiągnięć docenić jego działalność poprzez zamieszczenie w ustawie zasadniczej stosownych przepisów dotyczących GIODO.

Rangę GIODO z pewnością wzmocniłby fakt umieszczenia go wprost wśród innych organów konstytucyjnych, stąd popieram pogląd wyrażany przez B. Banaszaka i K. Wygodę,

---

[1076] Zob. W. Sokolewicz, *Uwaga 2 do Rozdziału IX „Organy kontroli państwowej i ochrony prawa”,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, Warszawa 2003, s. 4-5.

iż brak jest przeszkód, aby w rozdziale IX bądź rozdziale II Konstytucji RP, gdzie znajduje się art. 51, umieścić przypisy dotyczące GIODO[1077]. Przez pryzmat swojej działalności i wykonywanych działań, których istota obecnie znacząco wzrasta w obliczu zagrożenia prywatności jednostki w wielu płaszczyznach życia, organ, jakim jest GIODO, powinien w niedalekiej przyszłości uzyskać rangę organu konstytucyjnego.

Przed GIODO jako organem ochrony prawa do prywatności stoją cały czas nowe wyzwania, by jeszcze skuteczniej chronić prywatność człowieka. Jest to o tyle trudne, iż w dzisiejszych czasach wyznaczenie sztywnych granic pomiędzy tym, co publiczne, a tym co prywatne, nie jest łatwe. Poważnym wyzwaniem jest zapewnienie ochrony dla prywatności człowieka adekwatnej do istniejących dziś zagrożeń. Realizacja przez GIODO wszystkich założeń i celów powinna uwzględniać przede wszystkim specyfikę dzisiejszych czasów. Prawo musi reagować na zmieniający się świat i zapewniać ochronę praw i wolności w każdych możliwych warunkach na płaszczyźnie wertykalnej i horyzontalnej. Internet będący niejednorodną płaszczyzną komunikacyjną (np. poczta mailowa, komunikatory tekstowe czy głosowe, aplikacje mobilne, różne strony www), programy szpiegowskie, niechciane oprogramowanie, *spamming*, monitoring, cyberprzestępczość to tylko niektóre z współczesnych zagrożeń dla prywatności człowieka, które powinny być także przedmiotem analizy i prewencyjnych działań podejmowanych przez Generalnego Inspektora Ochrony Danych Osobowych. Powinna być stale i aktywnie popularyzowana działalność GIODO na wszystkich polach, które związane są z ochroną prywatności jednostki. Jest to ważne, by w społeczeństwie cały czas wzrastała świadomość wagi i potrzeby jej ochrony za sprawą istnienia i efektywnej działalności takiego organu jak GIODO.

Na koniec warto poczynić jeszcze ostatnią refleksję. Czy istnienie jednak w założeniu najdoskonalszych instytucji i najefektywniejsze działania ustawodawcy w kierunku zapewnienia ochrony prywatności jednostki jest w stanie stworzyć na tyle idealny system, że człowiek w pełni ochroni swoją prywatność „od oka, ucha i działań innych”? Jest to wielkie wyzwanie, chociaż nasuwają się wątpliwości, czy jest to w ogóle możliwe, gdyż postęp technologiczny zawsze wyprzedza regulacje prawne, które nie nadążają za „cudami” techniki. Wydaje się, że aktywna działalność GIODO we wszystkich wskazanych wcześniej obszarach mogłaby wypełniać deficyt regulacji prawny oraz ich nieefektywność wobec zmieniającej się rzeczywistości społeczno – gospodarczej. Organ ten jednak musi być wyposażony w niezbędne instrumenty prawne umożliwiające sprawne funkcjonowanie w obliczu

[1077] Zob. B. Banaszak, K. Wygoda, *op. cit.,* s. 55; G. Koksanowicz, *op. cit.,* s. 97.

nowoczesnej rzeczywistości oraz musi stale umacniać swój autorytet społeczny i akceptację dla podejmowanych, nierzadko kontrowersyjnych działań.

BIBLIOGRAFIA

Monografie

ABC wybranych zagadnień z ustawy o ochronie danych osobowych, Warszawa 2007.
Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.
Banaszak B., *Prawa jednostki i systemy ich ochrony*, Wrocław 1995.
Banaszak B., *Prawo konstytucyjne*, Warszawa 2008.
Banaszak B., Bernaczyk M., *Aktywizm sędziowski we współczesnym państwie demokratycznym*, Warszawa 2012.
Banyś T. A. J., Łuczak J., *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Wrocław 2013.
Barta J., P. Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011.
Barta J., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2013.
Barta J., R. Markiewicz R., *Główne problemy prawa komputerowego,* Warszawa 1993.
Barta J., Markiewicz R., *Internet a prawo*, Kraków 1999.
Boć J., *Komentarz do Konstytucji RP*, Wrocław 1998.
Boć J. red., *Konstytucje Rzeczypospolitej oraz komentarz do konstytucji RP z 1997 roku*, Wrocław 1998.
Boć J. red., *Prawo administracyjne*, Wrocław 2003.
Braciak J., *Prawo do prywatności,* Warszawa 2004.
Cieślak Z., Lipowicz I., Niewiadomski Z., Szpor G., *Prawo administracyjne*, Warszawa 2013.
Chróścielewski W., Organ *administracji publicznej w postępowaniu administracyjnym*, Warszawa 2002.
Dawidowicz W., *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970.
Dąbrowka A., Geller E., Turczyn R., *Słownik synonimów*, Warszawa 1993.
Drozd A. , *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2008.
Fajgielski P., *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne,* Lublin 2008.
Filipek J., *Prawo administracyjne. Instytucje ogólne. Część I*, Zakamycze 2003.
Fleszer D., *Zakres przetwarzania danych osobowych w działalności gospodarczej*, Warszawa 2008.
Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu,* Warszawa 2004.
Gesdorf M., *Komentarz do ustawy o Państwowej Inspekcji Pracy*, Warszawa 2008.
Gronowska B., *Wolność i bezpieczeństwo osobiste w sprawach karnych w świetle standardów Rady Europy*, Toruń 1996.
Grzybowski M. , *Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego*, Warszawa 1957.
Grzybowski M., *Systemy konstytucyjne państw skandynawskich*, Warszawa 1998.
Grzybowski M., Dembiński K., tłum., *Konstytucja Szwecji*, Warszawa 1991.
Hauser R., Leoński Z., Skoczylas A., *Komentarz do ustawy o postępowaniu egzekucyjnym w administracji,* Warszawa 2008.
Herdegen M., *Prawo europejskie*, Warszawa 2006.
Hofmański P., *Europejska Konwencja Praw Człowieka i jej znaczenie dla prawa karnego materialnego, procesowego i wykonawczego*, Białystok 1993.
Hofmański P., Zabłocki S., *Elementy metodyki pracy sędziego w sprawach karnych*, Warszawa 2011.

