UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO

W WARSZAWIE

INSTYTUT NAUK PRAWNYCH

MGR ANITA KLIMAS

KONSTYTUCYJNOPRAWNE ASPEKTY NORMATYWIZACJI „PRAWA DO BYCIA ZAPOMNIANYM”

Praca doktorska pisana pod kierunkiem
prof. dra hab. Bogumiła Szmulika

Warszawa 2025

Spis treści

Wykaz skrótów i skrótowców 6

Wprowadzenie 8

Rozdział 1. Konstytucyjna autonomia informacyjna jednostki jako komponent prawa do prywatności 18

1.1. Uwagi wstępne 18

1.2. Prawo do prywatności 21

1.2.1. Geneza prawa do prywatności 21

1.2.2. Problem z definicją prawa do prywatności 30

1.2.3. Ochrona prawa do prywatności w prawie europejskim oraz międzynarodowym 40

1.2.4. Ochrona prawa do prywatności w prawie polskim 58

1.2.5. Konstytucyjne ograniczenia prawa do prywatności 69

1.3. Regulacja konstytucyjna prawa do informacji 74

1.3.1. Prawo do autonomii informacyjnej na gruncie przepisów Konstytucji RP 74

1.3.2. Prawo do informacji jako prawo człowieka 85

1.3.3. Publicznoprawny charakter prawa do informacji 92

1.4. Oddziaływanie prawa do prywatności na autonomię informacyjną jednostki 102

1.4.1. Związek zakresu podmiotowego prawa do ochrony danych osobowych z prawem do prywatności 102

1.4.2. Relacje zachodzące pomiędzy prawem do ochrony danych osobowych a prawem do prywatności 109

1.5. Podsumowanie 113

Rozdział 2. „Prawo do bycia zapomnianym" w pracach Komisji Europejskiej i Parlamentu Europejskiego 118

2.1. Uwagi wstępne 118

2.2. Geneza „prawa do bycia zapomnianym" w oparciu o wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain z dnia 13 maja 2014 r., sygn. akt: C-131/12 123

2.3. Geneza Ogólnego Rozporządzenia o Ochronie Danych Osobowych (2016/679) ... 132

2.3.1. Prace legislacyjne nad przepisami unijnego Rozporządzenia a uchylenie Dyrektywy 95/46/WE 132

2.3.2. Idea ujednolicenia zasad ochrony danych osobowych w Unii Europejskiej 135

2.4. Uregulowanie „prawa do bycia zapomnianym" w przepisach Rozporządzenia (2016/679) 140

2.4.1. „Prawo do bycia zapomnianym" jako jedno z założeń Ogólnego Rozporządzenia o Ochronie Danych Osobowych 140

2.4.2. Prawo do usunięcia danych a „prawo do bycia zapomnianym” 144
2.4.3. „Prawo do bycia zapomnianym” w regulacjach prawnych RODO 153
2.5. „Prawo do bycia zapomnianym” w judykaturze 158
2.6. Ocena regulacji RODO – podsumowanie dwuletniego okresu obowiązywania.....161
2.7. Podsumowanie.....166
Rozdział 3. „Prawo do bycia zapomnianym” emanacją ochrony danych osobowych 172
3.1. Uwagi wstępne 172
3.2. Zdefiniowanie „prawa do bycia zapomnianym” 176
3.2.1. Problem z definicją „prawa do bycia zapomnianym” 176
3.2.2. Funkcje „prawa do bycia zapomnianym”.....181
3.2.3. „Prawo do bycia zapomnianym” – prawo publiczne czy prywatne.....187
3.3. Analiza „prawa do bycia zapomnianym” w oparciu o treść art. 17 Rozporządzenia nr 2016/679 190
3.3.1. Zakres podmiotowy „prawa do bycia zapomnianym” – podmiot uprawniony 190
3.3.2. Zakres podmiotowy „prawa do bycia zapomnianym” – podmiot zobowiązany 191
3.3.3. Zakres usunięcia danych osobowych przez administratora.....195
3.3.4. Podstawy żądania usunięcia danych.....198
3.4. Ograniczenia w stosowaniu „prawa do bycia zapomnianym” 202
3.4.1. Przesłanki wyłączające korzystanie z „prawa do bycia zapomnianym” 202
3.4.2. Problemy wynikające z realizacji „prawa do bycia zapomnianym” – kopie zapasowe i archiwalne oraz dane nieustrukturyzowane.....211
3.5. Podsumowanie.....216
Rozdział 4. Zakres oddziaływania „prawa do bycia zapomnianym” na krajowy porządek prawny 223
4.1. Uwagi wstępne 223
4.2. Implementacja przepisów Ogólnego Rozporządzenia o Ochronie Danych Osobowych do polskiego systemu prawnego 227
4.2.1. Przesłanki uchwalenia nowych regulacji krajowych, usunięcia kolizji i możliwości pozostawienia dotychczasowych norm prawnych 227
4.2.2. Charakter obowiązku informacyjnego administratora danych 230
4.2.3. Ryzyka na gruncie przepisów RODO związane z „prawem do bycia zapomnianym”.....232
4.3. Środki ochrony prawnej, zasady odpowiedzialności i administracyjne kary pieniężne za naruszenie „prawa do bycia zapomnianym” 239
4.3.1. Prawo do wniesienia skargi do organu nadzorczego.....239
4.3.2. Ochrona prawna przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu za naruszenie „prawa do bycia zapomnianym” 243

4.3.3. Prawo do odszkodowania 247
4.3.4. Procedura nakładania przez organ nadzorczy administracyjnych kar pieniężnych jako skutek naruszenia „prawa do bycia zapomnianym” 252
4.4. Obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych 255
4.4.1. Polityka bezpieczeństwa zgodnie z przepisami RODO 255
4.4.2. Pseudonimizacja i szyfrowanie danych 260
4.4.3. Szacowanie ryzyka dla podstawowych praw i wolności 264
4.4.4. Obowiązek oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych 267
4.5. Podsumowanie 271
Zakończenie 277
Bibliografia 285

Wykaz skrótów i skrótowców

CBOSA Centralna Baza Orzeczeń Sądów Administracyjnych

dok. Dokument

DPIA (Data Protection Impact Assessment) ocena skutków dla ochrony danych

Dyrektywa Dyrektywa 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 (Dz. U. L 281, 23/11/1995 P. 0031-0050)

Dz. U. Dziennik Ustaw

Dz. Urz. UE Dziennik Urzędowy Unii Europejskiej

EIOD Europejski Inspektor Ochrony Danych

EKES Europejski Komitet Ekonomiczno-Społeczny

EKPCz Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności

EOG Europejski Obszar Gospodarczy

ETPCz Europejski Trybunał Praw Człowieka

FTK Federalny Trybunał Konstytucyjny RFN

GIODO Generalny Inspektor Ochrony Danych Osobowych

k.c. Ustawa z dnia 23 kwietnia 1964 r.-Kodeks cywilny (Dz. U. 2024, poz. 1061, 1237)

k.p.a. Ustawa z dnia 14 czerwca 1960 r.-Kodeks postępowania administracyjnego (Dz. U. 2024, poz. 572)

k.p.c. Ustawa z dnia 17 listopada 1964 r.-Kodeks postępowania cywilnego (Dz. U. 2025, poz. 620)

Konstytucja RP, ustawa zasadnicza Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 nr 78, poz. 483)

KPP Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz. Urz. UE 2016 C 202)

MPPOiP Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966 r. (Dz. U. 1977 nr 38, poz. 167)

NSA Naczelny Sąd Administracyjny

ONSA Orzecznictwo Naczelnego Sądu Administracyjnego

ONZ Organizacja Narodów Zjednoczonych

OSNAPiUS Orzecznictwo Sądu Najwyższego: Izba Administracyjna, Pracy i Ubezpieczeń Społecznych

OSNC Orzecznictwo Sądu Najwyższego: Izba Cywilna

OTK Orzecznictwo Trybunału Konstytucyjnego

PUODO Prezes Urzędu Ochrony Danych Osobowych

rez. Rezolucja

RODO, Ogólne Rozporządzenie o Ochronie Danych Osobowych, Rozporządzenie unijne Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1)

SA Sąd Apelacyjny

SN Sąd Najwyższy

SO Sąd Okręgowy

SPI Sąd Pierwszej Instancji UE

TFUE Traktat o Funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. (Dz. Urz. UE 2016 C 202)

TK Trybunał Konstytucyjny

Traktat Konstytucyjny Traktat ustanawiający Konstytucję dla Europy z dnia 29 października 2004 r. (Dz. Urz. UE 2004 nr C 310)

Traktat Lizboński Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z dnia 13 grudnia 2007 r. (Dz. U. 2009 nr 203, poz. 1569)

TSUE Trybunał Sprawiedliwości Unii Europejskiej

TWE Traktat ustanawiający Wspólnotę Europejską

u.o.d.o. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 nr 133, poz. 883)

u.o.r.p.o. Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. 2019, poz. 730)

u.ś.u.d.e. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2024, poz. 1513)

UE Unia Europejska

ust. ustęp

WSA Wojewódzki Sąd Administracyjny

Wprowadzenie

Problematyka stanowiąca przedmiot niniejszej dysertacji dotyczy konstytucyjnoprawnych aspektów normatywizacji „prawa do bycia zapomnianym", a więc wyodrębnienia i sformułowania tego uprawnienia w akcie prawa unijnego, jakim jest Rozporządzenie nr 2016/679[1]. Koncepcja normatywizacji prawa jednostki nawiązuje do zaproponowanej przez T. Jasudowicza typologii ewolucji – myślenia o prawach człowieka[2]. Prawo do prywatności stało się jednym z najważniejszych dóbr osobistych człowieka. Dane osobowe są elementem życia prywatnego.

Prawo do prywatności podlega ciągłej ewolucji. Determinowane jest postępującym rozwojem technologicznym. Jednym z czynników mających wpływ na ewolucję poglądów jest rozwój techniki, w tym środków umożliwiających wkroczenie w życie prywatne jednostek wbrew ich woli i bez ich wiedzy. Potrzebę ochrony prywatności ukształtowało uprawnienie, na mocy którego jednostka ma prawo żądać, aby osoby nieuprawnione, nie ingerowały w jej życie prywatne, zwłaszcza poprzez rozpowszechnianie wiadomości na jej temat. Rozwój technik informacyjno-komunikacyjnych przyczynił się do postrzegania zagadnienia danych osobowych w szerszej perspektywie uwzględniającej nowe niebezpieczeństwa dla prywatności[3].

Unia Europejska od początku swojego funkcjonowania skupiała się na tworzeniu wspólnego dziedzictwa w zakresie ochrony godności człowieka, jego fundamentalnych praw i wolności. Ochrona danych osobowych znajduje swe źródła w prawie pierwotnym Unii Europejskiej. Ma charakter prawa podstawowego zagwarantowanego przepisami Karty Praw Podstawowych Unii Europejskiej[4] oraz Traktatu o Funkcjonowaniu Unii Europejskiej[5].

Jednym z pierwszych aktów prawa pochodnego Unii Europejskiej była Dyrektywa 95/46/WE[6]. Pomimo rozbudowanych postanowień dotyczących danych osobowych,

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1, dalej: RODO, Ogólne Rozporządzenie o Ochronie Danych Osobowych, Rozporządzenie unijne, Rozporządzenie nr 2016/679).

[2] M. Balcerzak, B. Gronowska, T. Jasudowicz, M. Lubiszewski, R. Mizerski, *Prawa człowieka i ich ochrona,* Toruń 2010, s. 27 i n.

[3] E. Milczarek, *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w Internecie,* Warszawa 2020, s. 38.

[4] Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz. Urz. UE 2016 C 202, dalej: KPP UE).

[5] Traktat o Funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. (Dz. Urz. UE 2016 C 202, dalej: TFUE).

[6] Dyrektywa 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 (Dz. Urz. UE L 281, 23/11/1995 P. 0031-0050, dalej: Dyrektywa).

Dyrektywa nie wyeliminowała rozdrobnienia ustawodawstw krajów członkowskich. Głównym powodem takiego stanu był wybór instrumentu legislacyjnego przez prawodawcę unijnego zakładającego minimalną harmonizację, przez co z uwagi na panującą swobodę w jej implementacji, Dyrektywa 95/46/WE nie wyznaczała standardu ochrony danych osobowych. Odpowiedzią na te wyzwanie było wejście w życie przepisów Ogólnego Rozporządzenia o Ochronie Danych Osobowych, których celem stało się dostosowanie regulacji poświęconych ochronie danych osobowych do potrzeb społeczeństwa informacyjnego oraz realiów technologicznych.

„Prawo do bycia zapomnianym" stanowiło jeden z elementów reformy europejskich przepisów ochrony danych osobowych. Pod pojęciem „prawa do bycia zapomnianym" kryje się uprawnienie, które ma posłużyć urzeczywistnieniu ochrony prywatności, przejawiającej się m.in. w autonomii informacyjnej wszystkich podmiotów danych osobowych, czyli każdego z nas[7]. Reforma miała zapewnić korzyści przede wszystkim osobom fizycznym poprzez wzmocnienie ich praw do ochrony danych osobowych oraz zaufania do środowiska cyfrowego.

Wybór tematu normatywizacji „prawa do bycia zapomnianym" w ujęciu konstytucyjnoprawnym wydał się dla Autorki wartościowy z kilku powodów.

Po pierwsze, prawo to, będące stosunkowo nowym elementem ochrony danych osobowych, nabrało znaczenia w erze cyfrowej, w której informacje raz opublikowane w Internecie mogą być dostępne bezterminowo, często wbrew woli danej osoby. Problem zagrożenia prywatności przejawiający się w łatwości gromadzenia, przechowywania i rozpowszechniania danych jest aktualny i zapewne nadal będzie w kontekście rosnącej ilości danych zbieranych przez wyszukiwarki internetowe, media społecznościowe i inne platformy cyfrowe. Pochylenie się nad tematyką normatywizacji „prawa do bycia zapomnianym" pozwoli na analizę, w jaki sposób regulacje prawne mogą ograniczać długotrwałe skutki tzw. cyfrowej nieśmiertelności informacji i zapobiegać problemom związanym z reputacją, cyberprzemocą, czy niekontrolowanym przetwarzaniem danych.

Po drugie, normatywizacja „prawa do bycia zapomnianym", czyli jego ujęcie w przepisach prawnych, jest istotna zarówno z perspektywy ochrony prywatności, jak i zrównoważenia konfliktu między dwoma konkurencyjnymi prawami, tj. prawem do informacji a prawem jednostki do kontroli nad swoimi danymi. Autorka pragnie podjąć się próby wyjaśnienia, jak normatywizacja „prawa do bycia zapomnianym" poprzez określenie

[7] P. Gutowski, *Prawo do bycia zapomnianym-usunięcie danych jako ochrona prywatności,* [dostęp: 22.02.2018] https://itls.pl/1063/prawo-do-bycia-zapomnianym-usuniecie-danych-jako-ochrona-prywatnosci/.

precyzyjnych kryteriów, wpłynie na decyzyjność, w jakich przypadkach usunięcie danych osobowych posiada pierwszeństwo nad prawem do informacji, przykładowo w odniesieniu do osób pełniących funkcje publiczne.

Po trzecie, normatywizacja „prawa do bycia zapomnianym" budzi liczne kontrowersje. Pojawiają się pytania o to, jak pogodzić je z wolnością słowa, jakie mechanizmy stosować przy ocenie wniosków o usunięcie danych oraz w jaki sposób zapobiegać nadużyciom. Te dylematy czynią „prawo do bycia zapomnianym" – zdaniem Autorki – jednym z ciekawszych i współczesnych tematów w debacie o ochronie danych osobowych i prawach cyfrowych.

Po czwarte, niniejsze opracowanie stanowi podjęcie próby zbadania i określenia normatywnej treści przyjmowanej regulacji, a także wpływu prawa do ochrony danych osobowych, a szerzej – prawa do prywatności, na „prawo do bycia zapomnianym". Ewolucja „prawa do bycia zapomnianym" nie była do chwili obecnej przedmiotem kompleksowego zainteresowania naukowego, które znalazłoby swoje odzwierciedlenie w obszerniejszym opracowaniu, w tym monografii. Dotychczasowe prace z tego zakresu mają charakter artykułów naukowych. Przygotowana rozprawa może zatem stanowić pierwsze szersze opracowanie zagadnienia w prawie polskim, a zatem wypełnić istniejący w tym obszarze nauki niedobór. Szerszym zainteresowaniem wśród doktryny prawa cieszy się charakterystyka Ogólnego Rozporządzenia o Ochronie Danych Osobowych. W rozprawie doktorskiej skupiono się na nowym, świeżym uprawnieniu zagwarantowanym przez RODO – dotychczas jeszcze szczegółowo niebadanym.

Wobec powyższego, analiza procesu normatywizacji pozwala śledzić, jak przepisy wpływają na rzeczywistą ochronę jednostek, ale też, jakie wyzwania pozostają do rozwiązania w prawie polskim i europejskim.

