KAROLINA MAŁAGOCKA

- Akademia Leona Koźmińskiego
- e-mail: kmalagocka@kozminski.edu.pl
- ORCID: 0000-0003-2544-2094

PRYWATNOŚĆ PO COVID-19. EKSPLORACJA KONCEPCJI CYFROWEJ WOLNOŚCI I JEJ ZNACZENIA PO PANDEMII

1. Wstęp

Prywatność to złożone i wieloaspektowe pojęcie, które ewoluowało w odpowiedzi na zmieniające się normy społeczne, wartości kulturowe i postęp technologiczny. Jest to koncepcja, którą trudno zdefiniować, ale można ją rozumieć jako nieodłączne pragnienie jednostek, by być wolnym od kontroli i nadzoru ze strony innych. Obejmuje ona zarówno fizyczne, jak i niematerialne granice, które jednostki wyznaczają, aby chronić się przed ingerencją. W rezultacie, prywatność jest badana w wielu dyscyplinach, w tym w prawie, psychologii, filozofii i socjologii. Niniejszy przegląd przyjmuje podejście porównawcze i opisowe, którego celem jest przedstawienie kontekstu zmian w postrzeganiu samego pojęcia, podejmowanych już prób wyznaczania granic i rozwoju prawa dotyczących prywatności z przyjęciem perspektywy globalnej, uwzględniającej zarówno regulacje jak i dorobek akademicki z różnych obszarów. Wiele badań przeprowadzonych w tej dziedzinie podkreśla wyzwanie, jakim jest zdefiniowanie i ustalenie jej granic, jak również brak konsensusu co do znaczenia prywatności i sposobu jej analizowania (Kuner i in. 2011; Moore 2008). W poniższej pracy, bazującej na metodzie przeglądu literatury oraz analizy dokumentów, przedstawione są propozycje rozumienia samego pojęcia, następnie istniejące regulacje prawne, a także związek pomiędzy prywatnością a pandemią COVID-19, ze szczególnym uwzględnieniem rozwi-

janych i adoptowanych rozwiązań cyfrowych. W ostatniej części tekstu opisane są trzy koncepcje, które nabrały szczególnego znaczenia w dobie przyspieszonej cyfryzacji, czyli: kontrola nad informacjami osobistymi, wolność od nadzoru oraz prawo do autonomii cielesnej.

2. Rozumienie pojęcia prywatności

Współcześnie, ze względu na rosnące znaczenie technologii informatycznych, prywatność może być rozumiana i definiowana jako zdolność jednostek do kontrolowania gromadzenia, wykorzystywania i ujawniania informacji prywatnych oraz do podejmowania świadomych decyzji o tym, jak ich dane są udostępniane i stosowane przez innych (Rengel 2013; Bajpai, Weber 2017; Jack, Sovannaroth, Dell 2019). Istnieje kilka uzasadnień dla takiego rozumienia i definicji prywatności. Po pierwsze, uznaje się w niej, że dane osobowe są cennym i wrażliwym dobrem, które należy chronić. W dobie cyfrowej transformacji dane są stale gromadzone, przechowywane i analizowane przez rządy, korporacje i inne podmioty w szerokim zakresie, w tym do celów tak różnych jak marketing, personalizacja, ale też profilowanie, nadzór czy bezpieczeństwo narodowe. Możliwość kontrolowania przez osoby fizyczne wykorzystania ich danych osobowych jest zatem niezbędna do ochrony ich autonomii, godności i dobrobytu. Jednocześnie są one jednak cennym zasobem, który przynosi korzyści nie tylko w biznesie, ale także ogółowi społeczeństwa. Udostępnianie danych dotyczących lokalizacji może pomóc w optymalizacji przepływu ruchu drogowego, a ujawnienie stanu zdrowia jest w stanie wspierać zarządzanie alokacją sił medycznych czy też ograniczanie rozprzestrzeniania się wirusów. Jednak gotowość do dzielenia się informacjami może być związana z kosztami emocjonalnymi i poznawczymi, a osoby dla których są one wysokie lub nawet na poziomie, który uznają za niekorzystny lub wręcz nieakceptowalny, mogą ograniczać skuteczność działań publicznych opartych na przetwarzaniu informacji (Rockenbach, Sadrieh, Schielke 2020; Saglam, Nurse, Hodges 2022). Po drugie, takie rozumienie prywatności uznaje, że prywatność nie jest prawem absolutnym, ale raczej równoważeniem konkurujących interesów (Krotoszynski 2016; Alibeigi, Munir, Karim 2019; Seubert, Becker 2021). Złożoność prywatności, która obejmuje kontrastujące cechy i definicje, stanowi wyzwanie w regulowaniu tego obszaru. Chociaż jednostki mają prawo do pry-