Hołda J., Hołda Z., Rybczyńska J.A., *Prawa człowieka. Zarys wykładu*, Warszawa 2008.
Iserzon E., *Prawo administracyjne*, Warszawa 1968.
Jagielski J., *Kontrola administracji publicznej*, Warszawa 2012.
Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010.
Janusz-Pohl B., *Ustrój organów ochrony prawnokarnej. Zarys wykładu*, Poznań 2011.
Jarosz Z., *Konstytucja V Republiki Francuskiej*, Warszawa 1997.
Jaroszyński M., Zimmermann M., Brzeziński W., *Polskie prawo administracyjne. Część ogólna*, Warszawa 1956.
Kamińska I., *Ochrona danych osobowych. Orzecznictwo sądów administracyjnych*, Warszawa 2007.
Kluska M., Kostewicz K., Leśniewski G., Wanio G., *Ochrona danych osobowych w działach kadr. Odpowiedzi na 370 najtrudniejszych pytań*, Wrocław 2014.
Kmieciak Z., *Skuteczność regulacji administracyjnoprawnej*, Łódź 1994.
Kołodziejczyk Ł., *Prywatność w Internecie*, Warszawa 2014.
Konarski X., *Internet i prawo w praktyce*, Warszawa 2002.
Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004.
Krasuski A., Skolimowska D., *Dane osobowe w przedsiębiorstwie*, Warszawa 2007.
Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych, w obecnym i nadchodzącym stanie prawnym*, Warszawa 2014.
Kuczma P., *Prawa człowieka w zarysie*, Polkowice 2012.
Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010.
Kuźniar R., *O prawach człowieka. Idee, instytucje, praktyka*, Warszawa 1992.
Kuźniar R., *Prawa człowieka*, Warszawa 2002.
Kwiecień R., *Miejsce umów międzynarodowych w porządku prawnym państwa polskiego*, Warszawa 2000.
Leoński Z., *Zarys prawa administracyjnego*, Warszawa 2004.
Lipowicz I., *Administracyjnoprawne zagadnienia informatyki*, Katowice 1984.
Litwiński P., *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa 2009.
Łaszczyca G., Marzysz Cz., Matan A., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2007.
Malinowska I., *Rzecznik Praw Obywatelskich w systemie ochrony praw i wolności w Polsce*, Warszawa 2007.
Matczak M., *Kompetencje organu administracji publicznej*, Kraków 2004.
Mednis A., *Prawna ochrona danych osobowych*, Warszawa 1995.
Mednis A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999.
Michalska A., *Prawa człowieka w systemie norm międzynarodowych*, Warszawa 1982.
Michalski B., *Podstawowe problemy prawa prasowego*, Warszawa 1998.
Mik C., *Zbiorowe prawa człowieka. Analiza krytyczna koncepcji*, Toruń 1992.
Miller A. R., *The Assault on Privacy*, Ann Arbor 1971.
Motyka K., *Prawo do prywatności i dylematy współczesnej ochrony praw człowieka*, Lublin 2006.
Mrózek A., *Ustawowe prawo ochrony danych. Analiza porównawcza*, Toruń 1981.
Nowacki J., Tabor Z., *Wstęp do prawoznawstwa*, Kraków 2002.
Ochendowski E., Prawo *administracyjne. Część ogólna*, Toruń 2013.
Oniszczuk J., *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego*, Kraków 2000.
Petzel J., *Informatyka prawnicza. Zagadnienia teorii i praktyki*, Warszawa 1999.

Philips J. (red.), *Oxford Wordpower. Słownik angielsko-polski z indeksem polsko- angielskim*, Oxford 1997.
Polaczek T., *Audyt bezpieczeństwa informacji w praktyce*, Gliwice 2006.
Polok M., *Bezpieczeństwo danych osobowych*, Warszawa 2008.
Prusak F., *Ustrój organów ochrony prawnej. Wprowadzenie. Teksty ustaw*, Warszawa 1999.
Puwalski M., *Prawo do prywatności osób publicznych*, Toruń 2003.
Radwański Z., *Prawo cywilne - część ogólna*, Warszawa 1997
Radwański Z., *Zarys części ogólnej prawa cywilnego*, Warszawa 1979.
Robertson A. H., *Privacy and Human Rights*, Manchester University 1973.
Sagan S., *Generalny Inspektor Ochrony Danych Osobowych w Polsce*, Warszawa 2011.
Sagan S., *Prawo konstytucyjne Rzeczypospolitej Polskiej*, Warszawa 2001.
Sagan S., Serzhanova V., *Organy i korporacje ochrony prawa*, Warszawa 2014.
Sakowska-Baryła M., *Prawo do ochrony danych osobowych*, Wrocław 2015.
Sarnacka K., *Prawo do informacji w polskim prawie konstytucyjnym*, Warszawa 2009.
Serafin S., Szmulik B., *Organy ochrony prawnej RP*, Warszawa 2010.
Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003.
Sibiga G., *Wystąpienie - nowa kompetencja Generalnego Inspektora Ochrony Danych Osobowych*, „Dodatek do Monitora Prawniczego" 2011, nr 3.
Sieńczyło-Chlabicz J., *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Kraków 2006.
Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.
Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Komentarz*, Kraków 1998.
Skrzydło W., Grabowska S., Grabowski R., *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, Warszawa 2009.
Sługocki J., *Prawo administracyjne. Podstawowe zagadnienia ustrojowe*, Warszawa 2007.
Sozański J., *Prawo Unii Europejskiej*, Warszawa-Poznań 2010.
Sójka-Zielińska K., *Kodeks Napoleona. Historia i współczesność*, Warszawa 2008.
Sójka-Zielińska K., *Wielkie kodyfikacje cywilne. Historia i współczesność*, Warszawa 2009.
Stefanowicz B., *Informacja*, Warszawa 2004.
Stelmachowski A., *Zarys teorii prawa cywilnego*, Warszawa 1998.
Styrna-Bartman K., Tuora-Schwierskott E., *Niemiecki Kodeks Cywilny. Przepisy §1- 432 niemieckiego kodeksu cywilnego z wyjaśnieniami w tłumaczeniu na język polski*, Regensburg 2014.
Sylwestrzak A., *Kontrola administracji publicznej w III Rzeczypospolitej Polskiej*, Gdańsk 2001.
Szałowski R., *Ochrona danych osobowych. Komentarz do ustawy z 29.08.1997*, Zielona Góra 2000.
Szewc T., *Publicznoprawna ochrona informacji*, Warszawa 2007.
Szmulik B., Przywora B., *Konstytucyjny system organów państwowych*, Warszawa 2014.
Szmulik B., Żmigrodzki M., *Ustrój organów ochrony prawnej*, Lublin 2005.
Szumiło-Kulczycka D., *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012.
Szymczak M. (red.), *Słownik języka polskiego*, t. 1, Warszawa 1978.
Szymczak M. (red.), *Słownik języka polskiego*, t. 3, Warszawa 1995.
Szyszkowski B., *Beniamin Constant. Doktryna polityczno-prawna*, Warszawa- Poznań-Toruń 1984.
Trociuk S., *Ustawa o Rzeczniku Praw Obywatelskich. Komentarz*, Warszawa 2005.
Trzciński J., *Pojęcie konstytucyjnego organu państwa socjalistycznego*, Warszawa-Kraków-Gdańsk 1974.

Ura E., *Prawo administracyjne*, Warszawa 2009.
Wawrzyniak J., *Prawo do prywatności. Zarys problematyki*, Warszawa 1994.
Westin A., *Privacy and Freedom*, New York 1967.
Winczorek P., *Komentarz do Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r*., Warszawa 2000.
Witkowski Z., *Prawo konstytucyjne*, Toruń 1998.
Włodyka S., *Ustrój organów ochrony prawnej*, Warszawa 1975.
Wolter A., Ignatowicz J., Stefaniuk K., *Prawo cywilne. Zarys części ogólnej*, Warszawa 2001.
Wronkowska S., Zieliński M., Ziembiński Z., *Zasady prawa. Zagadnienia podstawowe*, Warszawa 1974.
Zimmermann J., *Prawo administracyjne*, Warszawa 2006.
Zubik M., *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego*, Zakamycze 2000.
Zubik M*., Konstytucja III RP w tezach orzeczniczych Trybunału Konstytucyjnego i wybranych sądów*, Warszawa 2011.