Kwerenda źródeł i literatury przedmiotu oraz praktyki stosowania „prawa do bycia zapomnianym" pozwalają na sformułowanie kilku celów naukowych rozprawy doktorskiej. Głównym celem proponowanej rozprawy doktorskiej jest szczegółowa analiza sformułowanego w art. 17 Ogólnego Rozporządzenia o Ochronie Danych Osobowych „prawa do bycia zapomnianym". W opracowaniu tytułowego prawa podjęto próbę całościowego ujęcia problematyki wynikającej z treści przywołanego przepisu, z uwzględnieniem kontekstu aksjologicznego, historycznego oraz prawnego. Komentowany przepis, tj. art. 17 RODO, normuje problematykę prawa osoby, której dane dotyczą, do usunięcia danych jej dotyczących i odpowiadającego mu obowiązku administratora danych osobowych. Ustęp pierwszy reguluje przesłanki uprawniające podmiot danych do wysuwania żądania usunięcia

danych oraz obliguje administratora do spełnienia tegoż żądania bez zbędnej zwłoki. Ustęp drugi skupia się na podaniu do wiadomości informacji o usunięciu danych w wypadku ich upublicznienia, zaś w ustępie trzecim określone zostały wyłączenia dotyczące sytuacji, w których podmiotowi danych nie przysługują uprawnienia do żądania usunięcia danych i informowania o ich usunięciu. Problematyka „prawa do bycia zapomnianym" prowokuje do wskazania kilku szczegółowych celów badawczych. Należy do nich zaliczyć – po pierwsze, ukazanie związku i relacji, jakie zachodzą między triadą praw, tj. prawem do prywatności, prawem do ochrony danych osobowych i „prawem do bycia zapomnianym". Po drugie, szczegółowych analiz wymaga proces normatywizacji „prawa do bycia zapomnianym", czyli geneza „prawa do bycia zapomnianym", uwzględniająca prace prawodawcze na poziomie Unii Europejskiej i ich wpływ na rozwiązania legislacyjne przyjęte w państwach członkowskich, w tym zwłaszcza w Polsce. Po trzecie, ze względu na charakter *novum*, jaki niewątpliwie posiada tytułowe prawo, niezbędne wydaje się dookreślenie zakresu podmiotowego i przedmiotowego prawa, a także granic korzystania z niego i środków ochrony, przysługujących podmiotom danych. Po czwarte, szczegółowym celem badawczym jest próba rozwiązania przynajmniej części wątpliwości i problemów teoretycznych oraz praktycznych, na jakie natrafiają podmioty danych i administratorzy danych osobowych, a także instytucje stojące na straży realizacji prawa. Z jednej strony wspomniane Rozporządzenie uprościło procedurę żądania realizacji „prawa do bycia zapomnianym", z drugiej jednak występują liczne konflikty w relacjach „prawa do bycia zapomnianym" z innymi normami prawnymi, np. w szeroko rozumianej sferze nowoczesnych technologii.

Niniejsza dysertacja stanowi również próbę weryfikacji poniższych głównych hipotez:

1. „Prawo do bycia zapomnianym" rozwijało się w warunkach rewolucyjnych przemian technologicznych, a skutkiem jego urzeczywistnienia stały się pierwsze propozycje zmian regulacji szeroko pojmowanej sfery ochrony danych w sieci.
2. „Prawo do bycia zapomnianym" może prowadzić do konfliktu pomiędzy ochroną prywatności jednostki a prawem społeczeństwa do dostępu do informacji, co wymaga wypracowania kompromisu normatywnego.
3. „Prawo do bycia zapomnianym" można traktować jako rozwinięcie prawa do usunięcia danych osobowych, wzmacniając ochronę prywatności jednostki w środowisku cyfrowym poprzez rozszerzenie zakresu ochrony na dane rozpowszechnione w przestrzeni publicznej.
4. „Prawo do bycia zapomnianym" nie jest prawem absolutnym, a zatem powinno być równoważone z innymi wartościami i prawami.

5. Różnice w interpretacji „prawa do bycia zapomnianym” w porządkach prawnych państw członkowskich Unii Europejskiej oraz spoza Unii Europejskiej prowadzą do nierówności w ochronie prywatności obywateli w sferze cyfrowej.
6. „Prawo do bycia zapomnianym” wpływa na działalność mediów cyfrowych, ograniczając ich możliwość archiwizowania i publikowania informacji o przeszłości podmiotów danych.
7. „Prawo do bycia zapomnianym” może być wykorzystywane do cenzurowania niewygodnych informacji, przez co powoduje ryzyko ograniczenia wolności słowa, w szczególności w systemach prawnych o słabszych mechanizmach kontroli.

Aby osiągnąć powyższe cele pracy, skupiono się na problemach badawczych wyrażonych w postaci następujących pytań badawczych:

1. W jaki sposób kształtowało się „prawo do bycia zapomnianym”?
2. Czy istnieje zależność pomiędzy tzw. „triadą praw”, a więc prawem do prywatności, prawem do ochrony danych osobowych i „prawem do bycia zapomnianym”?
3. Jakie prace prawodawcze dotyczące „prawa do bycia zapomnianym” podjęto na poziomie Unii Europejskiej i jaki był ich wpływ na rozwiązania legislacyjne przyjęte w Polsce?
4. Czy „prawo do bycia zapomnianym” stanowi pewną nowość, czy też jest kontynuacją istniejącego porządku prawnego?
5. Czy „prawo do bycia zapomnianym” wyznacza granice dla innych praw podstawowych?
6. Jakie wyzwania technologiczne i prawne ograniczają skuteczność egzekwowania „prawa do bycia zapomnianym” w przestrzeni cyfrowej?

Odpowiedzi na te pytania zostaną przedstawione w kolejnych rozdziałach pracy.

Tytułowa problematyka rozprawy doktorskiej, przedmiot szczegółowych analiz oraz charakter źródeł i literatury przedmiotu wpłynęły na dobór metod niezbędnych do realizacji celów badawczych oraz weryfikacji hipotez naukowych.

W rozprawie doktorskiej została wykorzystana przede wszystkim metoda teoretyczno-prawna oraz dogmatyczno-prawna, przy pomocy, której została dokonana wykładnia językowa, funkcjonalna i systemowa tekstów normatywnych.

Rozdział drugi rozprawy doktorskiej został napisany przede wszystkim przy pomocy metody historyczno-prawnej. Wybór tej metody był uwarunkowany podjętym problemem badawczym, tzn. tworzeniem się innowacyjnej regulacji prawa Unii Europejskiej i prawa polskiego, a tym samym nowego uprawnienia, jakim jest „prawo do bycia zapomnianym”.

Przy dokonywaniu interpretacji „prawa do bycia zapomnianym" oraz formułowaniu wniosków, będących logicznym następstwem prowadzonych wywodów, wartościowych wskazówek oraz inspiracji dostarczyły rozwiązania i interpretacje przyjęte na poziomie unijnym, a także w niektórych państwach Unii Europejskiej, stąd pomocniczo zastosowano metodę porównawczo-prawną.

Mając powyższe na uwadze, rozprawa doktorska została przygotowana w oparciu o złożoną metodę, na którą składają się metody teoretyczno-prawna, dogmatyczno-prawna i historyczno-prawna, a także w ograniczonym zakresie porównawczo-prawna.

W zakresie prowadzonych rozważań zostały uwzględnione reprezentowane w piśmiennictwie oraz judykaturze poglądy, mające wpływ na analizowane zagadnienie. W związku z przyjętą w rozprawie doktorskiej metodologią, wykorzystano w niej przede wszystkim obowiązujące akty prawa Unii Europejskiej i akty prawa polskiego, dorobek orzecznictwa Trybunału Sprawiedliwości UE, Europejskiego Trybunału Praw Człowieka oraz uzupełniająco, ubogą w tej materii, judykaturę sądów polskich. Skorzystano także z opublikowanych artykułów naukowych z zakresu prawa konstytucyjnego, praw człowieka i prawa Unii Europejskiej. Szczególne zainteresowanie wzbudził wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie *Google Spain* (C-131/12)[8], który zapoczątkował falę analiz dotyczących obszaru stosowania „prawa do bycia zapomnianym", jego stosunku do wolności słowa oraz prawa do informacji. W polskim piśmiennictwie problematyka ta była podejmowana m.in. przez A. Mednisa, P. Litwińskiego, M. Gawrońskiego czy D. Lubaszę, którzy analizowali zarówno konstytucyjne uwarunkowania „prawa do bycia zapomnianym", jak i jego praktyczne skutki dla administratorów danych osobowych. W literaturze zagranicznej ważny wkład wniosły opracowania autorów, takich jak P. de Hert czy S. Gutwirth, koncentrujące się na konflikcie pomiędzy prawem do prywatności a wolnością wypowiedzi oraz granicach terytorialnego stosowania art. 17 RODO. Pomimo rosnącego zainteresowania problematyką „prawa do bycia zapomnianym", dostępna literatura – zarówno krajowa, jak i zagraniczna, nie jest pozbawiona ograniczeń. W polskim piśmiennictwie przeważają opracowania o charakterze komentarzowym i praktycznym. Literatura zagraniczna proponuje bardziej zróżnicowane poglądy, od filozoficznych po technologiczno-regulacyjne. Można jednak dostrzec powtarzalność i koncentrację na klasycznych sprawach, będących przedmiotem rozstrzygnięć TSUE, co może prowadzić do

[8] Wyrok TSUE z dnia 13 maja 2014 r., sygn. akt: C-131/12 w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protecciön de Datos (AEPD) i Mariowi Costeja Gonzàlezowi,* [dostęp:] http://curia.europa.eu/juris/liste.jsf?language=pl&num=C-131/12.

stagnacji interpretacyjnej. Zasadniczym mankamentem analizowanego dorobku jest niedostateczne uwzględnienie „prawa do bycia zapomnianym" w zestawieniu z dynamicznym rozwojem technologii, np. sztuczną inteligencją lub platformami cyfrowymi. W rozprawie doktorskiej Autorka podjęła próbę uzupełnienia tych luk poprzez przyjęcie podejścia systemowego, zawierającego konstytucyjne uwarunkowania prawa do prywatności oraz współczesne zagrożenia dla autonomii informacyjnej jednostki.

Rozprawa doktorska składa się z czterech rozdziałów merytorycznych, wprowadzenia i zakończenia. Dysertacja zawiera wykaz skrótów i skrótowców, bibliografię, a także streszczenie oraz słowa klucze w języku polskim i angielskim.

Rozważania zawarte w pierwszym Rozdziale poświęcone zostały dogłębnej analizie prawa do autonomii informacyjnej, stanowiącej jeden z fundamentalnych elementów prawa do prywatności. Autonomia informacyjna odnosi się do zdolności jednostki do decydowania o tym, jakie informacje na jej temat mogą być ujawnione, gromadzone i przetwarzane przez podmioty zewnętrzne. Autorka skoncentrowała się na zaprezentowaniu podstaw konstytucyjnych tego prawa, jego ewolucji historycznej, zakresu oraz wzajemnych relacji pomiędzy autonomią informacyjną a szeroko pojętą ochroną prywatności.

Na początku Rozdziału szczególny nacisk został położony na wyjaśnienie istoty prawa do prywatności, które odgrywa kluczową rolę w nowoczesnych systemach prawnych. Przeanalizowana została geneza, obejmująca historyczny rozwój tego prawa, począwszy od jego pierwszego sformułowania w artykule L. Brandeisa i S. Warrena z 1890 roku, gdzie przedstawiono koncepcję „prawa do bycia pozostawionym w spokoju". Zaprezentowano etapy ewolucji prawa do prywatności, które przekształciło się z pierwotnej ochrony fizycznej przestrzeni osobistej w bardziej złożone prawo do ochrony danych osobowych i autonomii informacyjnej. Pochylono się także nad trudnościami definicyjnymi prawa do prywatności. Pojęcie tego prawa nieustannie podlega interpretacji w odpowiedzi na zachodzące zmiany technologiczne i społeczne.

Kolejny fragment Rozdziału pierwszego został poświęcony ochronie prawa do prywatności, ze szczególnym uwzględnieniem regulacji międzynarodowych, europejskich oraz krajowych. Wykładni poddane zostały przepisy Konstytucji RP dotyczące prawa do ochrony danych osobowych oraz możliwości decydowania przez podmiot danych o ujawnianiu i przetwarzaniu informacji dotyczących jego życia prywatnego. Podkreślono znaczenie autonomii informacyjnej jako prawa człowieka o publicznoprawnym charakterze, które – podobnie, jak inne prawa podstawowe – może zostać ograniczone wyłącznie w ściśle określonych przypadkach, zgodnie z zasadą proporcjonalności.

W ostatniej części Rozdziału ukazano relacje, jakie zachodzą pomiędzy prawem do prywatności a ochroną danych osobowych. Choć ochrona danych osobowych niejednokroć postrzegana jest jako komponent prawa do prywatności, to stanowi odrębne prawo. Przeanalizowano związek pomiędzy zakresem podmiotowym prawa do ochrony danych osobowych a prawem do prywatności, jak również różnice i analogię pomiędzy tymi dwoma prawami.

W Rozdziale drugim Autorka skupiła się na analizie ewolucji „prawa do bycia zapomnianym" w unijnym porządku prawnym. Przedstawiła proces legislacyjny, który doprowadził do wypracowania „prawa do bycia zapomnianym" jako elementu Rozporządzenia unijnego.

Na początku Rozdziału drugiego, przedstawiono genezę „prawa do bycia zapomnianym" w kontekście przełomowego dla tej tematyki wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie *Google Spain* z dnia 13 maja 2014 roku. Wyrok ten odegrał kluczową rolę w ukształtowaniu przedmiotowego prawa uznając, iż obywatele mogą żądać usunięcia linków do treści naruszających ich prywatność z wyników wyszukiwania. Wobec tego, przeanalizowano motywy wyroku, jego wpływ na funkcjonowanie wyszukiwarek internetowych oraz znaczenie dla przyszłego rozwoju legislacji unijnej w zakresie ochrony danych osobowych.

Następnie została przedstawiona geneza Ogólnego Rozporządzenia o Ochronie Danych Osobowych, które weszło w życie w 2018 roku, zastępując wcześniejszą Dyrektywę 95/46/WE. Zwrócono uwagę na główne problemy, jakie pojawiły się podczas prac nad nowymi przepisami oraz na kompromisy, które zostały wypracowane w toku negocjacji pomiędzy Komisją Europejską, Parlamentem Europejskim i krajami członkowskimi UE. Autorka dodatkowo przeanalizowała, w jaki sposób prace legislacyjne nad RODO zmierzały do ujednolicenia zasad ochrony danych osobowych we wszystkich państwach członkowskich Unii Europejskiej.

Kolejnym elementem Rozdziału jest ukazanie relacji „prawa do bycia zapomnianym" w stosunku do prawa do usunięcia danych osobowych. Prawa te są ze sobą powiązane, ale nie są pojęciami tożsamymi. Należy podkreślić, że stosowanie „prawa do bycia zapomnianym" może zostać wyłączone, np. gdy przetwarzanie danych jest konieczne ze względu na interes publiczny lub wolność słowa.

Z praktycznego punktu widzenia, w Rozdziale drugim poddano pod rozwagę wybrane orzeczenia, zarówno TSUE, jak i sądów krajowych, które miały wpływ na wykładnię „prawa do bycia zapomnianym" oraz jego zastosowanie.

Rozdział zakończył się oceną regulacji zawartych w RODO, obejmując pierwszy, a zatem najświeższy dwuletni okres jego obowiązywania. Daje się zauważyć pozytywne aspekty regulacji, tj. zwiększenie ochrony prywatności i większą kontrolę obywateli nad ich danymi osobowymi, jak i wyzwania praktyczne związane np. z implementacją „prawa do bycia zapomnianym". Dzięki temu, możliwe jest wyciągnięcie wniosków na przyszłość z doświadczeń obowiązywania RODO w początkowych latach.

Rozdział trzeci traktuje o tym, że „prawo do bycia zapomnianym" stanowi istotny element ochrony danych osobowych. Zaprezentowano w nim kluczowe aspekty „prawa do bycia zapomnianym", konieczne do zrozumienia jego natury, funkcji oraz praktycznego znaczenia. W pierwszej części Rozdziału skoncentrowano się na próbie zdefiniowania „prawa do bycia zapomnianym" oraz na wyjaśnieniu trudności związanych z jego jednoznacznym określeniem. Pod rozwagę poddano także funkcje, jakie pełni „prawo do bycia zapomnianym", zarówno w sferze ochrony interesów jednostkowych, jak i w kontekście szerszych stosunków społecznych. Dyskutowany jest status prawny przedmiotowego prawa, tj. czy powinno być traktowane jako prawo o charakterze publicznym, czy o charakterze prywatnym, co wpływa na zakres odpowiedzialności i egzekwowania „prawa do bycia zapomnianym".

W kolejnej części Rozdziału trzeciego szczegółowo omówiono „prawo do bycia zapomnianym" w oparciu o art. 17 RODO. Poruszono temat jego zakresu podmiotowego, czyli to, kto może z niego skorzystać (podmioty uprawnione), jak też na kim spoczywają obowiązki związane z usunięciem danych osobowych (podmioty zobowiązane). Wyjaśniono, jakie czynności mogą być podejmowane przez administratora danych osobowych i w oparciu o jakie podstawy prawne można żądać usunięcia danych osobowych. Zakres obowiązków administratorów podkreśla znaczenie równoważenia interesów osoby żądającej usunięcia danych oraz interesów związanych z zachowaniem danych, np. z uwagi na cele prawne, historyczne lub archiwalne.

Ostatnia część Rozdziału została poświęcona ograniczeniom w stosowaniu „prawa do bycia zapomnianym". Wskazano na konkretne przesłanki wyłączające możliwość korzystania z tegoż prawa, w tym na przypadki, w których zachowanie danych osobowych jest konieczne ze względu na prawo do wolności słowa, interes publiczny, obowiązki prawne, czy też cele naukowe, statystyczne i historyczne. Ponadto, Autorka zwróciła uwagę na problemy praktyczne związane z realizacją „prawa do bycia zapomnianym", tj. istnienie kopii zapasowych i archiwalnych oraz trudności wynikające z przechowywania danych nieustrukturyzowanych. Te kwestie wskazują, iż nawet zaawansowane przepisy prawne nie są

w stanie całkowicie wyeliminować wyzwań odnoszących się do ochrony danych osobowych.

W ostatnim Rozdziale ukazano potrzebę stworzenia nowego aktu prawnego, którego przepisy są adekwatne do standardów przyjętych na poziomie Unii Europejskiej w obszarze ochrony danych osobowych. Podkreślono, że rozwój technologii, digitalizacja, a także zmieniające się warunki społeczne wymusiły potrzebę modernizacji przepisów krajowych. Wskazano przyczyny, dla których uchwalono ustawę o ochronie danych osobowych z dnia 10 maja 2018 roku[9] i powody, dla których wcześniejsza z dnia 29 sierpnia 1997 roku[10] okazała się nieefektywna. Pochylono się nad problematyką realizacji „prawa do bycia zapomnianym" i związanym z tym ryzykiem. Podjęto próbę oceny nałożenia na administratorów danych obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych. Omówiono m.in. szyfrowanie danych, pseudonimizację, czy prowadzenie rejestrów czynności przetwarzania, podkreślając ich znaczenie dla minimalizacji ryzyka naruszeń. Scharakteryzowano, ze szczególnym uwzględnieniem praktyki, środki ochrony prawnej, zasady odpowiedzialności i administracyjne kary pieniężne przysługujące podmiotowi danych za naruszenie „prawa do bycia zapomnianym". Zbadano przy tym, jak wysokość kar wpływa na przestrzeganie obowiązujących standardów ochrony danych oraz w jaki sposób zniechęca do łamania przepisów prawnych.