watności, to może ono wymagać zrównoważenia z innymi interesami, takimi jak bezpieczeństwo publiczne, narodowe lub ochrona własności intelektualnej. Uznanie potrzeby równowagi interesów jest ważne dla zapewnienia, że ochrona prywatności jest praktyczna i skuteczna. Po trzecie, w tej definicji prywatności uznaje się, że prywatność to nie tylko poufność, ale także kontrola. Osoby powinny mieć prawo do podejmowania świadomych decyzji o tym, jak ich dane osobowe są udostępniane, agregowane i stosowane, a także powinny mieć możliwość wycofania swojej zgody lub zażądania usunięcia informacji, jeśli tak postanowią. Jedną z propozycji konceptualizowania prywatności (lub prawa do prywatności) jest uznanie jej za „pewien rodzaj kontroli nad pewnymi sprawami" (Lundgren 2020:16), co oczywiście samo w sobie stanowi dość mało precyzyjne ujęcie. Może być ono rozumiane dalej jako niezbędność kontroli nad informacjami prywatnymi dla ochrony autonomii i godności jednostki oraz dla zapewnienia, że jednostki nie są poddawane nieuzasadnionym i arbitralnym formom nadzoru (Menges 2020; Haney, Acar, Furman 2021; Sharma, Dyer, Bashir 2021). Obecnie dostrzegana erozja prywatności jest napędzana przez połączenie interesów komercyjnych i politycznych. Pojawiające się argumenty o zwiększaniu bezpieczeństwa można uznać jednak za niekompletne, ponieważ nie uwzględniają złożoności ludzkiej natury (Blundell 2020).

Podsumowując, prywatność można dziś rozumieć i definiować jako zdolność osób fizycznych do kontrolowania agregacji, zastosowania i ujawniania informacji o nich oraz do podejmowania świadomych decyzji o tym, jak są one udostępniane i wykorzystywane przez innych. Takie rozumienie znajduje uzasadnienie w uznaniu informacji prywatnych za cenne dobro, które powinno być chronione poprzez zrównoważenie konkurujących ze sobą interesów jednostek i organizacji. Chroniąc prywatność jednostek, możemy zapewnić, że informacje osobowe są wykorzystywane w sposób odpowiedzialny, etyczny i społecznie korzystny, przy jednoczesnym poszanowaniu autonomii, godności i dobrobytu jednostki.

3. Regulacje dotyczące prywatności

W Unii Europejskiej głównym prawem dotyczącym prywatności konsumentów jest Rozporządzenie o ochronie danych osobowych (General Data Protection Regulation, GDPR). Weszło w życie w 2018 roku i ma zastosowanie do wszystkich

państw członkowskich UE oraz należących do Europejskiego Obszaru Gospodarczego. Główne założenia GDPR to ochrona prywatności i danych osobowych obywateli UE oraz zapewnienie im większej kontroli nad ich danymi (Kuner et al. 2021; Andrew, Baker 2021). Rozporządzenie wymaga od firm uzyskania wyraźnej zgody osób fizycznych na gromadzenie i przetwarzanie ich danych, ujawnienia wszelkich naruszeń oraz umożliwienia osobom fizycznym dostępu do swoich danych, ich sprostowania i usunięcia. GDPR nakłada również surowe kary za nieprzestrzeganie przepisów, w tym grzywny w wysokości do 4% globalnego przychodu firmy.

W Stanach Zjednoczonych nie istnieje prawo federalne, które w szczególny sposób odnosi się do prywatności konsumentów. Zamiast tego różne stany uchwaliły swoje własne regulacje. Najbardziej znaczącą z nich jest California Consumer Privacy Act (CCPA), która weszła w życie w 2020 roku. CCPA wymaga, aby firmy ujawniały, jakie dane osobowe gromadzą, dawały osobom fizycznym prawo do dostępu, usuwania i rezygnacji ze sprzedaży ich danych, a także nakłada kary za nieprzestrzeganie przepisów (Pardau 2018; Solove, Schwartz 2020). Ponadto niektóre sektory, takie jak opieka zdrowotna i finanse, podlegają regulacjom branżowym, ze szczególnym wskazaniem na Health Insurance Portability and Accountability Act (HIPAA) i Gramm-Leach-Bliley Act (GLBA), które określają specyficzne obowiązki przy zbieraniu i przetwarzaniu danych uznanych za wrażliwe.