Artykuły

Banaszak B., Wygoda K., *Regulacja prawna ochrony danych osobowych w Polsce w świetle ustawy z 29 sierpnia 1997 r. i standardów europejskich*, [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999.
Berlin I., *John Stuart Mill i cele życia*, [w:] *Cztery eseje o wolności*, red. I. Berlin, Poznań 2000.
Bichta T., *Rzecznik Praw Obywatelskich,* [w:] *Ustrój organów ochrony prawnej,* red. B. Szmulik, M. Żmigrodzki, Lublin 2003.
Bierć A., *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce - aspekty cywilnoprawne,* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999.
Błachnio- Parzych A., *Prawnokarna ochrona inspektora ochrony danych osobowych- przestępstwo udaremnienia lub utrudnienia kontroli przestrzegania przepisów o ochronie danych osobowych*, „Dodatek do Monitora Prawniczego" 2011, nr 3.
Bodio J., *Klasyfikacja organów ochrony prawnej*, [w:] *Ustrój organów ochrony prawnej. Część szczegółowa*, red. T. Demendecki, J. Bodio, G. Borkowski, Warszawa 2010.
Bogucka D., *Co nas będzie obowiązywało*, „Gazeta Prawna" z dnia 29 stycznia 2003 r.
Braciak J., *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002.
Braciak J., *Prawo do prywatności. Praktyczne i teoretyczne problemy współczesnego państwa*, „Zeszyty Luksemburskie" 2012, nr 1.
Brieskorn N., *Ochrona danych osobowych a zagrożenia* prywatności, [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999.
Byczkowski M., *Zarządzanie procesami przetwarzania danych osobowych*, [w:] *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, red. X. Konarski, G. Sibiga, Warszawa 2007.
Cisek R., [w:] *Dobra i usługi informacyjne w obrocie gospodarczym*, red. R. Cisek, J. Jezioro, A. Wiebe, Warszawa 2005.
Complak K., *O prawidłowe pojmowanie godności osoby ludzkiej w porządku RP*, [w:] *Prawa i wolności obywatelskie w Konstytucji*, red. B. Banaszak, A. Preisner, Wrocław 2002.
Corbain A., *Kulisy*, [w:] *Historia życia prywatnego. Tom 4: Od rewolucji francuskiej do I wojny światowej,* red. M. Perrot, Ossolineum 2006.

Czarnecki K., *Ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008.
Degórska K., *Prawo do ochrony życia prywatnego i rodzinnego*, [w:] *Prawa i wolności I i II generacji*, red. A. Florczak, B. Olechów, Toruń 2006.
Dmowski S. [w:] Dmowski S., Rudnicki S., *Komentarz do kodeksu cywilnego. Ks.1. Część ogólna*, Warszawa 1999.
Drozd A., *Zakres zakazu przetwarzania danych osobowych*, „Państwo i Prawo" 2003, nr 2.
Fajgielski P., Nowelizacja ustawy o ochronie danych osobowych- zakładane cele i przewidywane skutki, „Ochrona danych osobowych. Dodatek do Monitora Prawniczego" 2011, nr 3.
Galster J., *System organów państwowych*, [w:] *Prawo konstytucyjne*, red. Z. Witkowski, Toruń 2013.
Garlicki L., *Komentarz do art. 8 EKPCz*, [w:] *Konwencja i Ochronie Praw Człowieka i Podstawowych Wolności*, Tom I, *Komentarz do artykułów 1-18*, red. L. Garlicki, Warszawa 2010.
Garlicki L., *Nowe demokracje przed Europejskim Trybunałem Praw Człowieka*, [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009*, red. J. Jaskiernia, Toruń 2001.
Genz A., *Datenschutz in Europa und den USA: Eine Rechtsvergleichende Untersuchung unter Besonderer Berücksichtigung der Safe-Harbor-Lösung (DuD-Fachbeiträge)*, Jnuar 2004.
GIODO: unijna reforma to szansa na lepsza ochronę danych, „Dziennik Gazeta Prawna" z 18 września 2015 r.
GIODO potrzebuje więcej, „Gazeta Prawna" z 29 stycznia 2007 r., nr 20 (1890).
Gliszczyńska-Grabias A., Sękowska-Kozłowska K., *Komentarz do art. 17 MPPOiP*, [w:] *Międzynarodowy pakt Praw Obywatelskich (osobistych) i Politycznych*, red. R. Wieruszewski, Warszawa 2012.
Gonzáles Fuster G., *Datenschutz- und Informationsrecht. Ausgabe für Hessen*, Juris Lex 2015.
Górzyńska T., *Kto strzeże prywatności*, „Rzeczpospolita" z 26 maja 1997 r.
Gonzáles Fuster G., The Emergencje of Personal Data Protection as a Fundamental Wright of the EU, Law, Gevernance and Technology Series, Vol. 16.
Gronowska B., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii - problem poszanowania życia prywatnego człowieka na tle gromadzenia danych osobowych przez służby ochrony państwa*, „Prokuratura i Prawo" 2000, nr. 9.
Gross H., *The Concept of Privacy*, „New York University Law review" 1967, vol. 4.
Harla A. G., *Termin „dane osobowe"- uwagi de lege lata i de lege ferenda na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, „Palestra" 2001, nr 1-2.
Husak Z., *Struktura organów władzy publicznej*, [w:] *Konstytucyjny system organów państwa*, D. Dudek, Z. Husak, G. Kowalski, W. Lis, Warszawa 2013.
Jabłoński M., Węgrzyn J., Rzuciło J., *Znaczenie protokołu nr 7 do Traktatu z Lizbony dla procesów integracyjnych w Unii Europejskiej*, „Przegląd Prawa i Administracji" 2011, nr 86.
Jabłoński M., Wygoda K., *Zasady ochrony danych osobowych*,[w:] *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, red. J. Gołaczyński, Warszawa 2003.
Jagielski M., *Konstytucjonalizacja ochrony prywatności*, [w:] *Konstytucjonalizm a doktryny polityczno – prawne. Najnowsze kierunki badań*, red. R.M. Małajny, Katowice 2008.

Jarosz-Żukowska S., *Organ administracji publicznej*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, red. W. Skrzydło, S. Grabowska, R. Grabowski, Warszawa 2009.
Jarosz-Żukowska S., *Organ państwowy*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, red. W. Skrzydło, S. Grabowska, R. Grabowski, Warszawa 2009.
Jaskiernia J., *Rada Europy jako organizacja międzynarodowa*, [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009*, red. J. Jaskiernia, Toruń 2001.
Juszyński T., *Ochrona obywatela i konsumenta w świetle niemieckiej ustawy o ochronie danych osobowych*, „Państwo i Prawo" 1998, z. 3.
Kański L., *Prawo do prywatności, nienaruszalność mieszkania i tajemnicy korespondencji*, [w:] *Prawa człowieka. Model prawny*, red. R. Wieruszewski, Wrocław 1991.
Kawecki M., *Generalny Inspektor Ochrony danych Osobowych jako centralny organ administracji państwowej*, „Przegląd Prawa Technologii Informacyjnych. ICT Law Review" 2013, nr 1.
Kański L., *Prawo do prywatności (Miejsce w prawie polskim)*, Biuletyn Rzecznika Praw Obywatelskich, Materiały 1989, nr 4.
Kilian W., [w:] *Prawnicze i ekonomiczne aspekty komunikacji elektronicznej*, red. Gołaczyński J., Warszawa 2003.
Kluska M., *Dane chronione na nowo*, „IT w administracji" 2012, czerwiec.
Koksanowicz G., *Generalny Inspektor Ochrony Danych Osobowych*, [w:] *Ustrój organów ochrony prawnej*, red. B. Szmulik, M. Żmigrodzki, Lublin 2005.
Koksanowicz G., *Ochrona danych osobowych w świetle Konstytucji oraz Ustawy o ochronie danych osobowych*, [w:] *Konstytucyjny ustrój państwa*, T. Bojarski, E. Gdulewicz, J. Szreniawski, Lublin 2000.
Konarski X., Sibiga G., *Zmiany w ustawie o ochronie danych osobowych w świetle Dyrektywy 95/46/WE*, „Monitor Prawniczy" 2004, nr 12.
Konieczna B., *Decyzje GIODO w sprawach ochrony danych osobowych*, [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009.
Kopff A., *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1971, t. XX.
Kowalik K., *Safe Harbour*- porozumienie dotyczące wymiany danych osobowych miedzy krajami Unii Europejskiej a Stanami Zjednoczonymi, „Przegląd Prawa Europejskiego" 2002, nr 1 (11).
Kordasiewicz B., *Cywilnoprawna ochrona prawa do prywatności*, „Kwartalnik Prawa Prywatnego" 2000, z.1.
Kraemer R., Porzycki M., *Ochrona danych osobowych w instytucjach finansowych z amerykańskiej perspektywy*, „Transformacja Prawa Prywatnego" 2001, nr. 4.
Krasuski A., Zakres *podmiotowy ustawy o ochronie danych osobowych - uwagi de lege lata i de lege ferenda*, [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008.
Kubiński K. W., *Ochrona życia prywatnego człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny"1993, nr 1.
Kubot Z. , *Charakter prawny odpowiedzialności porządkowej w kodeksie pracy*, „Państwo i Prawo" 1975, nr 7.
Kuczma E., Kuczma P., *Generalny Inspektor Ochrony Danych Osobowych jako organ kontroli i ochrony prawa*, „Zeszyty Naukowe Dolnośląskiej Wyższej Szkoły Przedsiębiorczości i Techniki", Polkowice 2013, nr 6.