We wnioskach końcowych zawarto przegląd najważniejszych ustaleń, które zostały poczynione w wyniku prowadzonych badań związanych z wpływem prawa do prywatności i ochrony danych osobowych na realizację „prawa do bycia zapomnianym".

Rozprawa doktorska uwzględnia stan prawny na dzień 18 lipca 2025 roku.

[9] Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. 2019, poz. 1781).
[10] Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 1997 nr 133, poz. 883, dalej: u.o.d.o.).

Rozdział 1. Konstytucyjna autonomia informacyjna jednostki jako komponent prawa do prywatności

1.1. Uwagi wstępne

Powszechnie przyjętą zasadą jest ochrona każdej informacji osobowej i przyznanie znaczenia udzieleniu zgody przez osobę zainteresowaną na udostępnienie informacji[11]. Autonomia informacyjna przejawia się w prawie do samodzielnego decydowania o ujawnianiu informacji na swój temat innym osobom, jak też w prawie do kontrolowania tych informacji, jeżeli znajdują się w dyspozycji podmiotów trzecich. Przedstawiona definicja odnosi się do swobody decydowania o ujawnieniu informacji zarówno w świecie rzeczywistym, jak i w wirtualnym.

Autonomia cyfrowa jednostki jest fikcją w przestrzeni wirtualnej. Dostarczanie danych w sieci odbywa się na wiele sposobów, coraz częściej poprzez używanie aplikacji na smartfonach. Dużym zainteresowaniem cieszą się urządzenia typu *wearables*[12], czyli *smartwatch* (inteligentne zegarki), *smartband* (opaska na rękę służąca do rejestrowania aktywności fizycznej), *watchband* (inteligentna zegarko-opaska)[13]. Nie sposób przy tym pominąć problematyki portali społecznościowych, gdzie „trafiają ogromne zasoby danych dotyczących najrozmaitszych, w tym najbardziej intymnych, wydarzeń z życia wielu różnych osób. Co ważne, są to dane dotyczące nie tylko tych, którzy są użytkownikami tych serwisów. Wielu nie wie nawet, że w różnych serwisach można znaleźć o nich – mniej lub bardziej prywatne – informacje”[14]. Coraz to większe zainteresowanie przejawia się w analizowaniu informacji pochodzących z portali społecznościowych, nie tylko o przeglądanych stronach, ale i o wszystkich danych dotyczących konkretnej osoby, jej powiązaniach, miejscu zamieszkania czy znajomych[15].

Korzystając z Internetu, pozostawia się pewne ślady – informacje będące pożywką dla algorytmów, które analizują historię przeglądanych stron użytkowników. Dokonywane jest to

[11] Wyrok TK z dnia 11 października 2016 r., sygn. akt: SK 28/15 (Dz. U. 2016, poz. 2200).
[12] Z ang. urządzenia do noszenia.
[13] P. Leja, *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych,* „Prawo Mediów Elektronicznych” 2017, nr 3, s. 11.
[14] K. Siewicz, *Prywatność w serwisach społecznościowych. Nowe wyzwania dla ruchu wolnego oprogramowania,* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* red. G. Szpor, W. Wiewiórowski, Warszawa 2012, s. 189.
[15] A. Banaszewska, *Prawo do prywatności we współczesnym świecie,* „Białostockie Studia Prawnicze” 2013, z. 13, s. 132.

głównie przy pomocy plików *cookies*[16]. Na tej podstawie tworzony jest profil użytkownika z dopasowaną do niego reklamą czy produktem[17]. Aby uniknąć śledzenia przez te pliki, można wyłączyć ich obsługę w ustawieniach przeglądarki.

Swoboda udostępniania informacji przysługuje każdemu. Im więcej danych zostanie udostępnionych, tym łatwiej stracić nad nimi kontrolę. Wobec tego, można stwierdzić, że autonomia cyfrowa jednostki stanowi ważny komponent ochrony danych osobowych, a co za tym idzie – prawa do prywatności.

Autonomia informacyjna jest jednym z elementów prawa do prywatności. Uznawanie prawa do ochrony danych osobowych za pochodną prawa do prywatności nie jest pozbawione podstaw. Wiąże się to z niejednoznacznym zakresem pojęciowym terminu „prywatność". Biorąc pod uwagę szerokie rozumienie tego terminu zauważa się, że zagadnienie ochrony danych osobowych wchodzi w jego zakres. Zagrożenia, które godzą w prawo do ochrony danych osobowych, naruszają także prywatność. Szczególnie widoczne stało się to wraz z postępem cywilizacyjnym i technicznym. Stanowią one niebezpieczeństwo dla dającej się wyodrębnić sfery prywatności w postaci prywatności informacyjnej. Technologie informatyczne i komunikacyjne mają wpływ na nowe pojmowanie prawa do prywatności i na interpretowanie prawa do ochrony danych osobowych jako jego wyspecjalizowanej postaci połączonej z równoczesnym postępem prawa do informacji, prawa do transparencji życia publicznego, prawa do swobody i wolności wyrażania poglądów. Dopuszczalne jest zatem potraktowanie prawa do ochrony danych osobowych jako pewnego *novum* obszaru ochrony prywatności. Argumentem za uznaniem prawa do ochrony danych osobowych za wyspecjalizowany element prawa do prywatności jest założenie koncepcji, że prawo do ochrony danych osobowych sprowadza się do pozostawania anonimowym. Mieści się ono w prawie do bycia pozostawionym w spokoju[18], uznanym za węższe ujęcie prywatności.

W wyniku procesu przeobrażeń, prawo do ochrony danych osobowych wychodzi poza ramy pojęcia „prywatność". Interpretacja zagrożeń wynikających z zastosowania automatycznego przetwarzania danych uzasadnia szersze pojmowanie tego problemu. Automatyzacja przetwarzania danych osobowych może uniemożliwiać nie tylko realizację praw osobistych, lecz również politycznych i socjalnych. W ten sposób zakres prawa do ochrony danych osobowych ulega poszerzeniu, a jego granice wydają się jeszcze mniej wyraźne.

---

[16] Z ang. ciasteczka.
[17] K. Vries, *Identity, profiling algorithms and a world of ambient intelligence,* "Ethics and Information Technology" 2010, vol. 12, no. 1, s. 71.
[18] *"My home is my castle".*

Pomimo tego, że prawo do ochrony danych osobowych wywodzi się z prawa do prywatności, to ustawa zasadnicza poświęca tym prawom dwa odrębne przepisy[19]. Można wysnuć wniosek, że ich brzmienie nie upoważnia do tego, aby upatrywać istnienia pomiędzy nimi bezpośredniego związku, to jednak wzajemna niezależność nie stanowi przeszkody do uznania, iż ich zakresy mogą się krzyżować. Niedozwolone przetwarzanie danych osobowych narusza prywatność konkretnej osoby, choć zagrożenia prawa do prywatności nie sprowadzają się jedynie do przypadków nieuprawnionego przetwarzania danych. Zatem wyodrębnienie prawa do ochrony danych osobowych z prawa do prywatności nie oznacza całkowitego zerwania więzi pomiędzy tymi regulacjami konstytucyjnymi.

Prawo do ochrony danych osobowych służy ochronie prywatności w tej części, która odnosi się do informacji dotyczących danej osoby oraz gwarancji stanu niezależności, gdzie człowiek decyduje o zasięgu udostępniania informacji o swoim życiu, określanej mianem autonomii informacyjnej. Stąd też bezpośrednią funkcją prawa do ochrony danych osobowych jest zabezpieczenie prawa do prywatności. Podobne stanowisko zajął Trybunał Konstytucyjny, orzekając, że „prawo do prywatności statuowane w art. 47, zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51. Ten ostatni, rozbudowany przepis, odwołując się aż pięciokrotnie do warunku legalności – *expressis verbis* w ust. 1, 3, 4 i 5 oraz pośrednio przez powołanie się na zasadę demokratycznego państwa prawnego w ust. 2, stanowi też konkretyzację prawa do prywatności w aspektach proceduralnych”[20]. Gdy za punkt wyjścia potraktuje się zasadę godności człowieka z art. 30 ustawy zasadniczej, na pierwszy plan wysuwa się funkcja obu tych praw do zapewnienia poszanowania godności człowieka. Założenie, że godność jest źródłem wszystkich wolności i praw, pozwala dostrzec związek zachodzący pomiędzy prawem do prywatności a prawem do ochrony danych osobowych w innym kontekście. Różnorodność polega na zaakcentowaniu znaczenia godności jako wspólnego źródła analizowanych praw.

Powiązania pomiędzy prawem do prywatności a prawem do ochrony danych osobowych są uwypuklone na gruncie rozważań nad międzynarodowymi gwarancjami ochrony danych osobowych. Międzynarodowe regulacje posługują się terminem „prywatność”, które obejmuje ochronę informacji o charakterze osobowym. Zauważane jest

[19] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 nr 78, poz. 483, dalej: Konstytucja RP, ustawa zasadnicza).
[20] Wyrok TK z dnia 19 maja 1998 r., sygn. akt: U 5/97, OTK ZU 1998, nr 4, poz. 46.

to w art. 12 Powszechnej Deklaracji Praw Człowieka[21], w art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych[22], czy w art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[23]. Stosowanie zawartych w nich gwarancji osłabia siłę argumentów przemawiających za wyodrębnieniem prawa do ochrony danych osobowych od prawa do prywatności.

Rozdział pierwszy został poświęcony ukazaniu, że prawo do prywatności jest ściśle powiązane z prawem do ochrony danych osobowych, a prawo do ochrony danych osobowych jest pochodną prawa do prywatności. Poddano analizie problematykę, w jaki sposób prawo do prywatności oddziałuje na autonomię informacyjną jednostki zagwarantowaną przez przepisy ustawy zasadniczej.

1.2. Prawo do prywatności

1.2.1. Geneza prawa do prywatności

Prawo do prywatności jako odrębna kategoria jurydyczna posiada krótką historię. Samuel D. Warren i Louis D. Brandeis pod koniec XIX stulecia stworzyli nowe pojęcie prawa do prywatności. Autorzy nawiązywali do zasady *common law* ochrony jednostki[24]. Wcześniej funkcjonowało ono jedynie w języku potocznym i można przyjąć, że od początku dziejów ludzkich było zakorzenione w świadomości człowieka[25]. Wyżej wymienione nazwiska to najczęściej pojawiające się w publikacjach naukowych poświęconych przedmiotowemu prawu w kontekście jego genezy. Na łamach „Harvard Law Review" nr 4 w dniu 15 grudnia 1890 r. opublikowali artykuł pt.: „The right to privacy"[26] określając, że prawo do prywatności utożsamiane jest z prawem do bycia pozostawionym w spokoju *(to be let alone)*[27]. Publikacja ta jest uważana za dzieło przełomowe, nie ze względu na pojęcie prawa do prywatności, a za

[21] Powszechna Deklaracja Praw Człowieka (przyjęta i proklamowana rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) w dniu 10 grudnia 1948 r. w Paryżu), [dostęp:] https://amnesty.org.pl/wp-content/uploads/2016/04/Powszechna_Deklaracja_Praw_Czlowieka.pdf.
[22] Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966 r. (Dz. U. 1977 nr 38, poz. 167, dalej: MPPOiP).
[23] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 roku (Dz. U. 1993 nr 61, poz. 284, dalej: EKPCz).
[24] S.D. Warren, L.D. Brandeis, *The right to privacy,* "Harvard Law Review" 1890, nr 4, s. 193-220.
[25] W literaturze przedmiotu uważa się natomiast, że koncepcja prawa do prywatności wpierw pojawiła się w nauce niemieckiej na przełomie XVIII/XIX wieku. Mowa tam jednak o prawach osobistości. Por. J. Braciak, *Prawo do prywatności,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2002, s. 291.
[26] Dosłownie: prawo do prywatności.
[27] S.D. Warren, L.D. Brandeis, *The right...,* s. 193-220.

nowe postrzeganie praw obywatelskich, z jednoczesnym ich poszerzaniem o samoistne dobro, którego celem była ochrona sfery życia prywatnego. Do chwili powstania tego artykułu i zaprezentowania w nim postulatów odnoszących się do prawa do prywatności, amerykańska myśl prawnicza nie uznawała oddzielnego prawa.

Prawo do prywatności przejawiało się już wcześniej, m.in. w orzeczeniach amerykańskich sądów[28]. Uznano je za najcenniejsze prawo człowieka cywilizowanego[29]. Dopiero jako osobna prawna kategoria pojawiło się w odpowiedzi na nadmierne inwigilowanie życia prywatnego S.D. Warrena[30], w szczególności spotkań towarzyskich organizowanych przez jego współmałżonkę[31]. Posłużono się przy tym szeregiem angielskich oraz amerykańskich orzeczeń, gdzie sądy sięgały po różne podstawy prawne, mianowicie naruszenie własności, pogwałcenie tajemnicy czy warunków kontraktu. Jednak działania, które podlegały ocenie można było postrzegać jako jedną, samoistną kategorię wkraczania w sferę życia prywatnego[32]. Według prekursorów prawa do prywatności chroni ono nienaruszalną osobowość człowieka. Postulowali, aby prawu do prywatności przyznano nowatorską ochronę jako wartości *per se* samoistnej[33]. Podkreślano jednak, że podobnie jak inne prawa, podlega ono pewnym ograniczeniom, np. nie może być podstawą do zakazu publikacji osób, które same uczyniły siebie przedmiotem tego zainteresowania, czy też nie może zabronić rozpowszechniania informacji w szczególnie uzasadnionych przypadkach przewidzianych przez prawo. Stanowisko Warrena i Brandeisa nie znalazło od razu aprobaty w nauce prawa, jak i w judykaturze amerykańskich sądów[34].

Warren i Brandeis dopatrzyli się, że postęp technologiczny wpływa na niebezpieczeństwo godzenia w zakres prywatności jednostki. Pojawiła się konieczność wykorzystania środków prawnych, które służyłyby ochronie tego dobra. Aby dokonać oceny,

---

[28] Pierwszym orzeczeniem sądowym, w którym odniesiono się do prawa do prywatności był wyrok Sądu Najwyższego New Hampshire w sprawie Ward vs. Bartlett z 1816 roku, gdzie sędzia uznał, że strona pozwana bezprawnie naruszyła prawo do domowej prywatności i bezpieczeństwa mieszkania.

[29] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016, s. 16.

[30] M. Wach, *Prawo do prywatności osób publicznych w Stanach Zjednoczonych,* „Państwo i Prawo" 2004, nr 8, s. 79-80.

[31] D. Glancy, *The Invention of the right to privacy,* "Arizona Law Review" 1979, nr 21, s. 1-39.

[32] M. Sakowska-Baryła, *Prawo do ochrony danych osobowych,* Wrocław 2015, s. 24.

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

[34] Przełomowym w tym zakresie był wyrok z 1905 r. w sprawie Pavesich vs. New England Life Insurance Co., w jakim uznano powództwo znanego artysty przeciwko firmie ubezpieczeniowej, która wykorzystała jego zdjęcie w celach reklamowych. W uzasadnieniu sąd stwierdził, że prawo do prywatności ma swój początek w prawie naturalnym. W innej sprawie, 3 lata wcześniej, z powództwa Roberson przeciwko Rochester Folding Box Co., Sąd oddalił pozew przyjmując, że skoro judykatura nie wykształciła jeszcze swojej jednostajnej linii orzeczniczej, to ochrona prywatności nie może zostać zastosowana bez naruszenia zasad państwa prawa. Co istotne, wymiar sprawiedliwości podkreślał niematerialny charakter naruszenia.

czy doszło do naruszenia prywatności konkretnej jednostki, należy zbadać, czy wywołano u niej wewnętrzne – umysłowe albo zmysłowe – cierpienia *(mental suffering)*[35]. Zasadą *common law* jest zapewnienie ochrony osobie i jej własności. Prawnicy wskazywali na postępującą ewolucję życia społecznego. Postulowali, aby prawo do prywatności uznać za dobro autonomiczne, niemające związku z jakimkolwiek innym prawem. Jedną z ważniejszych tez, wysnutych przez tych autorów, która aktualnie również znajduje swoje zastosowanie jest to, że człowiek nie musi uzasadniać, ani udowadniać powodów zakazu wkraczania w zakres swojej prywatności. Prywatność winna podlegać ochronie, gdyż każdej osobie przysługuje uprawnienie do kontroli swego życia, które nie dotyczy innych, i w jakim wolność od zewnętrznego zainteresowania jest warunkiem zachowania indywidualizmu[36]. Granicą prawa do prywatności jest jednak prywatność innych osób oraz ograniczenia niezbędne dla dobra publicznego.

Innym naukowcem, który zajmował się zagadnieniem prywatności był Joseph Kohler. Na początku XX wieku, a dokładniej w 1907 r. zdefiniował prywatność jako swobodę rozporządzania wiadomościami na swój temat, w odniesieniu do tajemnicy korespondencji[37]. Od tego momentu niewątpliwie nastąpił wzrost zainteresowania tą problematyką, który był spowodowany wieloma czynnikami. Z początku wpływały na to doświadczenia wojen, w późniejszych latach rozwój techniki, oddziałujący na jakość życia człowieka, niosący za sobą zagrożenia w środowisku społecznym i publicznym. Człowiek, będąc ze swej natury istotą społeczną, ma potrzebę przebywania wśród innych ludzi. Z drugiej strony, winien mieć zagwarantowany spokój i odpoczynek. Możliwość zaspokojenia tych potrzeb jest jednym z fundamentalnych elementów warunkujących jakość życia dzisiejszego człowieka[38].