W Chinach głównym prawem dotyczącym prywatności konsumentów jest Ustawa o ochronie informacji osobistych (Personal Information Protection Law, PIPL), która weszła w życie w listopadzie 2021 roku (The Diplomat 2021). Ustawa ma na celu ochronę prywatności osób fizycznych i danych osobowych przed gromadzeniem, wykorzystywaniem i ujawnianiem przez firmy. W przeciwieństwie do wcześniejszych przepisów, takich jak Ustawa o cyberbezpieczeństwie, Ustawa o bezpieczeństwie danych i Ustawa o handlu elektronicznym, PIPL zawiera jasne definicje informacji osobowych i wrażliwych danych osobowych, a także wprowadza zasadę minimalizacji. Podobnie jak unijne GDPR, PIPL określa, że firmy powinny gromadzić jedynie minimalną ilość danych osobowych niezbędnych do osiągnięcia zamierzonego celu, co zmniejsza możliwość niewłaściwego wykorzystania danych osobowych w przyszłości. Wymaga od firm uzyskania zgody osób fizycznych na gromadzenie i przetwarzanie ich danych, ujawnienia celu i zakresu gromadzenia danych oraz umożliwienia osobom fizycznym dostępu do swoich da-

nych, ich poprawiania i usuwania. PIPL nakłada również kary za nieprzestrzeganie przepisów, w tym grzywny i zawieszenie działalności gospodarczej.

W innych obszarach, takich jak region Azji i Pacyfiku oraz Ameryka Łacińska, istnieje wiele przepisów i regulacji dotyczących prywatności, które różnią się w zależności od kraju. Niektóre państwa przyjęły przepisy podobne do GDPR, podczas gdy inne mają słabszą ochronę prywatności. W trakcie pandemii COVID-19 i po niej nastąpiły zmiany w przepisach dotyczących prywatności, takie jak złagodzenie niektórych wymogów dotyczących przetwarzania danych do celów zdrowia publicznego. Ogólnie jednak nacisk na ochronę danych osobowych i prawa do prywatności pozostał priorytetem dla rządów i organów regulacyjnych na całym świecie.

4. Prywatność a pandemia COVID-19

Pandemia COVID-19 doprowadziła do podjęcia przez rządy na całym świecie bezprecedensowych środków mających na celu kontrolę rozprzestrzeniania się wirusa. Wiele z nich miało znaczący wpływ na swobody obywatelskie, a także budziło obawy o zakres cyfrowego nadzoru i możliwości jednostek w decydowaniu o podleganiu tym zasadom. Skłania to do rozważań o tym, że koncepcja cyfrowo ograniczonej wolności zyskała na aktualności i znaczeniu w następstwie pandemii. Technologie cyfrowe odegrały zasadniczą rolę w umożliwieniu rządom monitorowania i śledzenia przemieszczania się obywateli w czasie pandemii. Aplikacje do śledzenia zostały wykorzystane do ostrzegania osób, które miały kontakt z kimś, kto uzyskał pozytywny wynik testu na obecność COVID-19, oraz do monitorowania przestrzegania nakazów kwarantanny i izolacji. Chociaż środki te były skuteczne w kontrolowaniu rozprzestrzeniania się wirusa, wzbudziły również obawy dotyczące prywatności i nadzoru (Bengio i in. 2021). Jedną z kluczowych obaw jest to, że wykorzystanie tych technologii może stać się trwałe, a rządzący zauważą zalety dalszego korzystania z aplikacji do śledzenia kontaktów i innych narzędzi monitorowania ruchów obywateli, nawet gdy nie ma już zagrożenia dla zdrowia publicznego.

Kolejna obawa dotyczy potencjalnie dyskryminacyjnego charakteru technologii, które znalazły zastosowanie w czasie pandemii. Aplikacje do śledzenia kontaktów mogą być mniej skuteczne na obszarach, gdzie ludzie nie mają dostępu do

smartfonów lub niezawodnych połączeń internetowych. Może to prowadzić do sytuacji, w której osoby w niektórych społecznościach są nieproporcjonalnie dotknięte pandemią i środkami podejmowanymi w celu jej kontrolowania.