Kuczma E., *Ochrona danych osobowych przez przedsiębiorcę*, [w:] *Przedsiębiorca w społecznej gospodarce rynkowej*, „Prace naukowe Uniwersytetu Ekonomicznego we Wrocławiu", red. T. Kocowski, J. Gola, Wrocław 2014, nr 372.
Kuczma E., *Perspektywy ochrony danych osobowych w Unii Europejskiej*, [w:] *25 Jahre Teutsch- Polnische Juristen - Vereinigung e.V.- Festschrift zum Jubiluj. Niemiecko- polskie Stowarzyszenie Prawników - Księga pamiątkowa z okazji 25- letniego jubileuszu,* red. E. Tuora-Schwierskott, Regensburg 2015.
Kuczma E., *Pozycja ustrojowa i rola Europejskiego Inspektora Ochrony Danych w procesie przetwarzania danych osobowych w Unii Europejskiej*, [w:] *Polska wobec standardów Unii Europejskiej*, red. P. Kuczma, Polkowice 2015.
Kulesza E., *Pozycja i uprawnienie Generalnego Inspektora Ochrony Danych Osobowych w świetle ustawy o ochronie danych osobowych. Uwagi de lege lata i de lege ferenda*, „Przegląd Sejmowy" 1999, nr 6(35).
Kulesza E., *Pozycja prawna Generalnego Inspektora Ochrony Danych Osobowych*, [w:] *Przetwarzanie i ochrona danych*, red. G. Szpor, Katowice 1998.
Kulesza E., *Rejestr musi być aktualny*, „Rzeczpospolita" z 31 sierpnia 2000 r.
Kulesza E., *Zdrowie: zasada i wyjątki*, „Rzeczpospolita" z 4 maja 2000 r.
Kulesza E., G. Sibiga G., *Wykonanie obowiązku rejestracji zbiorów danych osobowych przez kasy chorych*, „Prawo i Medycyna" 2000, nr 6-7.
Kurzępa B., *Przestępstwa z ustawy o ochronie danych osobowych*, „Prokuratura i Prawo" 1999 r., nr 6.
Kuźniar R., *Międzynarodowe systemy ochrony praw człowieka*, „Sprawy Międzynarodowe" 1981.
Lijowska M., *Koncepcja ogólnego prawa osobistości w niemieckim i polskim prawie cywilnym*, „Kwartalnik Prawa Prywatnego" 2001, z. 4.
Lipowicz I., *Konstytucyjne prawo do informacji a wolność informacji*, [w:] *Wolność informacji i jej granice*, red. G. Szpor, Katowice 1997.
Lipowicz I., *Teza nr 3 do art. 51 Konstytucji RP*, [w:] *Konstytucje Rzeczypospolitej oraz komentarz do konstytucji RP z 1997 roku*, red. J. Boć, Wrocław 1998.
Małajny R. M., *Alternatywne koncepcje podziału władzy państwowej w XX w.,* [w:] *Idee jako źródło instytucji politycznych i prawnych*, red. L. Dubel, Lublin 2003.
Małajny R. M., *Systematyka polskich organów państwowych i ich charakter prawny*, „Studia Prawnicze" 1989, z.1.
Małajny R. M., *Zasada rozdziału władzy państwowej – prolegomena*, [w:] *Państwo i prawo wobec współczesnych wyzwań. Teoria i filozofia państwa i prawa oraz aksjologia demokracji i ochrony praw człowieka. Księga jubileuszowa Profesora Jerzego Jaskierni*, red. R. Czarny, K. Spryszak, Tom 5, Toruń 2012.
Martysz Cz., *Pozycja ustrojowa Generalnego Inspektora Ochrony Danych Osobowych*, [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009.
Matwiejuk J., *Konstytucyjne wolności, prawa i obowiązki człowieka i obywatela*, [w:] *Prawo konstytucyjne*, red. M. Grzybowski, Białystok 2009.
Mednis A., *Administrator bezpieczeństwa informacji po nowelizacji ustawy o ochronie d*anych osobowych z 7.11.2014 r. – ocena rozwiązań, [w:] Aktualne problemy ochrony danych osobowych, dodatek do Monitora Prawniczego, 2015, nr 6.
Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i dyrektywie Unii Europejskiej*, „Państwo i Prawo" 1997, nr 6.
Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, cz. II, ODO 2000, nr 2.
Mednis A., *Postulowane zmiany w ustawie o ochronie danych osobowych*, „Ochrona Danych Osobowych. Biuletyn ABI" 2000, nr 3.

Mednis A., *Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?*, [w:] *Prywatność a jawność - bilans 25-lecia i perspektywy na przyszłość,* Warszawa 2016.
Mednis A., *U nas i gdzie indziej*, „Rzeczpospolita" z dnia 21 stycznia 1995 r.
Mednis A., *Ustawa o ochronie danych osobowych a zagraniczne regulacje w tym zakresie*, [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008.
Michalska – Badziak R., [w:] *Prawo administracyjne*. *Pojęcia, instytucje, zasady w teorii i orzecznictwie*, red. Z. Zduniewska, B. Jaworska-Dębska, R. Michalska-Badziak, E. Olejniczak-Szałowska, M. Stahl, Warszawa 2000.
Mielnik Z., *Prawo do prywatności (wybrane zagadnienia)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 2.
Młynarska- Sobaczewska M., *Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej*, „Przegląd Prawa Konstytucyjnego" 2013, nr 1(13).
Młynarska- Sobaczewska M., Sakowska M,. *„Klauzula prasowa" z ustawy o ochronie danych osobowych jako gwarancja wolności wypowiedzi*, „Państwo i Prawo" 2005, nr 1.
Modzelewska M., *Państwo wobec ochrony prywatności informacyjnej*, [w:] *Silne państwo*, red. M. Szyszkowska, Warszawa 1997.
Motyka K., *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Seria: Administracja i Zarządzanie" 2010.
Niczyporuk J., *Administracja ochrony danych osobowych*, [w:] *Prawa jednostki w społeczeństwie informatycznym*, red. M. Grzybowski, Rzeszów 1999.
Nowacki A.M., *Radziecki łącznik*, „Rzeczpospolita" z 2 marca 2000 r.
Nowak M., *Trzy generacje praw człowieka. Ich znaczenie w świetle przesłanek ideowych i historycznych oraz w świetle ich genezy*, [w:] *Prawa człowieka – geneza, koncepcje, ochrona,* red. B. Banaszak, Wrocław 1993.
Nowakowski B., *Ochrona danych osobowych*, [w:] *System kontroli GIODO i ochrona informacji niejawnych. Praktyczne wskazówki ochrony i kontroli danych osobowych i informacji niejawnych,* red. A. Jędruszczak, B. Nowakowski Warszawa 2011.
Orłowski W., *Organy władzy publicznej oraz system organów państwa*, [w:] *Konstytucyjny system organów państwowych*, red. E. Gdulewicz, Lublin 2009.
Ożegalska- Trybalska J., *Adresy e- mailowe a dane osobowe*, Biuletyn Administratorów Bezpieczeństwa Informacji, Grudzień 2001.
Pagallo U. , M. Durante M., *Legal Memories and the Right to be Forgotten*, [w:] *Protection of Information and the Right to Privacy- A new Equilibrium?*, [w:] *Law, Governance and Technology Series,* red. Floridini L., Vol. 17.
Pieniążek A., *Rzecznik Praw Obywatelskich w systemie organów państwa,* [w:] *Ustrój i struktura aparatu państwowego i samorządu terytorialnego*, red. W. Skrzydło, Warszawa 1997.
Pilc B., *Kontrola przestrzegania przepisów o ochronie danych osobowych po wprowadzeniu w OchrdanOsobU elementów treści protokołu kontroli*, „Dodatek do Monitora Prawniczego" 2011 r., nr 3.
Płonka- Bielenin K., *Zakres pojęcia „zadania publiczne" i próba pokreślenia istoty ich realizacji przez organizacje pożytku publicznego*, „Administracja- Teoria- Dydaktyka- Praktyka"2011, nr 2.
Posiadła A., Winiecka S., *Ochrona danych osobowych w świetle wybranych orzeczeń Europejskiego Trybunału Praw Człowieka*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008.
Prawna ochrona danych osobowych. Uzasadnienie projektu ustawy przyjętego przez Radę Ministrów 13 sierpnia 1996 r., „Przegląd Rządowy" 1996 r., nr 10.