Odmienne od Warrena i Brandeisa stanowisko zajął William Prosser, Dziekan Szkoły Prawa Uniwersytetu Kalifornijskiego w Berkeley. Starał się wykazać różnorodność orzeczeń odwołujących się do naruszenia prywatności. Uważał, że prawo do prywatności swoim zakresem odnosi się do naruszenia czterech różnych interesów, które co prawda są podobne nazwą, ale poza nią nie mają ze sobą nic wspólnego, poza tym, że każda z nich ingeruje w prawo do bycia pozostawionym w spokoju. William Prosser wyodrębnił następujące delikty: naruszenie odosobnienia danej jednostki, publiczne ujawnienie niezręcznych dla niej

[35] A. Mednis, *Prawo do prywatności a interes publiczny,* Warszawa 2006, s. 59.
[36] M. Safjan, *Prawo do ochrony życia prywatnego,* [w:] *Podstawowe prawa jednostki i ich sądowa ochrona,* red. L. Wiśniewski, Warszawa 1997, s. 127-128.
[37] M. Pryciak, *Prawo do prywatności,* [w:] *Prawa człowieka: idea, instytucje, krytyka,* red. M. Sadowski, P. Szymaniec, Wrocław 2010, s. 213.
[38] J. Braciak, *Prawo do prywatności,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2004, s. 291.

faktów, stawianie podmiotu w niekorzystnym dla niego świetle, przywłaszczenie nazwiska lub wizerunku innej osoby dla własnej korzyści[39]. Nie sposób pominąć, że konstruowane w ten sposób pojęcie prywatności odbywa się w sensie negatywnym, bowiem wskazuje się na sytuacje, gdzie dochodzi do naruszenia prawa do prywatności.

Publiczne rozpowszechnianie danych należących do sfery prywatności jest zbieżne z ochroną danych osobowych. Interpretacja ta zdaje się być niepełna, dlatego że skupia się tylko na prywatności informacyjnej, pomijając tym samym inne cechy specyficzne dla tego zjawiska. Warto zaznaczyć, że już w latach 30. XX wieku niejako tożsamy pogląd wyraził Leon Green. W jego ocenie prywatność jest jednym z siedmiu interesów bądź faz osobowości człowieka obok jego integralności fizycznej, uczuć i emocji, zdolności do działania, nazwiska, wizerunku oraz historii. Według niego zaliczenie tych wszystkich wymienionych elementów w jedną kategorię deliktową kreuje „niepokojące poczucie sztuczności"[40].

Źródła prywatności można wywodzić z przekazów czy koncepcji filozoficzno – prawnych. Jedni przedstawiciele doktryny prawa uznają prywatność jako cechę nierozerwalnie przypisaną człowiekowi, towarzyszącą jemu od zawsze, choć nie zawsze uświadomioną. Przyjmują oni, że zupełnie pierwsze źródła prawa do prywatności można odnaleźć w Kodeksie Hammurabiego, czy w Biblii[41]. Inni poszukują jej genezy w rozważaniach o prawie natury i wolności. Oni z kolei uważają, że omawiane prawo do prywatności pochodzi z idei zaprezentowanych przez Grocjusza, Hobbesa, Locke'a, Monteskiusza, czy J.J. Rousseau[42]. Formalnoprawna ochrona prywatności nie ma jednak długiej tradycji, gdyż narodziła się w okresie ostatnich stu lat[43].

Żadne spośród praw XX wieku nie oddziaływało na obszary życia społecznego i politycznego jak prywatność[44]. Ówczesne środowiska intelektualne poświęcały wiele swojej uwagi prawu do prywatności. Problematyka ta stała się powszechna w tamtejszej poezji i prozie, niejednokrotnie pojawiała się w tekstach literackich, nawet jako postać tytułowa[45].

Sytuacja nieco skomplikowała się po konstytucjonalizacji prawa do prywatności, które nastąpiło na drodze sądowej, a nie ustawodawczej. Uchwalona w 1789 r. Federalna Karta Praw *(Bill of Rights)* nie regulowała prawa do prywatności, ale niektóre z jej sformułowań się do niego odnosiły. Sądy amerykańskie, zwłaszcza federalny Sąd Najwyższy, upatrywały

[39] W. Prosser, *Privacy,* „California Law Review" 1960, nr 48, s. 388.
[40] L. Green, *The right to privacy,* "Illinois Law Review" 1932, nr 27, s. 239.
[41] M. Jagielski, *Konstytucjonalizacja ochrony prywatności,* [w:] *Konstytucjonalizm a doktryny polityczno-prawne. Najnowsze kierunki badań,* red. R. Małajny, Katowice 2008, s. 264.
[42] M. Jagielski, *Konstytucjonalizacja ochrony prywatności*…, s. 265.
[43] J. Braciak, *Prawo do prywatności…,* s. 280.
[44] K. Motyka, *Prawo do prywatności,* „Zeszyty naukowe Akademii Podlaskiej w Siedlcach" 2010, nr 85, s. 10.
[45] D. Finnell, *Invasions of privacy,* "The Laurel Review" 1993, nr 27, s. 89.

związku z prywatnością w Czwartej Poprawce, która weszła w życie w dniu 15 grudnia 1791 roku[46]. Prawo do prywatności zgodnie z przyjętą wówczas linią orzeczniczą było w szczególny sposób zastrzeżone dla ludzi i traktowane na równi z jakimkolwiek innym prawem[47]. Jednak dopiero w rozpatrywanej sprawie Griswold przeciwko Connecticut Sąd Najwyższy uznał, że prawo do prywatności zawarte jest w samej Konstytucji Stanów Zjednoczonych. Sędzia William O. Duglas tak stwierdził: „mamy tu do czynienia z prawem do prywatności – starszym niż Karta Praw, starszym nawet niż nasze partie polityczne, starszym niż nasz system oświatowy"[48]. Sędzia posłużył się teorią półcieni sfer z Pierwszej, Trzeciej, Czwartej, Piątej, Dziewiątej i Czternastej Poprawki, tzw. *penumbras.* Są one wyrazem prawa do prywatności *sensu stricte.* W prawie konstytucyjnym Stanów Zjednoczonych półcień obejmuje grupę praw pochodzących od innych, wyraźnie chronionych w Karcie Praw[49]. Wykorzystano technikę ekstrapolacji, która polega na próbach przewidywania przyszłych informacji na podstawie danych historycznych[50]. Sędzia Black w zdaniu odrębnym spostrzegł, że chociaż ceni prywatność, to jest ona „szerokim, abstrakcyjnym i niejasnym pojęciem, które łatwo może zostać zawężone, ale które z drugiej strony, może być łatwo interpretowane jako konstytucyjny zakaz wielu innych rzeczy niż rewizje i zatrzymania"[51]. Wyrażone stanowisko przez ww. sędziego potwierdziło się w późniejszych latach. Nastąpiło dalsze rozszerzanie prawa do prywatności. Początkowo prawo to utożsamiane było tylko z małżeństwem, rodziną i domem[52]. Doszło do redefinicji podmiotów prawa do prywatności. Prawa do prywatności nie pojmowano już jako uczestników instytucji społecznej, jaką jest małżeństwo, ale jako zbiór jednostek niezależnych od przypisanych im ról[53]. Dokonano przejścia od starego do nowego pojęcia prywatności. Najpierw istniała potrzeba ochrony jednostki przed inwigilacją. Dopiero z czasem prywatność chroniła wolność wyboru. Prawo do prywatności zaczęto postrzegać jako wolność ingerencji bez ograniczeń ze strony władzy w niektóre formy aktywności, nie zaś jako wolność od

[46] "Prawa ludu do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać przez nieuzasadnione rewizje i zatrzymanie. Nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją oświadczeniem. Miejsce podlegające rewizji oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone". Tłum. A. Pułło, *Konstytucja Stanów Zjednoczonych Ameryki,* Warszawa 2002, [dostęp:] libr.sejm.gov.pl.
[47] L.M. Seidman, *The problems with privacy's problem,* "Michigan Law Review" 1995, nr 93, s. 1079-1101.
[48] Griswold vs. Connecticut, U.S. 1965, nr 381, s. 486.
[49] B. Denning, G. Reynolds, *Comfortably Penumbral,* "Boston University Law Review" 1997, vol. 77, s. 1089-1092.
[50] W. Sokolewicz, *Prawo do prywatności…,* s. 232.
[51] K. Gonera, E. Łętowska, *Artykuł 190 Konstytucji i jego konsekwencje w praktyce sądowej,* „Państwo i Prawo" 2003, nr 53/9, s. 3-7.
[52] A. Katz, *Privacy and Pornography: Stanley vs. Georgia,* "Supreme Court Review" 1969, s. 203-217.
[53] M. Sandel, *Moral Argument and Liberal Toleration: Abortion and Homosexuality,* "California Law Review" 1989, nr 77, s. 527.

ujawniania intymnych spraw. Zaczęto chronić prywatność nie z uwagi na praktyki społeczne, a ze względu na indywidualny wybór, który ona zabezpiecza[54]. Nastąpiło przejście od prywatności informacyjnej do prywatności decyzyjnej[55]. Zakładano upadek rodziny jako jednej z grup społecznych i rozszerzenie prywatności na jednostkę jako taką[56].

Jednym z powodów do krytyki była ekspansja prawa do prywatności. Niektórzy uczeni porównywali ją do inwazji w amerykańskim prawie i kulturze. Ekspansja była utożsamiana z efektem kuli śniegowej[57]. Rozprzestrzenianie się pojęcia prawa do prywatności jest wynikiem braku jej klarownej definicji. Pojęcie prawne winno być zasadą, która następnie przekształca się w normę, a ta zaś z kolei doprowadza do powstania zbioru zastosowań. Stanie się to nierealne do momentu, w którym nie wprowadzi się określonych granic pojęciowych. Prywatność zyskała miano pojęciowej próżni[58]. Mimo tego stała się podstawą wszelkich praw i obowiązków. Zaczęto dokonywać jej różnicowania na prywatność fizyczną (związaną z integralnością fizyczną jednostek), decyzyjną (odnoszącą się do swobodnego podejmowania decyzji), komunikacyjną (wolność wypowiedzi), terytorialną (chroniącą własność danego podmiotu) oraz informacyjną (nawiązującą do danych osobowych)[59].

W Polsce, tak samo jak w innych krajach, przez długi okres ochronie podlegały tylko niektóre elementy prawa do prywatności[60]. Jako odrębne prawo chronione, zostało uregulowane na początku lat 30. XX wieku w art. 255 § 2 ustawy karnej[61]. Wówczas przedmiotowe prawo stanowiło przesłankę wykluczającą przeprowadzenie dowodu prawdy w sytuacji, kiedy dotyczyło czynów powodujących naruszenie czci. Dopiero po II wojnie światowej, 30 lat później, zaczęto częściej wracać do tego pojęcia. Pierwsza przesłanka, mająca na celu ochronę życia prywatnego, która została znormatywizowana, pochodzi z 1984 roku. Uregulowano ją w prawie prasowym[62].

Sporządzając bilans prawnej ochrony prywatności, należy zauważyć, że nie zaczynano

---

[54] C.A. Ball, *Communitarianism and Gay Rights,* "Cornell Law Review" 2000, nr 85, s. 463.
[55] P. Boling, *Privacy As Autonomy vs. Privacy As Familial Attachment. A conceptual approach to right to privacy cases,* "Policy Studies Review" 1994, nr 13, s. 91-110.
[56] J.L. Dolgin, *The family in transition. From Griswold to Eisenstadt and Beyond,* "Georgetown Law Journal" 1994, nr 82, s. 1538.
[57] T. Gerety, *Redefining Privacy,* „Harvard Civil Rights-Civil Liberties Law Review" 1977, nr 12, s. 234.
[58] J.J. Thomson, *The right to privacy,* „Philosophy and public affairs" 1975, nr 4, s. 295-314.
[59] R. Abeyrante, *Attacks on America-Privacy implications of heightened security measures In The United States, Europe and Canada,* "Journal of Air Law and commerce" 2002, nr 67, s. 90.
[60] M. Gdula, *Wprowadzenie do prawa do prywatności w prawie polskim,* [w:] *Ochrona prywatności w nowych technologiach. Publikacja studenckiego Koła Naukowego Blok Prawa Komputerowego,* Wrocław 2015, s. 29.
[61] Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r.-Kodeks karny (Dz. U. 1932 nr 60, poz. 571).
[62] Ustawa z dnia 26 stycznia 1984 r.-Prawo prasowe (Dz. U. 2018, poz. 1914).

w tej dziedzinie od zera[63]. Był już pewien dorobek nauki i judykatury. Andrzej Kopff stwierdził, że istnieje prawo osobistości, które chroni liczne dobra. Z tego założenia wyprowadził koncepcję sfery prywatności i intymności życia osobistego[64]. Co niektórzy dopatrują się trzeciej sfery, a mianowicie powszechnej dostępności. Sfera prywatności obejmowała ponadto sferę życia społecznego. Do sfery życia osobistego autor zaliczał przeżycia osobiste człowieka, o których dana osoba przekazuje jedynie najbliższym. Ta sfera wolna jest od ingerencji osób trzecich. Podejmując się próby zdefiniowania pojęcia sfery prywatności życia osobistego, Andrzej Kopff kierował się kryterium usprawiedliwionego zainteresowania, które nie powinno być odłączone od świata zewnętrznego. Nie może być oderwane od interakcji jednostki ze środowiskiem i będącej efektem tej relacji zaciekawieniem. Nieco szerzej pojmował sferę prywatności. Obejmowała swym zakresem zdarzenia z życia rodzinnego, które z reguły są udostępniane gronu znajomych i przeznaczone właśnie dla tych osób. Rzeczona sfera nie podlega ochronie w tak ścisłym zakresie. Istnieją przesłanki, które uzasadniają wkroczenie w nią osób postronnych. Sfera powszechnej dostępności znajduje się zaś poza jakimkolwiek obszarem ochrony[65].

Polski prawnik zważał na praktykę spostrzegania poszczególnych sfer w takim zakresie, w jakim dana jednostka ma możliwość wyalienowania się od ogółu społeczeństwa w obszarze swojego życia prywatnego. Jako pierwszy wywiódł, że ochrona prawa do prywatności ma swoje odzwierciedlenie w art. 23 i 24 k.c.[66]. Był to zatem pewien etap rozważań nad koncepcją ochrony prywatności o charakterze cywilnoprawnym. Konstytucja Rzeczypospolitej Polskiej nie definiuje terminu „dobra osobiste". W doktrynie pojęcie to opiera się na istnieniu praw podmiotowych. Cechami charakterystycznymi dla tych praw są ich niemajątkowy charakter, ścisły związek z podmiotem, jak również okoliczność polegająca na tym, że są one zaliczane do praw bezwzględnych. Zatem sferę do prywatności można interpretować jako czołowe pojęcie jednostkowych dóbr osobistych, a nie jako delikt za ich naruszenie[67]. Wobec tego, Konstytucja RP traktuje prywatność jako prawo podstawowe, a konieczność jej ochrony wynika bezpośrednio z zasad demokratycznego państwa prawnego[68]. Zwieńczeniem procesu implementowania prywatności do konstytucyjnego

[63] A. Mednis, *Prywatność od epoki analogowej do cyfrowej-czy potrzebna jest redefinicja?,* [w:] *Prywatność a jawność-bilans 25-lecia i perspektywy na przyszłość,* red. A. Mednis, Warszawa 2016, s. 3.
[64] J. Braciak, *Prawo do prywatności…,* s. 134.
[65] K. Degórska, *Prawo do ochrony życia prywatnego i rodzinnego,* [w:] *Prawa i wolności I i II generacji,* red. B. Bolechów, A. Florczak, Toruń 2006, s. 147.
[66] Ustawa z dnia 23 kwietnia 1964 r.-Kodeks cywilny (Dz. U. 2024, poz. 1061, 1237, dalej: k.c.).
[67] I. Dobosz, *Przesłanki cywilnoprawnej ochrony przed podsłuchem,* „Zeszyty Naukowe UJ. Prace z Wynalazczości i Ochrony Własności Intelektualnej" 1992, nr MLXII, s. 58.
[68] Wyrok TK z dnia 21 października 1998 r., sygn. akt: K 24/98, OTK 1998, nr 6.

systemu wartości stał się art. 47 ustawy zasadniczej, według którego „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Polski ustrojodawca nie zdecydował się na wprowadzenie zamkniętej definicji pojęcia prywatności. Norma prawna wskazana w art. 47 Konstytucji RP określa sfery kojarzone z życiem prywatnym. Katalog dóbr chronionych z przywołanego przepisu nie wprowadza zamkniętej listy, a jedynie służy jako wyliczenie przykładowych wartości podlegających ochronie[69].

Koncepcja Andrzeja Kopffa miała ogromny wpływ na dalsze badania zakresu prawa do prywatności. Nauka prawa konstytucyjnego ją akceptowała, ale od początku wskazywała na próbę doprecyzowania i ujednolicenia pojęcia tego dobra. Pojawiały się też głosy krytyczne, a nowsze opracowania w tej materii skupiały się na wykazaniu niedociągnięć i niedokładności w zastosowaniu tej idei. Ranga życia prywatnego znajduje swoje odzwierciedlenie w samej Konstytucji RP, jak i w regulacjach międzynarodowych. Prywatność wiąże się z innymi pojedynczymi dobrami o osobistym charakterze. Poszczególne dobra chronione służą zagwarantowaniu nadrzędnej wartości, jaką jest godność istoty ludzkiej. Stąd też normalne jest zjawisko, że przenikają się nawzajem, korelują ze sobą. Wyłania się ścisły związek pomiędzy godnością stanowiącą podstawę konstytucyjnych wolności i praw, a wszelkimi działaniami, jakie wkraczają w prywatność jednostki[70]. W tym miejscu może pojawić się nieścisłość wynikająca z przytoczonego twierdzenia. Przyjęło się bowiem, że prawo do prywatności cechuje się samoistnością. Łącząc je z innymi dobrami chronionymi, można powiedzieć, że dochodzi do utraty tego atutu. Temu zjawisku przyjrzał się z bliska Krzysztof Kubiński, który wywiódł, że taka wykładnia prowadziłaby do wniosku, iż nie byłoby działań godzących wyłącznie w życie prywatne człowieka, nie powodując tym samym naruszenia żadnego ze znanych dóbr osobistych, co często się zdarza[71].