Zastosowanie technologii cyfrowych do egzekwowania nakazów kwarantanny i izolacji wzbudziło również obawy dotyczące należytego procesu i rządów prawa. W niektórych krajach osoby, które uzyskały pozytywny wynik testu na obecność COVID-19 lub były w bliskim kontakcie z osobą, która uzyskała pozytywny wynik, zostały poddane przymusowej kwarantannie w obiektach zarządzanych przez rząd. Chociaż w niektórych przypadkach może to być konieczne, aby zapobiec rozprzestrzenianiu się wirusa, rodzi to również pytania o legalność tych środków i prawa osób, które są nimi dotknięte (Chan, Saqib 2021). Obawy o prywatność mogą wyjaśniać niechęć do pobierania i używania aplikacji do śledzenia kontaktów, podczas gdy jednocześnie występowało poczucie zagrożenia rozwojem epidemii (Hassandoust, Akhlaghpour, Johnston 2021).

Podsumowując, zastosowanie technologii cyfrowych do monitorowania i śledzenia ruchów obywateli wzbudziło poważne obawy dotyczące prywatności, nadzoru, dyskryminacji, sprawiedliwego procesu i dostępu do technologii. Chociaż środki te mogą być konieczne w krótkim okresie, aby kontrolować rozprzestrzenianie się wirusa, ważne jest, aby rządy stosowały przejrzyste i zgodne z obowiązującymi regulacjami zasady dotyczące technologii cyfrowych ograniczających swobodę. Istotna wydaje się również, nawet bardziej niż przed wybuchem pandemii COVID-19, kwestia zapewnienia możliwie szerokiego i sprawiedliwego dostępu do technologii cyfrowych, tak aby każdy mógł skorzystać z możliwości, jakie one oferują.

5. Prywatność w dobie cyfrowej transformacji

Wpływ systemów i technologii komputerowych na prywatność i swobody obywatelskie stwarza sytuację, w której zasadne wydaje się rozwijanie różnych koncepcji rozumienia prywatności. W niniejszej pracy proponuję bliższe przyjrzenie się trzem koncepcjom, których głównymi założeniami są:

- kontrola nad informacjami osobowymi,
- wolność od inwigilacji,
- prawo do autonomii cielesnej.

Kontrola nad informacjami osobowymi to koncepcja, która podkreśla znaczenie możliwości określenia przez osoby fizyczne sposobu, w jaki ich dane osobowe są gromadzone, wykorzystywane i udostępniane przez innych. Wraz z rozwojem technologii cyfrowych i Internetu, nastąpił okres aprecjacji danych, stały się one bardziej dostępne i cenne dla podmiotów trzecich, takich jak korporacje i rządy (Brough, Martin 2021; Johnson, Shriver, Goldberg 2023). Kontrola ma zatem zasadnicze znaczenie dla zapewnienia, że jednostki mają możliwość ochrony swojej prywatności i ograniczenia wykorzystania swoich danych osobowych w zakresie, który uznają za stosowny. Systemy i technologie komputerowe ułatwiły z jednej strony pozyskiwanie, ale jednocześnie umożliwiły tworzenie ustawień prywatności w niektórych usługach, a także stosowanie narzędzi szyfrowania. Wciąż jednak sytuacja daleka jest od równowagi, gdyż korzystający z rozwiązań cyfrowych nie zawsze posiadają pełną wiedzę o sposobach agregacji danych, brakuje też umiejętności w zarządzaniu dostępem, a czasem także alternatywnych metod zaspokojenia potrzeb, np. obserwujemy dominację wybranych systemów mobilnych lub platform społecznościowych w poszczególnych krajach.

Jednym z przykładów wykorzystania nowych technologii, który ilustruje, jak konsumenci przynajmniej częściowo stracili kontrolę nad swoimi danymi, jest adopcja rynkowa inteligentnych urządzeń domowych, takich jak inteligentne głośniki, kamery bezpieczeństwa i termostaty. Są one zaprojektowane do zbierania i przekazywania dużych ilości danych o działaniach, nawykach i preferencjach korzystających (Abdi i in. 2021). Z jednej strony oferują wygodę i rozbudowaną funkcjonalność, jednak stanowią również istotne zagrożenie dla prywatności konsumentów. Na przykład inteligentne głośniki, takie jak Alexa firmy Amazon czy Google Home, stale nasłuchują poleceń głosowych, co oznacza, że bez przerwy rejestrują i przekazują dane audio do swoich serwerów. Dane te mogą obejmować osobiste rozmowy, wrażliwe informacje i inne prywatne szczegóły, którymi osoby fizyczne niekoniecznie chcą się dzielić się z podmiotami zewnętrznymi. Podobnie inteligentne kamery bezpieczeństwa przeznaczone do monitorowania domów i nieruchomości są przystosowane do przesyłania danych wideo do zdalnych serwerów w celu przechowywania i analizy. Może to obejmować nagrania z codziennych czynności osób fizycznych, w tym ich wejścia i wyjścia, interakcje z innymi, a także szczegóły z życia, w tym rutyny dnia codziennego, które podlegają agregacji, przetworzeniu, a w przyszłości mogą służyć do celów rozwoju technologii czy uczenia maszynowego.