Przybysz P., *Kompetencje egzekucyjne Generalnego Inspektora Ochrony Danych Osobowych oraz postępowanie egzekucyjne prowadzone przez organ ochrony danych osobowych*, „Monitor Prawniczy" 2011, nr 3.
Przywora B., *Generalny Inspektor Ochrony Danych Osobowych w Polsce – stan obecny i postulaty de lege ferenda,* [w:] *Państwo demokratyczne, prawne i socjalne. Studia konstytucyjne. Księga jubileuszowa dedykowana profesorowi Zbigniewowi Antoniemu Maciągowi. Tom 1 Studia konstytucyjne,* red. M. Grzybowski, P. Tuleja, Kraków 2014.
Pułło A., *O jedno rozumienie podziału władz w nauce prawa konstytucyjnego*, „Państwo i Prawo" 1983, z. 6.
Pryciak M., *Prawo do prywatności*, „Studnia Erasmiana Wrtislaviensia" 2010, nr 4.
Radwański Z., *Kodeks cywilny a prawo regulujące zagadnienia rodziny,* [w:] *Problemy współczesnego prawa cywilnego (konferencja naukowa)*, Warszawa 1982.
Resich Z., *Nowy etap w rozwoju międzynarodowej ochrony praw człowieka*, „Państwo i Prawo" 1973.
Rzuciło J., *Prawo do prywatności i ochrona danych osobowych*, [w:] *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, red. M. Jabłoński, Wrocław 2014.
Safjan M., *Granice autonomii człowieka w prawie współczesnym*, „Rocznik Polskiej Akademii Umiejętności", 2002/2003, Kraków 2004.
Safjan M., *Prawo do ochrony życia prywatnego,* [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, red. L. Wiśniewski, Warszawa 1997.
Safjan M., *Prawo do ochrony życia prywatnego,* [w:] *Szkoła Praw Człowieka. Teksty wykładów,* Warszawa 1996.
Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6.
Safjan M., Wyrzykowski M., Banaszak B., Kulesza W. [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski M., Warszawa 1999.
Sagan S., *Generalny Inspektor Ochrony Danych Osobowych*, [w:] *Organy i korporacje ochrony prawa,* red. S. Sagan, J. Ciechanowska, Warszawa 2010.
Sagan S., *Pojęcie organu*, [w:] *Organy i korporacje ochrony prawa,* red. S. Sagan, J. Ciechanowska, Warszawa 2010.
Sagan S., *Szwedzkie doświadczenia w zakresie gromadzenia i wykorzystywania danych osobowych*, [w:] *Prawa jednostki w społeczeństwie informacyjnym*. *Materiały Ogólnopolskiej Konferencji Naukowej*, red. M. Grzybowski, Rzeszów 1999.
Sakowicz A., *Ochrona danych osobowych*, „Jurysta" 2001, nr 10.
Sakowska M. *„Klauzula prasowa" z ustawy o ochronie danych osobowych jako gwarancja wolności wypowiedzi*, „Państwo i Prawo" 2005, nr 1.
Sakowska M., *Pojęcie „zbiór danych" na gruncie ustawy o ochronie danych osobowych*, „Radca Prawny" 2005, nr 2.
Sakowska M., Pozycja ustrojowa i zadania Generalnego Inspektora Ochrony Danych Osobowych, „Przegląd Sejmowy" 2006, nr 2.
Santor G., *The Right to be Forgotten. Dynamics of Privacy and Publicity, [w:] Protection of Information and the Right to Privacy- A new Equilibrium?*, [w:] *Law, Governance and Technology Series*, red. Floridi L., Vol. 17.
Sarnecki P., *Art. 47*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom III, red. L. Garlicki, Warszawa 2003.
Sarnecki P., [w:] *Ustrój Unii Europejskiej i ustroje państw członkowskich,* red. P. Sarnecki, Warszawa-Kraków 2007.
Sibiga G., *Nowelizacja ustawy o ochronie danych osobowych*, „Monitor Prawniczy" 23/2001.

Sibiga G., *Zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych*, „Monitor Prawniczy" 1999, nr 8.
Simonides J., *Ewolucja systemu ochrony praw człowieka w Europie*, [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009*, red. J. Jaskiernia, Toruń 2001.
Siostrzonek A., *Dane osobowe gromadzone w bazach danych i ich ochrona w prawie polskim*, „Rejent" 1999, nr 9.
Skrzydło W., *Konstytucyjne założenia systemu organów państwa i ich wpływ na kształt aparatu państwowego*, [w:] *Ustrój i struktura aparatu państwowego i samorządu terytorialnego*, red. W. Skrzydło, Warszawa 1997.
Sokolewicz W., *Le droit de „privacy" et ses limitations*, [w:] *Rapports Polonais, preséntés au IX Congrès International de Droit Comparé*, Warszawa-Wrocław 1974. Sokolewicz W., Prawo do prywatności, [w:] *Prawa Człowieka w Stanach Zjednoczonych*, red. L. Pastusiak, Warszawa 1985.
Sokolewicz W. , *Rozdział I „Rzeczpospolita", artykuł 7*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. Garlicki L., Warszawa 2007.
Sokolewicz W. , *Rozdział IX „Organy kontroli państwowej i ochrony prawa"*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom III, red. Garlicki L., Warszawa 2003.
Sokolewicz W., *Uwaga 2 do Rozdziału IX „Organy kontroli państwowej i ochrony prawa"*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Tom III, red. L. Garlicki, Warszawa 2003.
Solove D. J., Hoofnagle Ch. J., *A Model Regime of Privacy Protection*, "University of Illinois Law Review", Vol. 2006, No. 2.
Sut P., *Czy sfera intymności jest dobrem osobistym chronionym w prawie polskim?,* „Palestra' 1995, nr 7/8.
Sylwestrzak A., *Konstytucja RP z 1997 r. – nowe interpretacje podziału władz*, [w:] *Dziesięć lat Konstytucji Rzeczypospolitej Polskiej*, red. E. Gdulewicz, H. Zięba-Załucka, Rzeszów 2007.
Sylwestrzak A., *NIK a Konstytucja*, „Kontrola Państwowa" 1998, nr 1.
Szafarz R., *Dorobek traktatowy Rady Europy*, [w:] *Valeat aequitas. Księga pamiątkowa ofiarowana Księdzu Profesorowi Remigiuszowi Sobańskiemu*, red. M. Pazdan, Prace Naukowe Uniwersytetu Śląskiego, Nr 1905.
Szczerba A., *Europejski Inspektor Ochrony Danych - niezależny organ*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008.
Szmak Sz., *Europejskie standardy w zakresie ochrony danych osobowych - zarys problemu*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów,* red. G. Goździewicz, M. Szabłowska, Toruń 2008.
Szpor G., *Kontrola administracji*, [w:] *Prawo administracyjne*, red. Z. Cieślak, I. Lipowicz, Z. Niewiadomski, G. Szpor, Warszawa 2013.
Szpor G., *Publicznoprawna ochrona danych osobowych*, „Przegląd Ustawodawstwa Gospodarczego" 1999, nr 12.
Szpor G., *Uwarunkowania skuteczności regulacji ochrony danych osobowych*, [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009.
Szpunar A., *O ochronie sfery życia prywatnego,* „Nowe Prawo" 1982.
Szpunar A., *Szkoda wyrządzona przed urodzeniem dziecka*, „ Studia cywilistyczne" 1969, t. XIII-XIV.
Szustakiewicz P., *Kontrole Generalnego Inspektora Ochrony Danych Osobowych*, „Kontrola Państwowa" 2007, nr 6.