W okresie transformacji ustrojowej, zasługi w sferze ochrony prywatności posiadał Rzecznik Praw Obywatelskich, który został powołany ustawą z 1987 roku[72]. W przygotowywanych przez siebie sprawozdaniach odwoływał się do przepisów Międzynarodowego Paktu Praw Obywatelskich i Politycznych, a zwłaszcza do art. 17 MPPOiP normującego, że „nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję, ani też na bezprawne

[69] K. Łakomiec, *Konstytucyjne gwarancje ochrony prywatności informacyjnej wobec rozwoju nowych technologii,* „Przegląd Legislacyjny" 2015, nr 1, s. 64.
[70] Wyrok TK z dnia 23 czerwca 2009 r., sygn. akt: K 54/07, OTK-A 2009, nr 6, poz. 86.
[71] K.W. Kubiński, *Ochrona życia prywatnego człowieka,* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1993, z. 1, s. 64.
[72] Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. 2019, poz. 730, dalej: u.o.r.p.o.).

zamachy na jego cześć i dobre imię". Z podsumowania za lata 1988 i 1989 wynika, że Rzecznik Praw Obywatelskich zajmował się następującymi kwestiami z obszaru prawa do prywatności – naruszenie tajemnicy lekarskiej w związku z ujawnieniem rodzajów chorób na zwolnieniach lekarskich dzieci, naruszenie korespondencji, przeprowadzanie zbyt szczegółowego wywiadu z kandydatami do pracy w Ministerstwie Spraw Wewnętrznych PRL, udzielanie przez organy skarbowe informacji o obywatelu jako o osobie prywatnej na poczet prowadzonego sporu, ujawnianie przez milicję nieuprawnionym podmiotom danych zameldowanych w hotelach osób.

Trybunał Konstytucyjny, podzielając zresztą stanowisko ówczesnego Rzecznika Praw Obywatelskich, wywiódł prawo do prywatności z zasady demokratycznego państwa prawnego w wyroku z dnia 12 grudnia 2005 roku[73]. Wartości konstytucyjne są powiązane z systemem norm wartości naturalnych. Są spokrewnione z zasadami, ponieważ „zdania o wartościach można przekonstruować w zdania o zasadach, nie tracąc przy tym treści"[74]. W tym kontekście, prawo do prywatności wraz z prawem do ochrony danych osobowych jako współzależne od godności istoty ludzkiej są wartościami konstytucyjnymi. Godność z kolei stanowi fundament demokratycznego państwa prawnego. Argumentacja Trybunału Konstytucyjnego zakładała, że koncepcja prawa do prywatności zyskała trwałe miejsce we współczesnych państwach demokratycznych. Stało się to jeszcze zanim Konstytucja RP uznała prawo każdego człowieka do poszanowania jego życia prywatnego *expressis verbis*. Trybunał Konstytucyjny zauważył, że prywatność w dużej mierze odwołuje się do ochrony informacji w odniesieniu do danej osoby. Zapewnia jej stan niezależności, w którym człowiek posiada możliwość decydowania o zasięgu rozpowszechniania danych go dotyczących i ujawniania informacji o swoim życiu osobistym. Prywatność zaś zbudowana jest z różnych kręgów, które są w prawny sposób otwarte na oddziaływania zewnętrzne, gdzie konstytucyjnie zagwarantowana aprobata nie jest tożsama dla wkroczenia władzy w jej sferę[75]. W roku 1991 Polska stała się członkiem Rady Europy, a dwa lata później ratyfikowała Europejską Konwencję Praw Człowieka, która poprzez wprowadzony do niej art. 8 przyznawała każdemu prawo do poszanowania życia prywatnego i rodzinnego, nienaruszalności mieszkania i tajemnicy korespondencji. Trybunał Konstytucyjny zwrócił również uwagę na to w wyroku z dnia 24 czerwca 1997 roku, że prawo do prywatności obejmuje swym zakresem ochronę tajemnicy majątku obywatela – zatem odnosi się do

[73] Wyrok TK z dnia 12 grudnia 2005 r., sygn. akt: K 32/04 (Dz. U. 2005, nr 250, poz. 2116); OTK-A 2005, nr 11, poz. 132.
[74] R. Alexy, *Teoria praw podstawowych,* Warszawa 2010, s. 117.
[75] Wyrok TK z dnia 12 grudnia 2005 r., sygn. akt: K 32/04…

posiadanych przez niego kont bankowych i realizowanych przez niego transakcji[76]. Prawo do prywatności uległo jurydyzacji jako wyraz poczucia indywidualności, odrębności oraz niepowtarzalności jednostki. Z drugiej jednak strony, wskazując na źródło konstytucjonalizacji ochrony prywatności, zwraca się uwagę na to, że znaczenie prawa do prywatności wywodzi się z ustawodawstwa zwykłego. To właśnie na poziomie ustawowym było ono najpierw kształtowane. Tam też pojawiały się określone instrumenty ochronne. Dopiero z czasem prawo do prywatności zyskało na znaczeniu na tyle, aby usytuować się w aktach rangi konstytucyjnej. Pomimo że ustawodawca traktował prawo do prywatności jako swoiste novum, to już na poziomie ustaw zasadniczych zajęło ono miejsce obok klasycznych instytucji, do których zaliczała się ochrona tajemnicy korespondencji, nienaruszalność mieszkania, czy ochrona dobrego imienia[77].

Praktyka pokazała, że pomimo swej ogólnikowości przejawiającej się w prawie do bycia pozostawionym w spokoju, określenie to do dzisiaj wykorzystuje się w judykaturze i literaturze przedmiotu jako najczęściej przyjmowane określenie treści prawa do prywatności, co świadczy o tym, że uzyskało powszechną aprobatę[78]. Idea prawa do prywatności jest zatem próbą ochrony niezależności jednostki przed podejmowaniem działań ją ograniczających, a w ujęciu *sensu largo* oznacza prawo do decydowania o swoim życiu osobistym i dokonywanych w nim wyborach[79].

1.2.2. Problem z definicją prawa do prywatności

Prawo do prywatności zalicza się do praw człowieka pierwszej generacji, a prywatność jako niezależne dobro prawne podlega ochronie we współczesnych systemach prawnych. Instytucja praw człowieka ma charakter interdyscyplinarny[80]. Z interdyscyplinarnością zagadnień, które są przedmiotem badań prawoznawstwa, wiąże się problem konieczności stworzenia koncepcji w zakresie metodologii nauk prawnych, jaka uregulowałaby określone instrumenty do współdziałania nauk prawnych z innymi naukami. Źródeł idei praw człowieka należy niewątpliwie upatrywać w sferze filozofii i teologii[81]. Badaniem ich powstania i rozwoju zajmują się głównie historycy, natomiast

[76] Wyrok TK z dnia 24 czerwca 1997 r., sygn. akt: K 21/96, OTK 1997, nr 2, poz. 23.
[77] M. Jagielski, *Konstytucjonalizacja ochrony prywatności…,* s. 269.
[78] W. Sokolewicz, *Prawo do prywatności…,* s. 525.
[79] A. Mednis, *Prawo do prywatności a interes publiczny…,* s. 55.
[80] B. Szmulik, *Prawa człowieka-pojęcie, geneza oraz klasyfikacja,* [w:] *Dylematy praw człowieka,* red. T. Gardocka, J. Sobczak, Toruń 2008, s. 443-453.
[81] M. Jabłoński, S. Jarosz-Żukowska, *Prawa człowieka i systemy ich ochrony. Zarys wykładu,* Wrocław 2004, s. 20.

funkcjonowaniem praw psychologowie i socjologowie. Interdyscyplinarny charakter praw człowieka w szczególności podkreśla Tadeusz Jasudowicz. Definiuje on prawa człowieka jako „złożone zjawisko normatywne", które „szeroko otwiera ramiona na penetrację różnorakich nurtów myślenia i różnorakich nauk"[82]. Koncepcja praw człowieka została wdrożona do wielu dziedzin prawa krajowego i międzynarodowego[83]. W literaturze przedmiotu zauważa się różne typologie kolejnych stadiów ewolucji praw człowieka. Tadeusz Jasudowicz wyróżnia następujące etapy, tj.: idealizację, konceptualizację, normatywizację, konstytucjonalizację, internacjonalizację i realizację. Normatywizację dzieli się na dwa podetapy: pozytywizację oraz jurydyzację.

Pierwszy z podetapów polega na ujmowaniu praw człowieka w jednostki redakcyjne tekstów prawnych[84], mając na celu objęcie skonceptualizowanych dóbr i wartości ochroną prawną, przy pomocy odpowiednich instytucji i instrumentów prawnych. Ten etap wymaga interdyscyplinarnej współpracy badaczy prawa i badaczy koncentrujących się na naukach społecznych. Badanie zaś samych aktów prawnych, w których to spisywane są prawa człowieka, należy do zainteresowań nauki prawoznawstwa. Analiza procesów, przyczyn i uwarunkowań prowadzących do podetapu pozytywizacji dokonywana jest z kolei przez psychologów, socjologów i politologów[85].

Jurydyzacja, inaczej mówiąc interpretacja, jest drugim z podetapów normatywizacji i polega na „filtrowaniu przepisów wyrażających prawa człowieka przez kategorie i narzędzia świata prawników"[86]. Ma to zapewnić podejmowanie prawnych, a nie politycznych decyzji w stosowaniu praw człowieka. Osiągnięcie tego etapu powinno doprowadzić do sytuacji, w której prawa człowieka będą autonomicznym zainteresowaniem sfery nauki prawa. Pochylenie się nad dynamiką jurydyzacji pozwala lepiej zrozumieć relację pomiędzy prawem międzynarodowym a prawami człowieka. Nowe instrumenty prawnej ochrony praw człowieka powinny być spójne z już istniejącym prawem międzynarodowym praw człowieka, mieć charakter fundamentalny i wynikać z przyrodzonej godności i wartości osoby ludzkiej, być precyzyjne, aby można było wyodrębnić uprawnienia i obowiązki, dostarczać skutecznych mechanizmów implementacji oraz posiadać szerokie międzynarodowe

[82] M. Balcerzak, B. Gronowska, T. Jasudowicz, M. Lubiszewski, R. Mizerski, *Prawa człowieka…,* s. 27.
[83] M. Freeman, *Prawa człowieka,* Warszawa 2007, s. 13.
[84] M. Błachut, *Prawnicze interpretacje praw człowieka,* [w:] *Z zagadnień teorii i filozofii prawa. Lokalny a uniwersalny charakter interpretacji prawniczej,* Wrocław 2009, s. 125.
[85] J. Łakomy, *Prawa człowieka w perspektywie interdyscyplinarnej,* „Wrocławskie Studia Erazmiańskie" 2010, tom IV, s. 138.
[86] M. Błachut, *Prawnicze interpretacje praw człowieka…,* s. 125.

poparcie[87]. W oparciu o uwarunkowania jurydyzacji, koncepcja praw człowieka obejmuje pewne minimum, co do którego stworzono adekwatne narzędzia pozytywnoprawne. Stąd wynika ważna konkluzja, która stanowi, że to, co zostało uznane w instrumentach prawa międzynarodowego nie może być podstawą kwestionowania praw człowieka w nich nieuwzględnionych[88].

W nauce prawa brakuje jednak jednolitej, akceptowanej definicji praw człowieka. Podkreśla się ich związek z godnością istoty ludzkiej. Pojęcie prywatności kojarzone jest z konkretnym człowiekiem, kiedy to dominują przymiotniki, takie jak „osobiste", „indywidualne", a więc określające jego osobowość. Prawo do prywatności zaliczane jest do kategorii dobra osobistego. Z uwagi jednak na szeroki zakres pojęcia, konieczne jest jego dookreślenie. Dobra osobiste to wartości o szczególnym znaczeniu, objęte są ochroną na gruncie prawa cywilnego w oparciu o treść art. 23 i 24 k.c.[89]. W ostatnich latach zauważa się wzmożoną aktywność sądów, które zaliczają określone wartości do nowych dóbr osobistych. Ma to związek z ciągle pojawiającymi się nowymi zagrożeniami dla duchowej sfery życia człowieka[90]. W znacznym stopniu zauważalne jest, że prywatność zyskała miano „generalnej etykiety przylepionej do bagażu wartości i praw"[91].

Poszanowanie prawa do prywatności może prowadzić do poszanowania godności. Krzysztof Wygoda podnosi, że „poszanowanie prywatności człowieka poprzez pozostawienie go w spokoju, wyrażające się w nieingerencji ze strony państwa oraz innych podmiotów w pewną określoną w Polsce konstytucyjnie sferę życia jednostki i zabezpieczeniem jej przed nieuprawnionymi działaniami zmierzającymi do naruszenia tej sfery, przyczynia się do poszanowania godności"[92]. Prawo do prywatności wypływa z prawa do godności[93] i jest zaliczane do kategorii praw podmiotowych[94]. Zatem można wywieść, że prywatność jest prawem przynależnym każdej osobie, bez względu na jej status majątkowy, intelektualny i społeczny. Tego prawa nie można się zrzec, jednak można swobodnie kształtować jego

[87] Rezolucja o tworzeniu norm międzynarodowych w dziedzinie praw człowieka (rez. 41/120) przyjęta przez Zgromadzenie Ogólne NZ 4 grudnia 1986 r.
[88] M. Piechowiak, *Filozofia praw człowieka. Prawa człowieka w świetle ich międzynarodowej ochrony,* Lublin 1999, s. 61.
[89] Z. Radwański, A. Olejniczak, *Prawo cywilne-część ogólna,* wyd. 11, Warszawa 2005, s. 161.
[90] M. Pazdan, *Dobra osobiste i ich ochrona,* [w:] *Prawo cywilne-część ogólna,* red. M. Safjan, Warszawa 2012, s. 119.
[91] S. Davies, *The Re-Engineering the Right to Privacy,* [w:] *Technology and Privacy: The New Landscape,* red. P.E. Agre, M. Rotenberg, Cambridge 1998, s. 143.
[92] K. Wygoda, *Ochrona danych osobowych i prawo do informacji o charakterze osobowym,* [w:] *Prawa i wolności obywatelskie,* red. B. Banaszak, A. Preisner, Warszawa 2002, s. 401.
[93] A. Mączyński, *Konstytucyjne prawa do godności i prawa do prywatności,* [dostęp: 16.04.2014] http://26konferencja.giodo.gov.pl/data/resources/MaczynskiA_paper.pdf, s. 2-3.
[94] M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice: wolność informacji, prawo dostępu do informacji publicznej, ochrona danych osobowych,* Wrocław 2002, s. 61.

zakres. Prawom człowieka nadaje się zatem uniwersalny, przyrodzony, niezbywalny i nienaruszalny charakter. Wymienione zasady są jednak ogólnikowe i w praktyce są modyfikowane na gruncie różnych systemów ochrony praw człowieka. Normą zaś jest wprowadzanie rozwiązań polegających na limitacji lub derogacji konkretnych praw przez władzę publiczną, ograniczających się do wyjątkowych sytuacji. W takim rozumieniu, prywatność jest dobrem publicznoprawnym, ponieważ głównym adresatem jest państwo, na którym ciążą obowiązki o charakterze negatywnym – zakaz nieusprawiedliwionej ingerencji oraz obowiązki o charakterze pozytywnym – ukształtowanie regulacji wewnętrznych mających na celu poszanowanie prawa do prywatności w ujęciu horyzontalnym, tj. jednostka a jednostka. Ochrona prywatności, która zakłada prawo wyłącznej kontroli osoby nad uszczegółowioną sferą życia winna być postrzegana w dwóch płaszczyznach. Pierwszą z płaszczyzn jest układ horyzontalny charakterystyczny dla stosunków jednostki z innymi jednostkami. Drugą natomiast, układ wertykalny w odniesieniu do relacji jednostka a władza publiczna[95]. Należy w tym miejscu rozgraniczyć sferę autonomiczną jednostki od tej, gdzie władza publiczna może pełnoprawnie wkraczać. W tym sensie od lat aprobowanym poglądem jest ten, który zakłada hamowanie nadmiernej ingerencji państwa w przyznaną jednostce wolność.

W literaturze przedmiotu wyróżniono więc dwa zasadnicze podejścia do sfery prywatności. Pierwsze z nich kładzie nacisk na konieczność zwiększania poziomu ochrony tego prawa. Ma to swój związek przede wszystkim z liberalnym poglądem, że istnieje niejednolicie definiowana strefa życia, która nie podlega kontroli ze strony państwa i innych osób. Drugie podejście z kolei ma na celu ograniczenie sfery prywatności, uzasadniając to działaniem odpowiednio wyspecjalizowanych instytucji państwowych, zwalczających zagrożenia godzące w bezpieczeństwo społeczne i państwowe[96].

Instytucja prywatności wiąże się z interesem własnym jednostki. Upatruje swój początek w jej dobru oraz w działaniach przez nią podejmowanych, zmierzających do ochrony tej wartości. Stanowi to wyraz przeciwieństwa do aktywności podejmowanej dla dobra wszystkich. Pojęcie wartości nie zostało zdefiniowane w Konstytucji RP, co pozwala przyporządkować ją do kategorii pojęć zastanych[97]. Należy jednak zauważyć, że prywatność dotyczy także tego obszaru, jaki nie podlega zewnętrznej kontroli. Stąd też pojęcie to można definiować jako spektrum wolnego poruszania się, domena autonomicznej i niezależnej

[95] M. Safjan, *Prawo do ochrony życia prywatnego…,* s. 213; Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01, OTK-A 2002, nr 1, poz. 3.
[96] J. Braciak, *Prawo do prywatności…,* s. 278.
[97] L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu,* Warszawa 2014, s. 129.

aktywności[98]. W zależności od społeczeństwa kulturowego, w którym funkcjonuje człowiek, prywatność jest różnie określana w obszarze interakcji, stopnia dystansu i skali alienacji[99]. Prywatność w znaczeniu normatywnym zakłada uprawnienie podmiotu do tworzenia i kształtowania prywatnej sfery życia, aby stała się ona wolna od ingerencji i zamknięta dla innych. Jak zauważył Marek Safjan „prywatność ma podlegać ochronie właśnie dlatego i tylko dlatego, że przyznaje się każdej osobie prawo do wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a w której wolność od ciekawości jest swoistą *conditio sine qua non* swobodnego rozwoju jednostki"[100]. Proklamuje on tezę, że prywatność jest obszarem niedostępności, który powinien być objęty szczególną ochroną przed dociekliwością innych. Ujęcie prywatności w kategorii wartości autonomicznej narodziło się w amerykańskim prawie konstytucyjnym, gdzie są one traktowane tożsamo.