Problem z tymi urządzeniami polega na tym, że konsumenci często mają ograniczoną kontrolę nad gromadzonymi i przesyłanymi przez nie danymi. Na przykład wiele inteligentnych urządzeń domowych jest skonfigurowanych tak, aby automatycznie przesyłać dane na serwery producenta, przy niewielkim lub żadnym wkładzie ze strony konsumenta. Ponadto wielu producentów stosuje niejasne lub mylące polityki prywatności, które utrudniają zrozumienie, w jaki sposób dane są wykorzystywane i udostępniane. W rezultacie konsumenci często nie są świadomi pełnego zakresu gromadzonych informacji ani tego, jak są one przetwarzane. Ten brak kontroli nad swoimi danymi może prowadzić do szeregu zagrożeń prywatności, w tym kradzieży tożsamości, oszustw i innych form wykorzystania (Solove 2021; Zainuddin i in. 2021).

Wolność od nadzoru to kolejna proponowana koncepcja rozumienia prywatności, która podkreśla znaczenie wolności jednostek od nieuzasadnionego nadzoru (Campbell, Brakel 2015; Andrew, Baker 2021). Wraz z pojawieniem się technologii cyfrowych, rządy i korporacje coraz częściej wykorzystują je do monitorowania aktywności jednostek w sieci i poza nią. Może to prowadzić do osłabienia wolności słowa i politycznego sprzeciwu, ponieważ jednostki mogą wahać się przed wyrażaniem kontrowersyjnych opinii lub angażowaniem się w aktywizm polityczny z obawy przed byciem zidentyfikowanym.

Jednym z przykładów wykorzystania nowych technologii, który ilustruje, w jaki sposób konsumenci mają obecnie poważnie ograniczone prawo do uwolnienia się od nadzoru państwa i jego instytucji, jest rosnące wykorzystanie danych biometrycznych do kontroli ruchu granicznego, zwłaszcza w kontekście pandemii COVID-19. W odpowiedzi na rosnące zagrożenie wirusem rządy w wielu krajach na świecie wprowadziły bardziej rygorystyczne środki, w tym wykorzystanie danych biometrycznych, takich jak rozpoznawanie twarzy i skanowanie tęczówki, w celu identyfikacji i śledzenia osób przekraczających granice. W Indiach rząd wdrożył oparty na biometrii system identyfikacji zwany Aadhaar, który łączy dane biometryczne osób z unikalnym numerem identyfikacyjnym, który jest wykorzystywany do różnych usług rządowych, w tym do kontroli granicznej. System ten został skrytykowany ze względu na umożliwienie nadzoru rządowego i ograniczenia prawa do prywatności osób fizycznych. Podobnie w Stanach Zjednoczonych Agencja Ochrony Celnej i Granicznej wdrożyła na kilku lotniskach i przejściach granicznych technologię rozpoznawania twarzy w celu weryfikacji tożsamości osób. Chociaż technologia ta ma na celu usprawnienie procedur kontroli granicznej,

budzi ona również obawy dotyczące nadzoru rządowego i możliwości nadużywania danych biometrycznych osób fizycznych. Ponadto wykorzystanie danych biometrycznych do kontroli ruchu granicznego może również pogłębić istniejące nierówności społeczne, zwłaszcza w przypadku osób ze społeczności zmarginalizowanych, które mogą mieć ograniczony dostęp do usług rządowych lub mogą być narażone na dyskryminację ze względu na swoją rasę lub pochodzenie etniczne. W tym wypadku warto podkreślić, że dane te mogą zostać zagregowane z innymi posiadanymi przez władzę informacjami oraz służyć do ograniczania wolności w przemieszczaniu się osób.