Szwed K., *Ewolucja ochrony danych osobowych na przykładzie Polski i Szwecji*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego. Seria prawnicza", Zeszyt 71/2011, Prawo 10.
Szyszkowski W., *Rozważania o prywatności*, [w:] *Wybrane problemy prawa konstytucyjnego,* red. W. Skrzydło, Lublin 1985.
Tinnefeld M-T., *Ochrona danych - kamień węgielny budowy Europy*, [w:] red. M. Wyrzykowski, *Ochrona danych osobowych*, Warszawa 1999.
Ura E., *Centralne organy administracji rządowej w okresie przemian ustrojowych państwa,* [w:] *Administracja i prawo administracyjne u progu trzeciego tysiąclecia. Materiały konferencji naukowej katedr prawa i postępowania administracyjnego*, Łódź 2000.
Verpeaux M., *Rada Konstytucyjna a ochrona praw podstawowych*, „Przegląd Sejmowy" 2010, nr 1.
Warren S. D., Brandeis L. D., *The right to privacy*, w: „Harvard Law Review", 1890, vol. 4.
Wiewiórowski W. R., *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, Ochrona danych osobowych. Aktualne problemy prawnej ochrony danych osobowych, „Monitor Prawniczy" 2012, nr 7.
Wikariak S, *Ochrona danych osobowych wymaga przeglądu setek aktów prawnych*, „Rzeczpospolita" z 21.09.2015.
Wiktorowska A., *Rodzaje organów administracji*, [w:] *Prawo administracyjne*, red. M. Wierzbowski, J. Jagielski, J. Lang, M. Szubiakowski, A. Wiktorowska, Warszawa 2011.
Wild M. , *Ochrona prywatności w prawie cywilnym (koncepcja sfer a prawo podmiotowe)*, „Państwo i Prawo" 2001, nr 4.
Wygoda K., *Ochrona danych osobowych i prawo do informacji o charakterze osobowym*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002.
Wygoda K., *Powoływanie Administratora Bezpieczeństwa Informacji jako zasada bezpiecznego przetwarzania danych na gruncie ustawy o ochronie danych osobowych*, „Przegląd Prawa i administracji" C/2, Wrocław 2015, No 3661.
Wyrozumska A., *Znaczenie prawne zmiany statusu Karty Praw Podstawowych Unii Europejskiej*, „Przegląd Sejmowy" 2008, nr 2 (85).
Yamazaki K., *Ochrona praw człowieka w krajach azjatyckich*, „Sprawy Międzynarodowe" 1990, nr 6.
Zielonacki A., *Wartości życia rodzinnego w świetle ochrony dóbr osobistych*, [w:] *Dobra osobiste i ich ochrona w polskim prawie cywilnym*, red. J. S. Piątkowski, Wrocław 1986.
Zimny W., *Czy adresy e- mailowe są danymi osobowymi?*, „Biuletyn Ochrona Informacji" 2002, nr. 2.
Zimny W., *Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z dnia 25 sierpnia 2001 r.*, „ODO Biuletyn ABI" 2001, nr 21.
Zimny W., *Trudności z terminem „zbiór danych" w ustawie o ochronie danych osobowych,* „Rzeczpospolita" z 6 września 2000 r., nr 208.
Zubik M., *Powoływanie członków Rady Polityki Pieniężnej w świetle zasad kadencyjności oraz działalności organów państwa*, „Przegląd Sejmowy" 2005, nr 4.
Żermen J., Ochrona danych osobowych, „Gazeta Prawna" 1996, nr 60.

Polskie akty prawne

Konstytucja PRL z 22 lipca 1952 r. (Dz. U. Nr 33, poz. 232).
Konstytucja RP z 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483).
Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93).
Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. Nr 24, poz. 151).

Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993).
Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. Nr 24, poz. 141).
Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. Nr 31, poz. 214).
Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24).
Ustawa z dnia 29 kwietnia 1985 r. o Trybunale Konstytucyjnym (Dz. U. Nr 22, poz. 9).
Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. Nr 21, poz. 123).
Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. Nr 16, poz. 95).
Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. Nr 234, poz. 1997).
Ustawa z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz. U. Nr 114, poz. 493).
Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz. 83).
Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121, poz. 591).
Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. Nr 13, poz. 59)
Ustawa z 29 czerwca 1995 r. o statystyce publicznej (Dz. U. Nr 88, poz. 439).
Ustawa z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. Nr 98, poz. 602).
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883)
Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. Nr 140, poz. 938.).
Ustawa z dnia 19 listopada 1999 r. Prawo działalności gospodarczej (Dz. U. Nr 101, poz. 1178).
Ustawa z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka (Dz. U. Nr 6, poz. 69).
Ustawa z dnia 21 stycznia 2000 r., o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej (Dz. U. Nr 12, poz. 136).
Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. Nr 50, poz. 580)
Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł (Dz. U. Nr 116, poz. 1216).
Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (Dz. U. z 2003 r. Nr 153, poz.1505)
Ustawa z dnia 11 kwietnia 2001 r. o zmianie ustawy o doradztwie podatkowym oraz niektórych innych ustaw (Dz. U. Nr 49, poz. 474).
Ustawa z 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (Dz. U. Nr 110, poz. 1189)
Ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 100, poz. 1087).
Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198).
Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. Nr 74, poz. 676).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204).
Ustawa z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej (tekst jedn. Dz. U. z 2006 r. Nr 23, poz.1695).
Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 33, poz. 285).

Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 33, poz. 285).
Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. Nr 173, poz. 1807)
Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800).
Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565.).
Ustawa z dnia 30 czerwca 2005 r. o kinematografii (Dz. U. Nr 132, poz. 1111 z późn. zm.)
Ustawa z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708).
Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzecznika Praw Pacjenta (Dz. U. z 2012 r., poz. 159).
Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. Nr 234, poz. 1570).
Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 229, poz. 1497).
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).
Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. poz. 1662).
Ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz. U. poz. 195).
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 1 października 2001 r. zmieniające rozporządzenie w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 121, poz. 1306).
Rozporządzenia Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków (Dz. U. z 2002 r. Nr 5, poz. 46.).
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 94, poz. 923).
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024.).
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 maja 2008 r. w sprawie wzoru formularza wniosku o nadanie statusu uchodźcy (Dz. U. Nr 92, poz. 579).
Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. Nr 252, poz. 1697).
Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji.(Dz. U. z 2014 r., poz. 1934).
Uchwała Senatu RP z dnia 23 listopada 1990 r. regulamin Senatu (M. P. z 2002 r. Nr 54, poz. 741).
Uchwała Sejmu RP z dnia 30 lipca 1992 r. regulamin Sejmu Rzeczypospolitej Polskiej (M. P. z 2002 r. Nr 23, poz. 398).