W doktrynie prawa niejednokrotnie zdarza się, że mamy do czynienia z mnogością terminologii związanej z poddaną analizie problematyką. Wyróżnia się sferę osobistą człowieka, prawno – osobistą sferę własną, sferę intymności czy obszar tajności. Ochrona życia prywatnego zmieniała się w zależności od kraju, systemu prawnego, czy zmian kulturowo – religijnych. Biorąc pod uwagę niniejsze rozważania, śmiało można wysnuć wniosek, że nie został wykształcony jeden uniwersalny system ochrony prywatności. Źródeł w definiowaniu pojęcia prywatności należy upatrywać w ustawie zasadniczej. W Konstytucji RP obok prawa do prywatności, można jeszcze wyodrębnić prawo do decydowania o swoich sprawach osobistych[101]. Główny nacisk powinien zostać położony na prawo do samookreślenia, a mniejszy na sferę życia intymnego. Niemniej, nie wykształciło się jednoznaczne pojęcie intymności, stąd też podmioty samodzielnie będą do niej zaliczały okoliczności niewymagające jakiejś szczególnej ochrony. Poszanowanie instytucji prawa do prywatności obejmuje również prawo do nawiązywania nowych kontaktów z innymi osobami[102]. Najbardziej charakterystycznym elementem prawa do prywatności jest właśnie prawo do odosobnienia, odizolowania się. Można je interpretować jako uprawnienie podmiotu do tworzenia swojej prywatnej strefy, tak aby była zamknięta dla innych. Stanowi ona przedmiot ochrony, dlatego że nadaje się każdej osobie prawo do wyłącznego zarządzania tym obszarem, który nie odnosi się do innych osób, natomiast niezależność od nich

[98] M. Pryciak, *Prawo do prywatności,* „Studia Erasmiana Wratislaviensia" 2010, nr 4, s. 212.
[99] J. Braciak, *Prawo do prywatności…,* s. 278.
[100] M. Safjan, *Prawo do ochrony życia prywatnego,* [w:] *Szkoła Praw Człowieka. Teksty wykładów,* Warszawa 2006, s. 211.
[101] M. Wild, *Ochrona prywatności w prawie cywilnym. Koncepcja sfer a prawo podmiotowe,* „Państwo i Prawo" 2001, nr 4, s. 58.
[102] Wyrok ETPCz z dnia 6 listopada 1980 r. w sprawie *Van Oosterwijck przeciwko Belgii,* sygn. akt: 7654/76, § 34, LEX nr 80814.

gwarantuje rozwój i prawidłowe funkcjonowanie jednostki.

Trwająca non stop ewolucja prawa do prywatności niesie za sobą nieustanne odkrywanie nowych dóbr znajdujących się w sferze prywatności jednostki[103]. Z niniejszego wynika, że próby nadania temu terminowi sprecyzowanych ram definicyjnych zawsze będą sprowadzać się do ogólnikowych określeń, wyznaczających zakres prywatności, aniżeli samą treść jej definicji. Trudności w sformułowaniu jednoznacznej definicji prywatności mogą wynikać z okoliczności, że jest ona wspólnym dla wszystkich dobrem, dla wielu gałęzi prawa, w tym prawa konstytucyjnego, cywilnego, administracyjnego i karnego. Próby analizowania tego terminu ugruntowały się w oparciu o orzecznictwo sądów polskich. Wymiar sprawiedliwości, ferując wyroki, dokonuje oceny, czy dany czyn zabroniony miał wpływ na zagrożenie i naruszenie sfery prywatności. Na ogół wyróżnia się rodzaje naruszeń, przed którymi należy chronić jednostkę. Na tej podstawie trudno jest podać zakres prywatności, jak i prawa do prywatności w sensie pozytywnym, w sposób generalno – abstrakcyjny[104].

Podobnie, jak nie istnieje jedna uniwersalna definicja praw człowieka, w prawie polskim nie ma definicji legalnej prawa do prywatności. Badając literaturę przedmiotu, niebywale ciężko jest znaleźć jedną, dokładną definicję pojęcia prywatności w obowiązujących porządkach prawnych poszczególnych państw. Określenie definicji jest bardziej zasługą nauki prawa i judykatury, niż samego prawodawcy[105]. Badacze podejmujący tę problematykę swoją uwagę skupiają w szczególności na wskazywaniu i charakteryzowaniu sfer, jakie należy objąć ochroną przy pomocy rozwiązań prawa do prywatności. Drugie podejście podkreśla listę czynności, które opowiadają się za naruszeniem życia prywatnego jednostki. Prawo do prywatności jest pojęciem niezwykle złożonym, na które składa się życie rodzinne, mir domowy, dobra osobiste człowieka, integralność człowieka, ochrona danych osobowych, tajemnica korespondencji, treść komunikatorów, czy sfera intymna osoby ludzkiej. W polskim piśmiennictwie prawniczym można powtórzyć za przywoływanym wcześniej historykiem, a zarazem prawnikiem Andrzejem Kopffem, że na dobro osobiste w postaci życia prywatnego składa się to wszystko, co ze względu na uzasadnione odseparowanie się jednostki od ogółu społeczeństwa służy jej do rozwoju psychicznej, bądź fizycznej osobowości oraz zachowania osiągniętej pozycji społecznej[106].

---

[103] A. Sakowicz, *Prywatność jako samoistne dobro prawne (per se),* „Państwo i Prawo" 2006, nr 1, s. 29.
[104] B. Kordasiewicz, *Cywilnoprawna ochrona prawa do prywatności,* „Kwartalnik Prawa Prywatnego" 2000, z. 1, s. 28-29.
[105] J. Hołda, Z. Hołda, D. Ostrowska, J.A. Rybczyńska, *Prawa człowieka. Zarys wykładu,* Warszawa 2008, s. 114.
[106] A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne),* [w:] *Studia Cywilistyczne,* tom XX, Kraków 1972, s. 20 i in.

Kolejne podejście zaprezentowane zostało przez J. Thomsona definiującego prawo do prywatności jako pochodną prawa własności i nietykalności osobistej. Inna grupa przedstawicieli nauki sprowadza prywatność do tożsamości intymnej podmiotu, a w ich ocenie najpoważniejszą formą naruszenia prywatności jest naruszenie autonomii seksualnej jednostki[107]. Co niektórzy stworzyli nawet własną konstrukcję definicji wyidealizowanej prywatności, uzależniając jej powstanie od następujących czynników, tj. brak dostępu do informacji o człowieku, brak fizycznego dostępu, brak skupiania na niej swojej uwagi[108].

Doktryna przyjmuje, że prywatność oznacza nie tylko stan pozostawania w spokoju. Prywatność to pewne wartości, które mogą być różne – w zależności od wielu czynników ważnych dla jednostki, w szczególności od kultury, wykształcenia. Są też i takie, gdzie uważa się, że winny być obligatoryjnie chronione, np. wolność, godność, poczucie indywidualności, bezpieczeństwo. Jedno jest pewne, bez prywatności nie byłby możliwy rozwój osobowości ludzkiej. Prywatność można definiować na wiele różnych sposobów. Podlega ona rozmaitym wykładniom[109]. W ujęciu wąskim, to stan, w ramach którego człowiek podejmuje decyzje o zasięgu informacji przekazanych innym podmiotom – jest to tzw. prywatność informacyjna, która zbliżona jest do sytuacji, gdzie prawdziwe będą dane przekazywane drugiemu o człowieku[110]. W znaczeniu szerokim, to stan, gdzie jednostka decyduje o sobie samej bez ingerencji osób trzecich[111]. Można ją nazwać sferą wolności[112]. Z tego wręcz wynika, że decyzja winna być samodzielna i niewymuszona, a wszelkie dalsze ujawnianie informacji pozostaje pod ścisłą kontrolą danej jednostki[113]. W tym ujęciu prawo do prywatności jest zagwarantowane przez wiele przepisów konstytucyjnych, wzajemnie się przenikających i uzupełniających[114]. Nieco inaczej postrzegał to Bogusław Banaszak. On z kolei stał na stanowisku, że zakresy pojęciowe danych przepisów niejednokrotnie na siebie zachodzą[115]. Nie jest możliwe sformułowanie takich norm konstytucyjnych, które zapewniłyby objęcie

[107] J. Braciak, *Prawo do prywatności…,* s. 295.
[108] W. Sokolewicz, *Prawo do prywatności…,* s. 253.
[109] K. Motyka, *Prawo do prywatności…,* s. 25-35.
[110] K. Michałowska, *Prawo do życia rodzinnego na tle ogólnie pojmowanej prywatności jednostki,* „Zeszyty Naukowe UEK" 2013, nr 911, s. 53.
[111] J. Braciak, *Prawo do prywatności…,* s. 130-131.
[112] F. Volio, *Legal Personality, Privacy and the Family,* [w:] *The International Bill of Rights: The Convent of Civil and Political Rights,* red. L. Henkin, New York 1981, s. 190.
[113] L. Kański, *Prawo do prywatności, nienaruszalność mieszkania i tajemnicy korespondencji,* [w:] *Prawa człowieka. Model prawny,* red. R. Wieruszewski, Wrocław 1991, s. 326.
[114] R. Grabowski, S. Grabowska, A. Młynarska-Sobaczewska, W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny,* Warszawa 2009, s. 396.
[115] Prawo do ochrony życia rodzinnego będzie nawiązywało do nienaruszalności mieszkania. Z kolei ochrona życia prywatnego chroni te same stany faktyczne, co tajemnica komunikowania się.

ochroną wszystkich możliwych sytuacji, a nie byłyby ukierunkowane na jej powielanie[116]. Wynika to z chęci ustawodawcy do wyszczególnienia tych praw, które są istotne dla jednostki żyjącej w demokratycznym państwie prawnym.

Już od dawna jawi się problem w dokładnym określeniu zakresu znaczeniowego *sensu largo* prawa do poszanowania życia prywatnego. Z tym zagadnieniem łączy się bogate orzecznictwo Europejskiego Trybunału Praw Człowieka, odnoszące się do wspominanego wcześniej art. 8 Europejskiej Konwencji Praw Człowieka. Zgodnie z treścią tego przepisu bada się ogólne twierdzenia, które charakteryzują istotę chronionej wartości, ale które to też wpływają na definicję życia prywatnego. W sprawie Van Oosterwijck przeciwko Belgii ETPCz uznał, że prawo do prywatności jest prawem do życia, uprawnieniem jednostki do życia zgodnego z jej wolą i bez rozgłosu.

Pojawia się potrzeba zagwarantowania sfery niedostępnej dla innych podmiotów. W tym przypadku prywatność pojmowana jest jako stan, którego celem jest ochrona przed dostępem do informacji nieuprawnionych do tego osób, a nawet z trywialnego powodu, tj. zwykłego zaspokojenia swojej ciekawości[117]. Prywatność sprowadzana jest również do tożsamości intymnej jednostki, a najpoważniejszym jej naruszeniem jest wtargnięcie się w jej seksualną sferę, bowiem pojmowana jest jako przyrodzone i stałe dobro[118]. Jednostka, korzystając z prawa do prywatności tworzy własną osobowość, podejmując przy tym decyzje w sprawach fizycznych i psychicznych.

Klasyfikacji pojęcia prywatności podjął się także Krzysztof Motyka. Wskazał na cztery fundamentalne typy definiowania prywatności – jako prawo do bycia pozostawionym w spokoju, prawo do kontroli informacji na swój temat, kontrola dostępu do osoby i niezależność jednostki. Zaprezentował on także minimalizację prywatności, która sprowadzała się do redukcji terminu prywatność. W zamian, pojęcie to zastępowano nietykalnością mieszkania, nietykalnością osobistą, czy ochroną własności. O ile można się zgodzić, że prywatność przejawia się pod różnymi postaciami, to nie można obejść się zupełnie bez tej myśli. W momencie braku sprecyzowanej regulacji prawnej, dziedzina pola aktywności podmiotu, którą można przyporządkować do sfery życia prywatnego, tak naprawdę może pozostać bez ochrony[119]. Prawo uległo jurydyzacji jako wyraz poczucia

[116] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Warszawa 2009, s. 245-246.
[117] B. Kordasiewicz, *Jednostka wobec środków masowego przekazu,* Wrocław 1991, s. 85.
[118] A. Sakowicz, *Prywatność jako samoistne dobro prawne…,* s. 27.
[119] J. Rzucidło, *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, s. 154.

jednostkowości[120].

Do zakresu pojęciowego tego prawa wlicza się także inne przejawy intelektualnych czy materialnych praw człowieka. Każde naruszenie praw jednostki powinno być traktowane jako naruszenie jej prywatności. Ochrona prywatności życia często nakłada się z innymi sferami podlegającymi ochronie prawnej, krzyżuje się z ich zakresami. Idea prywatności w swym założeniu proklamuje, że zabronione jest rozpowszechnianie informacji z uwagi na samą ich przynależność do sfery prywatności, a nie z powodu ich oceny, czy godzą w dobre imię konkretnego podmiotu. Prowadzi to do wniosku, że nie ma uniwersalnej i powszechnej granicy – to jednostka decyduje o jej autonomii informacyjnej. Prywatność zatem nie jest otwarta i dostępna dla wszystkich. Sprowadza się do odpowiedzi na pytanie, do jakiego stopnia jesteśmy znani innym ludziom i jak bardzo jesteśmy przedmiotem ich zainteresowań[121].

Prywatność odnosi się także do sfery życia rodzinnego jednostki. Powstaje bezwzględny zakaz ingerencji w rodzinę i prawo do ochrony prawnej w tym zakresie. W związku z tym można wyodrębnić następujące naruszenia, np. dotyczące statusu materialnego, rodzinnego nazwiska, ujawnienia ojcostwa. Prywatność obejmuje także intymniejsze informacje, np. o życiu seksualnym, o stanie zdrowia[122]. Ochrona rodziny jest szerokim zagadnieniem, obejmującym złożoność problemu, wymagającym szerszej ochrony prywatności.

Jeszcze innym składnikiem życia prywatnego jest poszanowanie korespondencji. W obecnych czasach ma ona różne formy, np. listy, e-maile, wiadomości tekstowe[123]. Prawo do poszanowania korespondencji z pewnością powinno przejawiać się w utrzymaniu w tajemnicy treści przekazywanej wiadomości, jeżeli tylko taką wolę wyraża nadawca. Tak naprawdę nie ma tutaj znaczenia, w jaki sposób i przy użyciu jakich środków jest przekazywana korespondencja[124]. Ochrona obejmuje „nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze

[120] A. Mednis, *Prawo do prywatności a interes publiczny…,* s. 79.
[121] R. Gavison, *Privacy and the Limits of Law,* "The Yale Law Journal" 1980, nr 3, s. 421.
[122] K.W. Kubiński, *Ochrona życia prywatnego człowieka…,* s. 65.
[123] Wyrok TK z dnia 30 lipca 2014 r., sygn. akt: K 23/11 (Dz. U. 2014, poz. 1055).
[124] M. Balcerzak, B. Gronowska, T. Jasudowicz, M. Lubiszewski, R. Mizerski, *Prawa człowieka…,* s. 370.

IMEI”[125]. W ramach tego mieści się ochrona przed tajnym kontrolowaniem jednostki oraz wykonywanych przez nią rozmów, nawet jeśli odbywać się to ma w miejscach ogólnodostępnych. Nie ma tym samym znaczenia przedmiot rozmowy. Nieistotne, czy wymiana informacji odnosi się do życia prywatnego, czy zawodowego. Jednostka ma zagwarantowane prawo do swobodnego komunikowania się. Tym samym wolność komunikowania się odnosi się nie tylko do tajemnicy korespondencji, ale również do kontaktów międzyosobowych[126]. Prawo to odwołuje się do prawa wolności wypowiedzi i wyrażania swojego poglądu. Dla niektórych może się to wydawać kuriozalne, ale w badanej literaturze przedmiotu plasuje się również na wysokim poziomie stanowisko, że prawo to obejmuje także ochronę miejsca zamieszkania. Miejsce to traktowane jest szczególnie, ponieważ stanowi sferę prywatności dla człowieka, a zarazem niedostępne dla innych w przypadku sprzeciwu danej jednostki. Można pokusić się o stwierdzenie, że w powyższej sytuacji nie będzie miała znaczenia okoliczność, jaki tytuł prawny do mieszkania ma podmiot, o ile w ogóle go posiada. Wystarczy, że jest to miejsce jego codziennego przebywania.

Słuszny jest pogląd, który nakazuje oddzielić prywatną sferę aktywności jednostki od tej o charakterze publicznym. Różnicowanie tych dwóch obszarów odbywa się zazwyczaj w oparciu o zobiektywizowane kryteria, a nie jedynie poprzez odniesienie się do decyzji, czy woli podmiotu. Mowa tutaj o osobach pełniących funkcje publiczne, czy o osobach powszechnie znanych, których popularność wynika zwykle z ich świadomej decyzji. Rzadko mają one wpływ na to, jakie informacje zostały udostępnione w obieg[127]. Wynika to z podejmowanej przez nich działalności[128]. Należy zauważyć, że co prawda prywatność obejmuje zachowanie anonimowości, to w obrocie pojawia się wiele informacji, obiektywnie istniejących, które są niezależne od samej osoby zainteresowanej, powodując tym samym łatwe ustalenie jej tożsamości. Prywatność powinna być traktowana jako dobro, gdzie podmiot wybiera, innymi słowy selekcjonuje, jakie elementy o sobie samym chce ujawnić osobie trzeciej. Takie pojmowanie prywatności jest bliskie autonomii informacyjnej – koncepcji prawa do ochrony danych osobowych, o czym mowa będzie w dalszych rozdziałach niniejszej rozprawy doktorskiej.