Innym przykładem wykorzystania nowych technologii, który ilustruje, w jaki sposób konsumenci mają obecnie poważnie ograniczone prawo do uwolnienia się od nadzoru państwa, jest rosnące wykorzystanie technologii nadzoru w kontekście protestów i ruchów społecznych. W ostatnich latach organy ścigania coraz częściej stosują technologie takie jak rozpoznawanie twarzy, czytniki tablic rejestracyjnych i monitorowanie mediów społecznościowych, w celu śledzenia protestów i ruchów społecznych. W założeniu przyjęte rozwiązania mają wspierać istotne społecznie cele, takie jak utrzymanie bezpieczeństwa i porządku publicznego, zapobieganie aktom agresji oraz terroryzmowi, jednocześnie jednak stanowią one również istotne zagrożenie dla prywatności osób i mogą ograniczać ich możliwości korzystania z prawa do wolności słowa i pokojowych zgromadzeń. Podczas protestów znanych jako sprawa George'a Floyda w Stanach Zjednoczonych w 2020 r. organy ścigania wykorzystały rozpoznawanie twarzy i inne technologie nadzoru do identyfikacji i śledzenia protestujących, co wywołało obawy dotyczące nadzoru rządowego i możliwości nadużywania danych osób fizycznych (Culver, McLeod 2023). Podobnie w Hongkongu rząd wykorzystał rozpoznawanie twarzy i inne technologie do monitorowania i śledzenia protestujących, co doprowadziło do obaw o naruszenie prywatności i inwigilację ze strony rządu. W celu ograniczenia pojawiających się kontrowersji istotne wydaje się opracowanie regulacji, a także kodeksów dobrych praktyk, które nadają priorytet prawom do prywatności osób fizycznych i ograniczają możliwość nadużywania technologii nadzoru. Może to obejmować wdrożenie ścisłych mechanizmów kontroli nad stosowaniem tych technologii przez organy ścigania, ograniczenie gromadzenia i zatrzymywania danych oraz zapewnienie przejrzystości i odpowiedzialności w zakresie stosowania tych technologii, również do profilowania czy w celu doskonalenia działania algorytmów.

Prawo do autonomii cielesnej to koncepcja, która podkreśla znaczenie wolności jednostek od niechcianej lub nieuzasadnionej ingerencji związanej z ich ciałem. Wraz z rozwojem technologii biometrycznych, takich jak rozpoznawanie twarzy i analiza DNA, dane dotyczące fizyczności stały się bardziej dostępne i cenniejsze dla podmiotów trzecich. Prawo do autonomii cielesnej ma zatem zasadnicze znaczenie dla zapewnienia jednostkom możliwości ochrony prywatności (Al-Turjman, Zahmatkesh, Shahroze 2022; Lin 2022). Jednym z przykładów wykorzystania nowych technologii, który ilustruje, jak konsumenci mają obecnie ograniczone prawo do autonomii cielesnej, jest rosnące wykorzystanie technologii rozpoznawania twarzy zarówno przez podmioty prywatne, jak i rządowe. Technologia rozpoznawania twarzy wykorzystuje dane biometryczne do identyfikacji osób na podstawie ich rysów twarzy i w ostatnich latach stała się coraz bardziej wszechobecna. Jej stosowanie umożliwia identyfikację osób bez ich wiedzy lub zgody, często na odległość i może być wykorzystywana do śledzenia ruchów i działań osób w czasie rzeczywistym. Departamenty policji w Stanach Zjednoczonych i innych krajach stosują technologię rozpoznawania twarzy do identyfikacji podejrzanych i śledzenia ruchów osób, często bez nakazu lub innego uzasadnienia prawnego. Ponadto prowadzone i opisywane badania z zastosowaniem technologii rozpoznawania twarzy wykazują niepokojące konkluzje, że jest mniej dokładna w przypadku identyfikacji osób o ciemniejszym kolorze skóry, co może skutkować nieproporcjonalnym i dyskryminacyjnym traktowaniem grup mniejszościowych (Bacchini, Lorusso 2019; Castelvecchi 2020; Waelen 2023). Może to nasilić istniejące uprzedzenia społeczne i jeszcze bardziej ograniczyć autonomię cielesną jednostek. Podsumowując, coraz szersze zastosowanie technologii rozpoznawania twarzy jest przykładem tego, jak konsumenci mają obecnie poważnie ograniczone prawo do autonomii cielesnej w kontekście wpływu systemów komputerowych i technologii na prywatność. Technologia ta może być wykorzystywana do identyfikowania i śledzenia osób bez ich wiedzy lub zgody, a także może być stosowana w sposób nieproporcjonalnie wymierzony w grupy mniejszościowe. Istotne w tym kontekście wydaje się, aby decydenci, zanim podejmą decyzję o szerokiej adopcji, przyjęli regulacje obligujące jej twórców do uwzględniania etycznych implikacji rozpoznawania twarzy oraz opracowali przepisy i najlepsze praktyki, które priorytetowo traktują autonomię ciała i prawo do prywatności (Kostka, Steinacker, Meckel 2021; Smith, Miller 2022).