Międzynarodowe akty prawne

Karta Narodów Zjednoczonych z dnia 26 czerwca 1945 r. (Dz. U. z 1947 r. Nr 23, poz. 90 z późn. zm.).
Powszechna Deklaracja Praw Człowieka i Obywatela z 10 grudnia 1948 r.
Europejska Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz. U. z 1998 r. Nr 147, poz. 962.).
Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966 r. **(**Dz. U. z 1977 r. Nr 38, poz. 167).
Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. z 2003 r. Nr 3, poz. 25).
Układ z Schengen z dnia 14 czerwca 1985 r. (Dz. U. L 350 z 30.12.2008)
Traktat o funkcjonowaniu Unii Europejskiej z dnia 11 grudnia 1991 r. (Dz. Urz. UE C 306 z 17.12.2007.).
Układ Europejski z dnia 16 grudnia 1991 r. (Dz. U. z 1994 r. Nr 11, poz. 38 z późn. zm.).
Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz. Urz. UE C 326 z 26.10.2012).

Akty prawa europejskiego

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. L Nr 281 z 23 listopada 1995 r.).
Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady Unii Europejskiej z 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym (Dz. Urz. L Nr 24 z 30 stycznia 1998 r.).
Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz. Urz. WE L 178 z 17.07.2000).
Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. WE L 201 z 31.07.2002).
Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 13.04.2006).
Rozporządzenie Parlamentu Europejskiego i Rady nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania konwencji dublińskiej.
Rozporządzenie Parlamentu Europejskiego i Rady 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 swobodnym przepływie tych danych (Dz. U. L 8 z 12.01.2001).
Rozporządzenie Parlamentu Europejskiego i Rady nr 343/2003 z dnia 18 lutego 2003 r. ustanawiające kryteria i mechanizmy określania Państwa Członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z Państw Członkowskich przez obywatela państwa trzeciego (Dz. Urz. UE L 50, z 25.02.2003 r.)

Decyzja Ramowa Rady 2008/997/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. Urz. L Nr 350 z 20.12.2008 r.).
Opinia 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych.

Inne akty prawne

Bundesgesetz über den Datenschutz BDSG; Federalna niemiecka ustawa o ochronie danych osobowych; Federalny Dziennik Ustaw I str 2.814; G. Verlag, Bundesdatenschutzgesetz: Bundesdatenschutzgesetz (BDSG),Auflage 2015.
Children's Online Privacy Protection Act; Ustawa o ochronie prywatności dzieci w sieci (15 U.S.C § 6501-6506).
Currency and Foreign Transactions Reporting Act, Bank Secrecy Act of 1970.
Driver's Privacy Protection Act; Ustawa o ochronie prywatności kierowcy (18 U.S.C § 2721).
Electronic Founds Transfer Act; Ustawa o elektronicznym przekazywaniu środków pieniężnych (15 U.S.C § 1693 i n.).
Personal Data Protection. Information on the Personal Data Act, Brochure Swedish Ministry Of Justice, s. 7, www.sweden.gov.pl.
Right to Financial Privacy Act; Ustawa o prawie do prywatności finansowej (12 U.S.C § 3401 i n.)
Telephone Consumer Protection Act; Ustawa o ochronie konsumentów usług telefonicznych (47 U.S.C § 227).
The Data act, 1973; Szwedzka ustawa o ochronie danych osobowych.

Orzecznictwo polskie

Orzeczenie TK z dnia 7 stycznia 1992 r., K 8/91, OTK 1992, nr 1, poz.5.
Uchwała TK z dnia 17 marca 1993 r., W 16/92, OTK w 1993 r., cz. I, s. 165.
Orzeczenie TK z dnia 28 maja 1997 r., sygn. K 26/96, OTK ZU 1997, nr 2, poz. 19.
Orzeczenie TK z dnia 24 czerwca 1997 r. K 21/96, OTK ZU 2 (11)1997, poz. 23.
Wyrok TK z dnia 19 maja 1998 r., U 5/97, OTK 1998, nr 4, poz. 46.
Wyrok TK z dnia 24 czerwca 1998 r., K 3/98, OTK ZU 1998, nr 4, poz. 52.
Wyrok TK z dnia 21 października 1998 r., K 24/98, OTK 1998, Nr 6, poz. 97.
Wyrok TK z dnia 17 listopada 1998, K 42/97, OTK ZU 1998, nr 7, poz. 113.
Wyrok TK z dnia 29 stycznia 2002 r., K 19/01, OTK-A 2002, Nr 1, poz. 1.
Wyrok TK z dnia 19 lutego 2002 r., U 3/01, Dz. U. 2002 Nr 19, poz. 197.
Wyrok TK z dnia 10 kwietnia 2002 r., K 26/00, OTK-A 2002, nr 2, poz. 18.
Wyrok TK z dnia 20 listopada 2002 r., K 41/02. M.P. 2002 Nr 56, poz. 763.
Wyrok TK z dnia 3 marca 2003 r., K 7/01, OTK-A 2003, Nr 3, poz. 19.
Wyrok TK z dnia 12 grudnia 2005 r., K 32/04, OTK-A 2005, Nr 11, poz. 132.
Orzeczenie TK z dnia 23 marca 2006 r. sygn. K 4/06, OTK ZU2006, seria A, nr 3, poz. 32.
Wyrok TK z dnia 28 września 2008 r., SK 52/05, Z.U. 125/7/A/2007.
Wyrok TK z dnia 15 stycznia 2009 r., K 45/07; OTK – A 2009, nr 1, poz. 3.
Postanowienie TK z dnia 8 czerwca 2009 r., SK 26/07; OTK-A 2009, nr 6, poz. 92.
Wyrok SN z dnia 2 czerwca 1972 r., I CR 42/72, OSPiKA 1973, nr 7-8, poz. 152.
Wyrok SN z dnia 18 stycznia 1984 r., I CR 400/83, OSNC 1984, nr 11, poz. 195.
Wyrok SN z dnia 24 maja 1999 r., II CKN 349/98, OSNC 1999, nr 12, poz. 212.
Postanowienie SN z dnia11 grudnia 2000 r., II KKN 438/00, *LexPolonica* nr 349110; Biuletyn SN 2001, nr 2.
Wyrok SN z dnia 5 września 2001 r., sygn. akt I CKN 1159/00, OSNC 2002 nr 5, poz. 67.