Katalog niniejszych naruszeń nie jest nigdzie enumeratywnie wyliczony. Powyżej zostały przedstawione jedynie wybrane przykłady, obrazujące szerokość interpretacji

[125] Wyrok TK z dnia 30 lipca 2014 r., sygn. akt: K 23/11…
[126] Wyrok TK z dnia 20 czerwca 2005 r., sygn. akt: K 4/04, OTK-A 2005, nr 6, poz. 64.
[127] J. Skrzydło, *Wolność słowa a ochrona prywatności osób powszechnie znanych w orzecznictwie ETPCz,* „Europejski Przegląd Sądowy” 2009, nr 7, s. 36.
[128] J. Sieńczyło-Chlabicz, *Dozwolona krytyka prasowa osób pełniących funkcje publiczne w orzecznictwie ETPCz,* „Europejski Przegląd Sądowy” 2007, nr 4, s. 39.

omawianego zagadnienia. Niezależnie od tego, należy dokonać oceny, w jakim stopniu prywatność jako wartość indywidualna jest przedmiotem ochrony prawnej. Kilkukrotnie już zostało powtórzone, że jest ona dobrem samoistnym, a zatem wymaga zagwarantowania jej osobnych regulacji w tym zakresie. Definicję prywatności w szerokim tego słowa znaczeniu zaproponowano m.in. w 1967 r. jako zwieńczenie owocnych obrad Nordyckiej Konferencji Prawników[129]. Za Krzysztofem Motyką należy powtórzyć fundamentalne sposoby ujmowania prywatności, a co za tym idzie – prawa do prywatności. Prywatność postrzegana jest jako przejaw osobowości jednostki oraz jej zdolności do samookreślenia jako osoby ludzkiej. Powinna być traktowana jako wyraz bliskoznaczny autonomii, a więc wolności w zakresie myśli i podejmowanych działań. Prywatność należy pojmować jako zdolność do kontroli nad rozpowszechnianymi informacjami wiążącymi się z jednostką, a przez to do wpływu na relacje z innymi podmiotami. Dopuszcza się definiowanie prywatności przez pryzmat przypisanych jej komponentów, a mianowicie tajemnicy, odosobnienia, intymności, spokoju psychicznego, wyłączności fizycznej i autonomii.

1.2.3. Ochrona prawa do prywatności w prawie europejskim oraz międzynarodowym

Tematyka ochrony praw człowieka jest uznawana za wyzwanie stojące przed systemami prawnymi XXI stulecia. Poruszana jest w działaniach podejmowanych przez Organizację Narodów Zjednoczonych. Objęcie ochroną praw podstawowych, z uwzględnieniem prawa do prywatności jest priorytetem dla ONZ, który w konsekwencji doprowadził do podjęcia rezolucji przez Zgromadzenie Ogólne, wydania decyzji w tym przedmiocie i publikacji raportów specjalnych Rady Praw Człowieka. W literaturze przedmiotu nieustannie podkreśla się wiodącą rolę państwa w zakresie przestrzegania, ochrony oraz realizacji praw człowieka[130]. Znaczącym dokumentem okazała się być rezolucja Rady Praw Człowieka z dnia 5 lipca 2012 roku[131]. Wskazano w niej bezpośrednio, że prawa, które podlegają ochronie w świecie rzeczywistym, winny być również chronione on-line. Następne akty normatywne związane z ochroną praw człowieka w Internecie zostały w 2014

[129] Z. Mielnik, *Prawo do prywatności (zagadnienia wybrane),* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, z. 2, s. 30.
[130] M.R. Bjarnadóttir, *Does the Internet Limit Human Rights Protection? The Case of Revenge Porn,* "JIPITEC" 2016, no. 7(3), s. 204.
[131] The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 29.06.2012, A/HRC/20/L.30.

roku[132] oraz dwa lata później[133] wyartykułowane w formie rezolucji Rady Praw Człowieka. Nowym zagadnieniem, któremu przyjrzano się z bliska w pierwszej z wymienionych rezolucji było rozpowszechnianie dostępu do Internetu jako narzędzia umacniającego alfabetyzację cyfrową oraz dostęp do informacji. Kraje zobowiązano także do szukania rozwiązań, w odpowiedzi na problemy wynikające z zapewnienia bezpieczeństwa w sieci oraz poszanowania prywatności i innych praw człowieka. Proklamowano powołanie instytucji o charakterze demokratycznym i transparentnym, działających w oparciu o zasadę praworządności, tak aby zagwarantować swobodę w Internecie, i w jak najszerszym stopniu wyeliminować niebezpieczeństwo z nim związane. Postulowano, ażeby państwa przy udziale partnerów społecznych przyjęły politykę publiczną, która potwierdzi globalny oraz otwarty charakter sieci Web. Głównym zaś założeniem powinno być dążenie do realizacji praw człowieka i powszechny dostęp do zasobów sieciowych. Druga rezolucja Rady Praw Człowieka ONZ kładła nacisk na walkę z nierównością przejawiającą się w dostępie do Internetu. Potępiono podejmowanie działań uniemożliwiających lub ograniczających udostępnianie informacji za pomocą sieci internetowej, a doprowadzających do naruszeń praw człowieka. W nawiązaniu do występujących zjawisk, powstał raport na temat sposobów eliminowania przepaści cyfrowej pomiędzy płciami z perspektywy praw człowieka[134]. W tym miejscu należy dodać, że również Zgromadzenie Ogólne ONZ podjęło uchwały związane z ochroną praw podstawowych w erze cyfrowej, zwłaszcza z prawem do prywatności[135]. Prawa człowieka mają podlegać ochronie w cyberprzestrzeni, a które to jednocześnie zapewniane są w trybie off-line. Założenie to zostało poparte nie tylko przez Organizację Narodów Zjednoczonych, ale i inne instytucje wprost związane z tą tematyką, w tym podmioty działające w branży informatycznej i organizacje pozarządowe[136]. Spotkania te koncentrowały się na debacie pomiędzy przedstawicielami różnych państw, międzynarodową społecznością internautów, Międzynarodowym Związkiem Telekomunikacyjnym,

[132] The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 20.06.2014, A/HRC/26/L.24.
[133] The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 27.06.2016, A/HRC/32/L.20.
[134] Report of the Office of the United Nations High Commissioner for Human Rights on ways to bridge the gender digital divide from a human rights perspective, [dostęp: 09.02.2017] http://www.ohchr.org/EN/Issues/Women/WRGS/Pages/WaystoBridgetheGenderDigital.aspx.
[135] General Assembly Resolution 68/167 on the right to privacy in the digital age, 18.12.2013; General Assembly Resolution 69/166 on the right to privacy in the digital age, 18.12.2014; General Assembly Resolution 71/199 on the right to privacy in the digital age, 16.11.2016.
[136] Wyniki przeprowadzonych badań i wysnute z nich wnioski zostały zebrane w dokumencie podsumowującym the Global Multistakeholder Meeting on the Future of Internet Governance w Sao Paulo w 2014 roku. Zob. NETmundial Multistakeholder Statement, Sao Paulo 2014, s. 4, [dostęp: 09.02.2017] http://net-mundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Departamentem ds. Społecznych i Ekonomicznych, Sekretariatem ONZ i Komisją Europejską. To tam właśnie po raz pierwszy opracowano zbiór *soft law* odnoszący się do zasad ładu internetowego. Na pierwszy plan wysunęła się problematyka dotycząca poszanowania i ochrony praw człowieka. Szczególną uwagę skierowano na uniwersalność praw człowieka, która obowiązuje w porządku internetowym, jak i stanowi podstawę jego ładu. Zauważono, że najbardziej narażonymi na niebezpieczeństwo wartościami jest zarówno prawo do wolności wypowiedzi, jak i prawo do prywatności, które zaliczane są do kategorii praw cyfrowych *(digital rights)*[137]. Ze względu na powszechną konieczność ochrony sfery prywatności, stworzono katalog uregulowań, które swoje zastosowanie znalazły w wielu aktach prawa międzynarodowego o różnej systematyce, a także zasięgu terytorialnym.

Jednym z pierwszych aktów międzynarodowych traktujących o prawie człowieka do prywatności była Powszechna Deklaracja Praw Człowieka. Pomimo tego, że nie jest umową międzynarodową, a tym samym, nie posiada mocy wiążącej, to jej postanowienia wskazują na pewne standardy praw człowieka. Głównym celem Deklaracji jest promowanie poszanowania praw i wolności jednostki oraz szerzenie za pomocą środków krajowych i międzynarodowych uznania oraz stosowania postulowanych gwarancji prawnych. Tak też, w art. 12 Powszechnej Deklaracji Praw Człowieka znajduje się postanowienie, że „nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu".

Wyżej wymieniony akt prawny wywarł znaczny wpływ na regulacje konstytucyjne wielu państw. W literaturze przedmiotu wskazuje się, że Powszechna Deklaracja Praw Człowieka posiada charakter prawa zwyczajowego. Ma to doniosłe znaczenie pod tym względem, że prawa określone w Deklaracji wiążą wszystkie państwa, bez względu na poziom ratyfikacji i przystąpienia do poszczególnych umów odnoszących się do praw człowieka[138]. Zakres gwarancji prawnych odzwierciedla powszechnie przyjęte rozumienie celu ustanawiania norm jako ochronę przed nieuprawnioną ingerencją państwa[139]. Poza ewolucją rozumienia zakresu prawa do prywatności i jej wpływu na należyte funkcjonowanie społeczeństwa demokratycznego przez lata reformie ulegał zasięg dopuszczalnych ingerencji i wyłączeń. Kryteria stosowania ograniczenia praw fundamentalnych, w rozumieniu

[137] W.H. Dutton, A. Dopatka, G. Law, V. Nash, *Freedom of Connection, Freedom of Expression, UNESCO Series on Internet Freedom,* [dostęp: 13.08.2017] http://unesdoc.unesco.org/images/0019/001915/191594e.pdf.
[138] J. Symonides, *Powszechna Deklaracja Praw Człowieka (po 60 latach od jej przyjęcia),* „Państwo i Prawo" 2008, nr 12, s. 11.
[139] W. Osiatyński, *Prawa człowieka-uniwersalizm i różnorodność,* „Państwo i Prawo" 2013, nr 11, s. 111.

dzisiejszych standardów prawa międzynarodowego, są wielopłaszczyznowe i obok porządku publicznego obejmują zasady moralne, czy zapewnienie powszechnego dobrobytu.

Następnym aktem poruszającym problematykę praw człowieka była Karta Praw Podstawowych Unii Europejskiej, która w art. 7 stanowi, że „Każdy ma prawo do poszanowania swego życia prywatnego i rodzinnego, domu i komunikowania się". Następujący po tym artykule przepis w ustępie 1. reguluje, iż „Każdy ma prawo do ochrony danych osobowych, które go dotyczą", w ustępie 2., że „Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą i prawo do spowodowania ich sprostowania". Co więcej, w oparciu o treść art. 8 ust. 3 KPP, przestrzeganie norm określonych we wcześniejszych ustępach, podlega kontroli niezależnego organu. W wyniku tego, ochrona prywatności, jak też ochrona danych osobowych, uzyskała w Unii Europejskiej znaczenie praw podstawowych. Treścią art. 7 oraz art. 8 Karty Praw Podstawowych wprowadzono prawa, a nie zasady, co jest jednoznaczne z tym, iż przedmiotowe gwarancje posiadają cechę bezpośredniej skuteczności przynależną ogółowi prawa Unii Europejskiej. W późniejszych orzeczeniach, Trybunał Sprawiedliwości UE zaczął utożsamiać istnienie gwarancji praw podstawowych z zasadami ogólnymi prawa wspólnotowego, w rezultacie czego objęcie praw ochroną uznano za jedno z wyzwań Trybunału[140]. Trybunał Sprawiedliwości UE przyjął, iż ochrona praw podstawowych, inspirowana tradycjami konstytucyjnymi państw członkowskich, powinna być wówczas gwarantowana w ramach struktury i celów Wspólnoty[141]. Rozwój orzecznictwa Trybunału był bezpośrednio związany z problematyką prymatu prawa wspólnotowego. Trybunał stanął na stanowisku, że prawo wspólnotowe nie może być oceniane przez pryzmat prawa krajowego, wobec czego zarysował się problem nieuwzględnienia w prawie wspólnotowym zbioru praw podstawowych[142]. Ujawniło się zagrożenie, że sądy krajowe pominą koncepcję absolutnego prymatu prawa wspólnotowego, skutkującej odrzuceniem ochrony praw podstawowych wynikających z regulacji konstytucyjnych. Zaczęto traktować Europejską Konwencję Praw Człowieka jako remedium w zakresie standardu ochrony praw podstawowych obowiązujących w prawie wspólnotowym. Pogląd ten nie jest powszechnie akceptowany przez sądy konstytucyjne krajów członkowskich, czego najlepszym przykładem jest Polska.

[140] Wyrok TSUE z dnia 12 listopada 1969 r. w sprawie *Stauder przeciwko Ulm,* sygn. akt: 29/69, EU:C:1969:57.
[141] Wyrok TSUE z dnia 17 grudnia 1970 r. w sprawie *Internationale Handelsgesellschaft,* sygn. akt: 11/70.
[142] T. Koncewicz, *Zasada pierwszeństwa prawa wspólnotowego przed prawem krajowym w orzecznictwie Trybunału Sprawiedliwości Wspólnot Europejskich,* [w:] *Węzłowe problemy w orzecznictwie Trybunału Sprawiedliwości Wspólnot Europejskich,* red. B. Banaszkiewicz, Biuro Trybunału Konstytucyjnego 2003, s. 8.

Jednakże w niektórych państwach członkowskich, idea prymatu prawa Unii Europejskiej została wprost uregulowana w przepisach rangi konstytucyjnej. Owocem dyskusji w przedmiocie znaczenia praw fundamentalnych w ponadnarodowym porządku prawnym było przyjęcie przez Parlament Europejski, Komisję i Radę deklaracji[143] eksponującej rangę praw podstawowych wynikających zwłaszcza z dorobku konstytucyjnego państw członkowskich oraz Europejskiej Konwencji Praw Człowieka. Deklaracja ta, pomimo tego, że była pozbawiona mocy wiążącej, stanowiła krok w ewolucji Wspólnot Europejskich do porządku ponadnarodowego, którego jednym z celów działania była ochrona praw podstawowych. Zagadnienie wprowadzania katalogu praw podstawowych na poziomie prawa wspólnotowego zostało rozwiązane dopiero wraz z przyjęciem Karty Praw Podstawowych. Początkowo miała ona stanowić część projektowanego Traktatu ustanawiającego Konstytucję dla Europy, niemniej jednak w związku z kłopotami dotyczącymi procedury ratyfikacyjnej, reforma nie weszła w życie[144].

Dokonując analizy prawa do prywatności na gruncie Karty Praw Podstawowych, w pierwszej kolejności należy zwrócić swoją uwagę na zakres podmiotowy i przedmiotowy tego prawa. Oba wyżej wymienione przepisy, mają charakter powszechny, bezwzględnie obowiązujący *ius cogens.* Z tego wynika, że nie są jedynie adresowane do obywateli krajów członkowskich. Analogicznie, jak w wypadku innych aktów międzynarodowych, twórcy Karty Praw Podstawowych nie wprowadzili definicji prywatności. Zdecydowali się to zastąpić katalogiem terminów, tj. poszanowaniem życia prywatnego i rodzinnego, domu i komunikowania się. Problematykę prawa do prywatności na gruncie tego aktu, należy łączyć z godnością człowieka, która nie tylko jest podstawowym prawem, ale stanowi źródło innych praw fundamentalnych, w tym „prawa do bycia zapomnianym"[145].

Porównując postanowienia Karty Praw Podstawowych z innymi aktami o charakterze międzynarodowym, trzeba dostrzec pewną zależność. Zgodnie z art. 52 ust. 3 KPP w zakresie, w jakim Karta zawiera prawa odpowiadające prawom zagwarantowanym w Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności, ich ranga i zasięg są identyczne. Konstrukcja przepisów art. 7 Karty Praw Podstawowych oraz art. 8 ust. 1 Europejskiej Konwencji Praw Człowieka różni się jedynie zastąpieniem terminu „dom" pojęciem „mieszkanie", jak też ochronę „komunikowania się" ochroną „korespondencji". Terminologię

[143] Deklaracja Parlamentu Europejskiego, Rady i Komisji z dnia 5 kwietnia 1977 r., [dostęp:] https://www.europarl.europa.eu/charter/docs/pdf/jointdecl_04_77_en_en.pdf.
[144] Traktat ustanawiający Konstytucję dla Europy z dnia 29 października 2004 r. (Dz. Urz. UE 2004 C 310, dalej: Traktat Konstytucyjny).
[145] J. Sobczak, *Komentarz do art. 7, Nb. 2,* [w:] *Karta Praw Podstawowych Unii Europejskiej,* Warszawa 2013, s. 421-477.

„dom" i „mieszkanie" można uznać za równoważne, a zakres ochrony związany z ich użyciem utożsamić z ochroną miru domowego. Ochronę zaś wszelkich form komunikowania się należy interpretować rozszerzająco, w porównaniu z tą zestawioną z ochroną korespondencji. Wynika to m.in. z orzecznictwa Europejskiego Trybunału Praw Człowieka, gdzie wprost orzekł on, że gwarancje odnoszące się do ochrony korespondencji winny być także używane wobec komunikacji elektronicznej, tj. e-mail, czy w ogóle realizowanej przy pomocy Internetu[146].