Podsumowując, dynamiczny rozwój i coraz szersze zastosowanie systemów komputerowych i technologii cyfrowych doprowadziły do zaproponowania różnych

koncepcji rozumienia prywatności. Kontrola nad informacjami osobistymi, wolność od nadzoru i prawo do autonomii cielesnej to trzy z nich, które mają zasadnicze znaczenie dla zapewnienia jednostkom możliwości ochrony ich prywatności oraz zachowania autonomii i godności w coraz bardziej cyfrowym i wzajemnie połączonym świecie. Niniejszy artykuł bada napięcia między prywatnością a ryzykiem nadzoru w kontekście zwiększonego zastosowania technologii w celu monitorowania i śledzenia mobilności, a także zachowań i stanu zdrowia obywateli podczas i po pandemii COVID-19. W podjętych rozważaniach podkreślono potrzebę większej przejrzystości w sposobie pozyskiwania, agregowania i wykorzystywania danych, a także regulacji prywatnych informacji. Pandemia wysunęła na pierwszy plan koncepcję nadzoru cyfrowego i jego potencjału w zakresie naruszania swobód obywatelskich. Trzy proponowane koncepcje rozumienia prywatności, a mianowicie kontrola nad informacjami osobowymi, wolność od nadzoru oraz prawo do autonomii cielesnej w kontekście wpływu systemów i technologii komputerowych na prywatność i wolności obywatelskie, są szczególnie ważne w warunkach postpandemii i przyspieszonej cyfryzacji społeczeństwa. Kontrola nad danymi osobowymi jest konieczna, aby zapewnić, że jednostki mają wpływ na to, jak ich dane są wykorzystywane. Wolność od nadzoru jest niezbędna do ochrony swobód obywatelskich i zapobiegania nadużywaniu władzy. Prawo do autonomii cielesnej ma kluczowe znaczenie w kontekście danych dotyczących zdrowia i ich potencjalnego wykorzystania do celów dyskryminacyjnych. Pandemia przyspieszyła integrację technologii cyfrowych z życiem codziennym, a pojęcia te są kluczowe dla zapewnienia ochrony praw jednostek w tej nowej rzeczywistości. Większa przejrzystość, odpowiedzialność i regulacja są potrzebne, aby zapewnić, że technologia jest wykorzystywana w sposób, który przynosi korzyści społeczeństwu bez naruszania praw jednostki. Artykuł podkreśla potrzebę zniuansowanego zrozumienia prywatności w świecie po pandemii oraz znaczenie zrównoważenia korzyści płynących z technologii z ochroną praw jednostki.

BIBLIOGRAFIA

Abdi N., Zhan X., Ramokapane K.M., Such J., 2021, *Privacy norms for smart home personal assistants*, "Proceedings of The 2021 Chi Conference on Human Factors in Computing Systems", s. 1–14.

ALibeigi A., Munir A.B., Karim M., 2019, *Right to Privacy*, *a Complicated Concept to Review*, "Right to Privacy, A Complicated Concept to Review".

Al-Turjman F., Zahmatkesh H., Shahroze R., 2022, *An overview of security and privacy in smart cities' IoT communications*, "Transactions on Emerging Telecommunications Technologies", 33(3), p.e3677.

Andrew J., Baker M., 2021, *The general data protection regulation in the age of surveillance capitalism*, "Journal of Business Ethics", 168, s. 565–578.

Bacchini F., Lorusso L., 2019, *Race, again: how face recognition technology reinforces racial discrimination*, "Journal of Information, Communication and Ethics in Society", 17(3).

Bajpai K., Weber. K., 2017, *Privacy in public: Translating the category of privacy to the digital age. In From categories to categorization: Studies in sociology, organizations and strategy at the crossroads. Research in the Sociology of Organization*.

Bengio Y., Ippolito D., Janda R., Jarvie M., Prud'homme B., Rousseau J.F., Sharma A., Yu Y.W., 2021, *Inherent privacy limitations of decentralized contact tracing apps*, "Journal of the American Medical Informatics Association", 28(1), s. 193–195.

Blundell B.G., 2020, *Privacy: An Outdated Concept?*, [w:] *Ethics in Computing, Science, and Engineering*, Springer, Cham, s. 109–209.