Wyrok SN z dnia 19 listopada 2003 r. , sygn. I PK 590/02, OSNP 2004, nr 20, poz. 351.
Wyrok SN z dnia 2 października 2006 r., V KK 243/06, OSNKW 2006, nr 12, poz.113.
Wyrok NSA z dnia 9 listopada 1999 r., II SAB 153/ 99, niepublikowany
Wyrok NSA w Warszawie z dnia 12 maja 2000 r., II SA 52/00, niepublikowany.
Wyrok NSA z dnia 19 kwietnia 2000 r., II SA 2619/99, „Wokanda" 2000, nr 7, s. 43.
Wyrok NSA z dnia 17 listopada 2000 r., sygn. akt II SA 1860/00, niepublikowany.
Wyrok Sądu Apelacyjnego w Krakowie z dnia 19 grudnia 2000 r., I ACa 794/00.
Wyrok NSA w Warszawie z dnia 2 marca 2001 r., II SA 401/00, LexPolonica nr 352750; „Wokanda" 2001, nr 9.
Wyrok NSA w Warszawie z dnia 28 listopada 2002 r., II SA 3389/01, LEX nr 241604.
Wyrok NSA w Gdańsku z dnia 20 lutego 2003 r., II SA/Gd 597/00, niepublikowany.
Wyrok NSA z dnia 27 listopada 2003 r., II SA 209/03.
Wyrok NSA w Warszawie z dnia 13 kwietnia 2007 r., II SA/Wa 2079/06, niepublikowany.
Wyrok NSA w Warszawie z dnia 28 stycznia 2008 r., I OSK 1365/06, LEX nr 453453.
Wyrok NSA z dnia 26 stycznia 2009 r., I OSK 174/08, LEX nr 478301.
Wyrok NSA z dnia 15 marca 2010 r., I OSK 756/09.
Wyrok NSA z dnia 6 września 2011 r., sygn. akt I OSK 1476/10.
Wyrok NSA z dnia 18 października 2011 r., sygn. akt I OSK 1742/10.
Wyrok NSA z dnia 30 listopada 2011 r., sygn. akt I OSK 2118/10.
Postanowienie NSA z dnia 30 maja 2012 r., sygn. I OSK 1109/12.
Wyrok WSA w Warszawie z dnia 22 stycznia 2004 r., II SA/Wa 3498/02, niepublikowany.
Wyrok WSA w Warszawie z dnia 3 czerwca 2004 r. , II SA/Wa 225/04, niepublikowany.
Wyrok WSA z dnia 17 listopada 2004 r., II SA/Wa 887/04.
Wyrok WSA w Warszawie z dnia 13 czerwca 2006 r., II SA/Wa 2016/05, niepublikowany.
Wyrok WSA w Warszawie z dnia 3 marca 2009 r., sygn. akt II SA/Wa 1495/08, LEX nr 530464.

Orzecznictwo ETPC

Orzeczenie z dnia 22 października 1981 r. w sprawie Dudgeon v. Zjednoczone Królestwo; A. 45, pkt 52.
Orzeczenie z dnia 26 marca 1987 r. w sprawie Leander v. Szwecja; skarga nr 9248/81.
Orzeczenie z dnia 7 lipca 1989 r. w sprawie Gaskin v. Wielka Brytania; skarga nr 10454/83.
Orzeczenie z dnia 16 grudnia 1992 r. w sprawie Wakefield v. Wielka Brytania, A.251-B, pkt 29.
Orzeczenie z dnia 25 marca 1993 r. w sprawie Costello-Roberts v. Zjednoczone Królestwo; A.247-C, pkt 36.
Orzeczenie z dnia 28 października 1994 r. w sprawie Murray v. Wielka Brytania; A.300-A, pkt 86.
Orzeczenie z dnia 25 listopada 1994 r. w sprawie Stjerna v. Finlandia; A.299-B.
Orzeczenie z dnia 24 października 1996 r. w sprawie Guillot v. Francja; RJD 1996, pkt 22.
Orzeczenie z dnia 27 sierpnia 1997 r. w sprawie M. S. v Szwecja, Reports 1997, skarga nr 20837/92.
Orzeczenie z dnia 16 lutego 2000 r. w sprawie H. Amann v. Szwajcaria; sprawa nr 27798/5, LEX nr 76904; I CR 252/68, OSNC 1970, Nr 1, poz. 18.
Orzeczenie z dnia 4 maja 2000 r. w sprawie Rotaru v. Rumunia; skarga nr 28341/95.
Orzeczenie z dnia 13 lutego 2003 r. w sprawie Odievre v. Francja; Wielka Izba, skarga nr 42326/98.
Orzeczenie z dnia 22 lipca 2003 r w sprawie Y.F. v. Turcja; skarga nr 24209/94.
Orzeczenie z dnia 16 lutego 2006 r. w sprawie Turek v. Słowacja; skarga nr 57986/00.

Orzeczenie z dnia 8 grudnia 2009 r. w sprawie Muñoz Díaz v. Spain; skarga 49151/07.
Wyrok z dnia 9 marca 2010 r. w sprawie Komisja Europejska v. Republika Federalna Niemiec; sprawa C-518/07.
Orzeczenie z dnia 6 października 2015 r. w sprawie Maximilian Schrems v. Data Protection Commissioner; C-362/14.

Inne dokumenty

„Biuletyn Komisji Konstytucyjnej Zgromadzenia Narodowego", nr XXVI.
Dokument Grupy Roboczej nr 105 z 19 stycznia 2005 r.; *Working dokument on data protection issues related to RFID technology.*
Europejski Inspektor Ochrony Danych a ochrona danych osobowych w instytucjach i organach Wspólnoty, Wspólnoty Europejskie 2009, Urząd Publikacji Unii Europejskiej 2009.
Hustinx P. J., *Rola Europejskiego Inspektora Ochrony Danych Osobowych w strukturach Unii Europejskiej zajmujących się ochroną danych*, Wykład Europejskiego Inspektora Ochrony Danych Osobowych, Warszawa 2004; dostępny na str: http://www.giodo.gov.pl/1520090/id_art/1013/j/pl/.
Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie „Europejskiej Agendy Cyfrowej" COM (2010) 245, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PL:PDF.
Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności- COM (2007) 228,http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52007DC0228&from=PL.
Konarski X., Opinia prawna dołączonej do stanowiska Polskiej Izby Informatyki i Komunikacji z 18 lutego 2008 r. do przedłożonego Sejmowi prezydenckiego projektu ustawy o zmianie ustawy o ochronie danych osobowych z 21 grudnia 2007 r., druk sejmowy nr 488 z 21 grudnia 2007 r., s. 90, dostępny na stronie: http://ww.sejm.gov.pl.
Notatka Komisji Europejskiej z 12.04.2014 r., http://www.giodo.gov.pl/259/id_art/7714/j/pl.
Projekt Dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych.
Projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.
Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych sporządzony w Strasburgu 8 listopada 2001 r. (Dz. U. z 2006 r. Nr 3, poz.15).
Rapport explicatif concernant la Convention pour la protection des personnes à l'ègard du traitement automatisè des donnèes à caractère personnel, Strasburg 1981.
Raport wyjaśniający do Konwencji nr 108; dostępny na stronie: http://www.giodo.gov.pl/230/id_art/1685/j/pl/.
Rekomendacja Organizacji Współpracy gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami.
Sprawozdanie nr 78/2012 na temat ochrony danych osobowych; informacje o pracach w Parlamencie Europejskim.
Sprawozdanie z działalności Europejskiego Inspektora Ochrony Danych za rok 2004 r.
Sprawozdanie z działalności Europejskiego Inspektora Ochrony Danych za rok 2006 r.

Sprawozdanie z działalności Europejskiego Inspektora Ochrony Danych za rok 2011r.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 1999.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2000.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2002.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2003.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2007.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2011.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2012.
Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013.
Statut stanowiącym załącznik do rozporządzenia Prezydenta RP z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 225, poz. 1350).
Wytyczne OECD z 1980 r., pkt 4, lit. a.
Wytyczne ONZ z 1990 r., pkt 6.
Zarządzenie nr 2/2012 Generalnego Inspektora Ochrony Danych Osobowych z dnia 04 stycznia 2012 r. w sprawie przyjmowania i rozpatrywania skarg i wniosków w Biurze Generalnego Inspektora Ochrony Danych Osobowych.
Zarządzenie nr 3/2012 Generalnego Inspektora Ochrony Danych Osobowych z dnia 18 lutego 2013 r. w sprawie zmiany Regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych.

Ważniejsze strony internetowe

https://www.privacyconference2015.org
http://www.giodo.gov.pl
http://www.edps.europa.eu
http://www.ec.europa.eu
http://www.oecd.org
https://secure.edps.europa.eu