Brough A.R., Martin K.D., 2021, *Consumer privacy during (and after) the COVID-19 pandemic*, "Journal of Public Policy & Marketing", 40(1), s. 108–110.

Campbell C., Van Brakel R., 2015, *Privacy as a line of flight in societies of mass surveillance* "Ethical Space: International Journal of Communication Ethics", 12(3/4), s. 39–46.

Castelvecchi D., 2020, *Is facial recognition too biased to be let loose?*, "Nature", 587(7834), s. 347–350.

Chan E.Y., Saqib N.U., 2021, *Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high*, "Computers in Human Behavior", 119.

China's Personal Information Protection Law and Its Global Impact, 2021, The Diplomat, https://thediplomat.com/2021/08/chinas-personal-information-protection-law-and-its-global-impact (dostęp: 30.04.2023).

Culver K.B., McLeod D.M., 2023, *"Anti-Riot" or "Anti-Protest" Legislation? Black Lives Matter, News Framing, and the Protest Paradigm*, "Journalism and Media", 4(1), s. 216–230.

Haney J.M., Acar Y., Furman S., 2021, *"It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security*. In *USENIX Security Symposium*, s. 411–428.

Hassandoust F., Akhlaghpour S., Johnston A.C., 2021, *Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective*, "Journal of the American Medical Informatics Association", 28(3), s. 463–471.

Jack M.C., Sovannaroth P., Dell N., 2019, *"Privacy is not a concept, but a way of dealing with life" Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia*, "Proceedings of the ACM on Human-Computer Interaction", 3(CSCW), s. 1–19.

Johnson G.A., Shriver S.K., Goldberg S.G., 2023, *Privacy and market concentration: intended and unintended consequences of the GDPR. Management Science*.

Kostka G., Steinacker L. and Meckel M., 2021, *Between security and convenience: Facial recognition technology in the eyes of citizens in China*, *Germany*, *the United Kingdom*, *and the United States*, "Public Understanding of Science", 30(6), s. 671–690.

Krotoszynski R.J., 2016, *Privacy revisited: A global perspective on the right to be left alone*, Oxford University Press.

Kuner C., Bygrave L.A., Docksey C., Drechsler L., Tosoni L., 2021, *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles*, "Update of Selected Articles" (May 4, 2021).

Kuner C., Cate F.H., Millard C., Svantesson D.J.B., 2011, *Privacy-an elusive concept. International Data Privacy Law*, 1(3).

Lin T., 2022, *Valuing intrinsic and instrumental preferences for privacy*, "Marketing Science", 41(4), s. 663–681.

Lundgren B., 2020, *A dilemma for privacy as control*, "The Journal of Ethics", 24(2), s. 165–175.

Moore A., 2008, *Defining privacy*, "Journal of Social Philosophy", 39(3).

Pardau S.L., 2018, *The California consumer privacy act: Towards a European-style privacy regime in the United States*, "J. Tech. L. & Pol'y", 23, s .68.

Rengel A., 2013, *Privacy in the 21st century*, Martinus Nijhoff Publishers.

Rockenbach B., Sadrieh A., Schielke, A., 2020, *Providing personal information to the benefit of others*, "PloS one", 15(8), p.e0237183.

Saglam R.B., Nurse J.R., Hodges D., 2022, *Personal information: Perceptions*, *types and evolution*, "Journal of Information Security and Applications", 66, s.103–163.

Seubert S., Becker C., 2021, *The democratic impact of strengthening European fundamental rights in the digital age: The example of privacy protection*, "German Law Journal", 22(1), s. 31–44.

Smith M., Miller S., 2022, *The ethical application of biometric facial recognition technology*, "Ai & Society", s. 1–9.

Sharma T., Dyer H.A., Bashir M., 2021, *Enabling user-centered privacy controls for mobile applications: Covid-19 perspective*, "ACM Transactions on Internet Technology (TOIT)", 21(1), s. 1–24.

Solove D.J., Schwartz P.M., 2020, *Information privacy law*, Aspen Publishing.

Solove D.J., 2021, *The myth of the privacy paradox*, "Geo. Wash. L. Rev.", 89.

Waelen R.A., 2023, *The struggle for recognition in the age of facial recognition technology*, "AI and Ethics", 3(1), s. 215–222.

Zainuddin N., Daud M., Ahmad S., Maslizan M., Abdullah, S.A.L., 2021, January, *A study on privacy issues in internet of things (IoT)*, [w:] *2021 IEEE 5th International Conference on Cryptography*, *Security and Privacy (CSP)*, s. 96–100.