W ocenie prawodawcy, gwarancje związane z ochroną prywatności i ochroną danych osobowych w pewnych obszarach się nie krzyżują, co prowadzi do wniosku, że nie każde naruszenie ochrony danych osobowych stanowi wkraczanie w obszar prawa do prywatności. Określając zakres praw i gwarancji związanych z ochroną danych osobowych, zdecydowano się wprowadzić najważniejsze zasady procesu przetwarzania danych, sprowadzające się do obowiązku rzetelnego przetwarzania, tylko w określonym celu, przy zastosowaniu podstawy prawnej lub zgody osoby, której dane dotyczą. Każda z tych zasad znajduje swoje odzwierciedlenie w przepisach prawa wtórnego Unii Europejskiej, a także w pozostałych dokumentach prawa międzynarodowego, których stronami są kraje członkowskie Unii Europejskiej. Wskazano ponadto najważniejsze prawa przysługujące podmiotowi danych, zwłaszcza nawiązujące do dostępu do zebranych danych oraz prawa do ich sprostowania. Rozwinięcie tych praw można znaleźć w regulacjach prawa wtórnego Unii Europejskiej oraz w innych wiążących aktach prawnomiędzynarodowych. Tak też, prawo do prywatności opierało się na innych umowach międzynarodowych z obszaru ochrony praw człowieka, natomiast definiując zakres ochrony danych osobowych wzorowano się na dokumentach mniej powszechnych, odwołujących się raczej do ochrony prywatności w związku z procesem przetwarzania danych osobowych w systemach informatycznych. W przypadku art. 8 Karty Praw Podstawowych nie będzie miał zastosowania art. 52 ust. 3, bowiem w treści Europejskiej Konwencji Praw Człowieka nie wzięto pod uwagę praw i gwarancji w obszarze ochrony danych osobowych w zakresie spójnym z art. 8 KPP.

Na podstawie art. 51 ust. 1 Karty Praw Podstawowych postanowienia Karty mają zastosowanie do instytucji, organów i jednostek organizacyjnych Unii Europejskiej, zaś do krajów członkowskich jedynie w części, w jakiej stosują one prawo UE. Stąd też, zasadny jest wniosek, że Karta Praw Podstawowych nie stanowi samodzielnego aktu prawa międzynarodowego, zaś jej zastosowanie w krajowym porządku prawnym jest ograniczone

[146] Wyrok ETPCz z dnia 3 kwietnia 2007 r. w sprawie *Copland vs. Wielka Brytania,* sygn. akt: 62617/00, § 44, [w:] M.A. Nowicki, *Europejski Trybunał Praw Człowieka. Wybór Orzeczeń 2007,* s. 127.

do sytuacji, w jakiej implementowane jest prawo Unii Europejskiej, tj. w granicach wynikających z zasady przyznania. Widoczny jest tutaj wyraźny dysonans stosowania Karty Praw Podstawowych w porównaniu z innymi normami prawa międzynarodowego. W nauce prawa zauważa się problem, często dominujący w polskim sądownictwie. Sprowadza się on do tego, że organy sądownicze nie pochylają się nad możliwością zastosowania Karty Praw Podstawowych, czasem tylko wzbogacają treść uzasadnienia ferowanych przez siebie wyroków wzmiankami pochodzącymi z KPP[147]. Analizując wpływ aktu na obszar praw fundamentalnych obowiązujących w polskim porządku prawnym, trzeba nadmienić o dołączeniu do Traktatu Lizbońskiego[148] protokołu nr 30 w przedmiocie stosowania Karty Praw Podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa[149]. Trybunał Sprawiedliwości Unii Europejskiej dokonał interpretacji przepisów, z której wynika, że protokół nr 30 nie podważa zastosowania Karty Praw Podstawowych przez prawo polskie. Postanowienia KPP powinny być nadal nieskrępowanie przestrzegane. Zarówno prawo do poszanowania prywatności, jak i ochrony danych osobowych zostało zagwarantowane w krajowych przepisach konstytucyjnych. Wobec czego, ograniczając się do zakresu nawiązującego do zagadnienia ochrony prywatności, umotywowany jest pogląd, że przyjęcie protokołu nr 30 nie ma wpływu na ograniczenie zakresu praw i wolności wynikających z Karty Praw Podstawowych w krajowym porządku prawnym[150].

Prawa unormowane w Karcie Praw Podstawowych mogą być ograniczane, jeśli jest to przewidziane aktem prawnym rangi ustawy oraz spełnia kryteria konieczności i proporcjonalności. Wymienione przesłanki zostały określone w art. 52 ust. 1 Karty Praw Podstawowych. Różnice, które można dostrzec pomiędzy Kartą Praw Podstawowych a pozostałymi umowami międzynarodowymi sprowadzają się do zdefiniowania w Karcie jednej klauzuli limitacyjnej dla wszystkich praw, a nie jak ma to miejsce w innych systemach ochrony praw człowieka, gdzie ograniczenia definiowane są osobno dla każdej z wprowadzanych gwarancji. Prowadzi to do konkluzji, że jeśli prawo regulowane przez Kartę Praw Podstawowych zostało przewidziane również w Europejskiej Konwencji Praw Człowieka, to ograniczenia odnoszące się do tego prawa, powinny wynikać z orzecznictwa, a nie zastosowania art. 52 ust. 1 KPP. Klauzula limitacyjna wynikająca z przywołanego

[147] M. Wróblewski, *Karta Praw Podstawowych Unii Europejskiej w polskim sądownictwie-problemy i wyzwania,* „Kwartalnik Krajowej Rady Sądownictwa" 2015, nr 2, s. 18.
[148] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z dnia 13 grudnia 2007 r. (Dz. Urz. UE 2009 nr 203, poz. 1569).
[149] Protokół w sprawie stosowania Karty Praw Podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa (Dz. Urz. UE 2009 nr 203, poz. 1569).
[150] Wyrok TSUE z dnia 21 grudnia 2011 r., sygn. akt: C-411/10 oraz C-493/10 (sprawy połączone) (Dz. Urz. UE C.2012.49.8).

przepisu może być używana tylko w granicach, w jakich prowadzi do przyznania większych praw jednostkom, aniżeli wynika to z Konwencji oraz orzecznictwa Europejskiego Trybunału Praw Człowieka. W takim rozumieniu, art. 52 ust. 3 pozostaje *lex specialis* w stosunku do generalnej zasady stosowania ograniczeń z art. 52 ust. 1 przedmiotowej Karty. Treść tego przepisu, charakteryzowana jest uprzednim dorobkiem orzeczniczym, gdzie prawa podstawowe (w tym prawo do prywatności), nie mają charakteru bezwzględnego. Mogą one podlegać różnorakim ograniczeniom, pod warunkiem, że skorelowane są z celami interesu ogółu, jakim służy omawiane działanie, oraz że nie stanowią nieproporcjonalnej i nieuprawnionej ingerencji w samą istotę praw w ten sposób zapewnianych[151]. Dzięki temu, przepisy art. 7 i 8 Karty Praw Podstawowych stały się fundamentem wydania przez Trybunał Sprawiedliwości Unii Europejskiej precedensowych orzeczeń, które odbiły swoje piętno na umocnieniu ochrony prywatności w systemach prawnych i sieciach informatycznych. Jedna z głośniejszych spraw dotyczyła sytuacji zatrzymania danych telekomunikacyjnych. Organ orzeczniczy uznał wówczas, iż środki państwowe nakazujące zatrzymanie danych nie wypełniają przesłanek proporcjonalności z art. 52 ust. 1 Karty Praw Podstawowych i w rezultacie sprzyjają naruszeniom gwarancji przewidzianych w art. 7 i 8 KPP, ponieważ po stronie użytkowników powstaje wrażenie, że ich życie prywatne podlega nieustannej kontroli[152]. Trybunał podjął tematykę ochrony praw podstawowych przed nieuprawnioną inwigilacją przez aparat państwowy. Rozstrzygnięcie to miało duże znaczenie praktyczne w krajowych systemach prawnych państw członkowskich Unii Europejskiej i skutkowały wzmocnieniem ochrony przewidzianej na gruncie art. 7 i 8 KPP.

Przełomowy wyrok został wydany w sprawie *Google Spain SL*, w której Trybunał dokonał rozszerzającej wykładni prawa do ochrony danych osobowych. Ponadto wykazał, iż prawo do poszanowania prywatności jednostki jest nadrzędne w stosunku do prawa do dostępu do informacji ogółu oraz interesu gospodarczego operatora wyszukiwarki internetowej[153].

Jeden z wyroków Trybunału Sprawiedliwości Unii Europejskiej rozstrzygnął kwestię efektywności ochrony związanej z ochroną danych osobowych w operacjach międzynarodowego przesyłania danych. Sprawę zapoczątkowała skarga wniesiona przez austriackiego obywatela z powodu przekazywania przez portal społecznościowy Facebook

[151] Wyrok TSUE z dnia 15 czerwca 2005 r. w sprawie *Dokter i inni,* sygn. akt: C-28/05, s. 75.
[152] Wyrok TSUE z dnia 21 grudnia 2016 r. w sprawie *Tele2,* sygn. akt: C-203/15 i C-698/15, [dostęp:] http://curia.europa.eu/juris/document/document.jsf;jsessionid=CDD148747DDB91158709E5CD59F825C6?text=&docid=186492&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=10671937.
[153] M. Rojszczak, *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE,* „Prawo Mediów Elektronicznych" 2017, nr 3, s. 30-41.

Ireland Ltd do USA danych osobowych swoich użytkowników i gromadzenie tych danych na serwerach zlokalizowanych poza terytorium Unii Europejskiej. Skarżący uznał, że dane z nim związane nie są poddawane procesowi przetwarzania w sposób zgodny z prawem UE, zwłaszcza poprzez możliwość nieodpartego dostępu do nich amerykańskich służb wywiadowczych[154]. Trybunał Sprawiedliwości Unii Europejskiej podkreślił, że unormowania prowadzące do ingerencji w prawa podstawowe z art. 7 i 8 Karty Praw Podstawowych powinny określać przejrzyste reguły w kategorii stosowania tych środków, jak również wskazywać na minimalne zabezpieczenia służące temu, aby osoby, których dane osobowe zostały dotknięte naruszeniem, miały na tyle zapewnione mechanizmy, aby chroniły one przed ryzykiem nadużyć. W każdej sytuacji, wprowadzenie takiego uregulowania dla podmiotów danych, gdzie nie ma możliwości uzyskania do nich dostępu, żądania sprostowania bądź usunięcia, prowadzi do nadużycia prawa do skutecznej ochrony prawnej.

Ewolucja techniki powoduje, że ludzkość boryka się z nowymi zagrożeniami i problemami związanymi z zapewnieniem należytego poziomu ochrony prywatności, w szczególności w przypadku korzystania z mediów elektronicznych. Stwierdzenie to potwierdził TSUE w jednym z kolejnych swoich wyroków, w jakim uznał, że definicja danych osobowych wynikająca z prawa Unii Europejskiej musi być zestawiona z istniejącymi możliwościami technicznymi. Oznacza to, że podmiot uprawniony do posiadania takich mechanizmów, które pozwolą na sprecyzowanie tożsamości osoby używającej mediów elektronicznych, jest zobowiązany do traktowania gromadzonych przez siebie zbiorów jako dane osobowe, nawet jeśli innym podmiotom informacje te nie pozwalają na identyfikację użytkowników. Orzeczenie to jest wskazówką, w jaki sposób należy odnosić prawa i gwarancje wynikające z prawa Unii Europejskiej do szybko rozwijającego się rynku e-usług świadczonych w sieciach informatycznych[155]. Wydany w tej sprawie wyrok odnosił się do konkretnego pytania prejudycjalnego związanego z potwierdzeniem, czy dynamiczne adresy IP mogą być uznawane za dane osobowe. W analogicznej sprawie wypowiedział się także Naczelny Sąd Administracyjny, wskazując, że „tam, gdzie adres IP jest na dłuższy czas lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja

[154] Wyrok TSUE z dnia 6 października 2015 r. w sprawie *Schrems,* sygn. akt: C-362/14, [dostęp:] http://curia.europa.eu/juris/liste.jsf?td=ALL&language=pl&jur=C,T,F&num=C-362/14.
[155] Wyrok TSUE z dnia 19 października 2016 r. w sprawie *Breyer,* sygn. akt: C-582/14, [dostęp:] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=PL.

umożliwiająca identyfikację konkretnej osoby fizycznej”[156].

Odrębnego omówienia wymaga rezultat funkcjonowania w obrębie krajów członkowskich Unii Europejskiej dwóch norm prawa międzynarodowego, kształtujących zbliżone, jak niejednakowe swobody i gwarancje w zakresie prawa do prywatności. Tak więc, jeżeli art. 7 Karty Praw Podstawowych jest powtórzeniem art. 8 ust. 1 Europejskiej Konwencji Praw Człowieka, a sama KPP wskazuje na potrzebę dokonywania interpretacji art. 7 w zakresie wynikającym z Konwencji Europejskiej, to powstaje ryzyko, iż objęcie ochroną przez dwa różne organy sądownicze identycznych praw wynikających z obu aktów normatywnych doprowadzi do utworzenia autonomicznych linii orzeczniczych, a w rezultacie do naruszenia zasady pewności prawa.

W dalszej kolejności należy przywołać art. 2 ust. 1 Międzynarodowego Paktu Praw Obywatelskich i Politycznych, w którym uznano, że „Każde z Państw Stron niniejszego Paktu zobowiązuje się przestrzegać i zapewnić wszystkim osobom, które znajdują się na jego terytorium i podlegają jego jurysdykcji, prawa uznane w niniejszym Pakcie, bez względu na jakiekolwiek różnice, takie jak: rasa, kolor skóry, płeć, język, religia, poglądy polityczne lub inne, pochodzenie narodowe lub społeczne, sytuacja majątkowa, urodzenie lub jakiekolwiek inne okoliczności”. Zaraz po przyjęciu Powszechnej Deklaracji Praw Człowieka rozpoczęły się prace związane z implementacją wiążących umów międzynarodowych. Opierając się na niej, miały doprowadzić do trwałego wprowadzenia do krajowych porządków prawnych podstawowych regulacji o tematyce praw człowieka. Tak też, art. 17 tego samego aktu stanowi w ustępie 1., że „Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię”, zaś w ustępie 2, iż „Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami”. Należy dostrzec, że prawo to nie ma charakteru bezwzględnego. Założenie to sprowadza się bowiem do poglądu, zgodnie z którym, skoro przesłankami o charakterze negatywnym są ingerencja samowolna bądź bezprawna, to *a contrario* ograniczenie prawa do prywatności, które nie posiada tych cech, jest dozwolone[157]. Podczas pracy nad tekstem MPPOiP dyskutowano także nad możliwością włączenia ust. 3, który miał uszczegóławiać zakres dopuszczalnych ingerencji ze strony państwa. Nie spotkało się to jednak z aprobatą, stąd też takie rozwiązanie nie zostało

[156] Wyrok NSA z dnia 19 maja 2011 r., sygn. akt: I OSK 1079/10, [dostęp:] http://orzeczenia.nsa.gov.pl/doc/42DC7AE3F0.
[157] A. Siostrzonek-Siergiel, *Prawo do prywatności a bezpieczeństwo publiczne realizowane przez proces karny,* „Kultura bezpieczeństwa. Nauka-Praktyka-Refleksje” 2014, nr 16, s. 406.

przyjęte[158].

W związku z powyższym, na mocy art. 28 ust. 1 MPPOiP powołano Komitet Praw Człowieka, uznany za podmiot uprawniony do monitorowania przestrzegania postanowień Paktu. Organ pochyla się nad interpretacją poszczególnych gwarancji ukształtowanych na podstawie Międzynarodowego Paktu Praw Politycznych i Obywatelskich, które są znane jako *general comments.* W komentarzu ogólnym nr 16, napisanym na potrzeby prawa do prywatności, Komitet wskazał, że gwarancje uregulowane na zasadzie art. 17 powinny przeciwstawiać się wszelkim typom naruszeń, także tym, które związane są z aktywnością innych podmiotów. Nie jest wskazane, aby ograniczały się jedynie do działań podejmowanych przez władzę publiczną. W efekcie tego, obowiązkiem każdego państwa jest implementacja takich przepisów wewnątrz kraju, które zniwelują wystąpienie tego typu naruszeń[159]. Postulat ten został wzmocniony w komentarzu ogólnym nr 31, gdzie wskazano, że zobowiązania na temat podstawowych praw człowieka, mające swoją podstawę w treści wskazanego dokumentu, mają skutek *erga omnes*[160]. Oznacza to między innymi, że wszystkie organy państwa, w których kompetencjach leży władza ustawodawcza, wykonawcza i sądownicza, przejmują na siebie ciężar odpowiedzialności za realizację obowiązków tworzonych na podstawie Paktu. Co ważne, w komentarzu ogólnym nr 16, Komitet swoją uwagę skierował na kwestię ochrony prywatności w związku z przetwarzaniem informacji w formie elektronicznej, podnosząc, iż proces przetwarzania musi być regulowany przez prawo wewnątrzkrajowe. Podkreślono potrzebę wdrożenia stosownych zabezpieczeń, praw dla podmiotów danych w przedmiocie uzyskania informacji o zakresie oraz celu przetwarzania danych osobowych, jak też uzupełniania i modyfikacji danych, zaś w przypadku przetwarzania z jednoczesnym naruszeniem obowiązujących przepisów prawa – do żądania sprostowania lub usunięcia danych. Komitet przedstawił swoje rozważania na temat stosowania prawa do usunięcia danych, zwłaszcza możliwości zgłoszenia żądania usunięcia danych zebranych w toku kontroli operacyjnej, które z uwagi na swój charakter nie mogą zostać wykorzystane w prowadzonym postępowaniu, a więc ich użycie zgodnie z celem, w jakim zostały zgromadzone jest iluzoryczne. W zaistniałej sytuacji, wystarczające jest oddzielenie spornych nagrań od akt sprawy, a fizyczne ich zniszczenie nie rodzi takiej

[158] A. Czubik, *Prawo do prywatności: Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe,* Kraków 2013, s. 264-265.
[159] Komitet Praw Człowieka, *General comment No. 16: Article 17 (Right to privacy),* [dostęp:] http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx, s. 1.
[160] Komitet Praw Człowieka, *General comment No. 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant,* [dostęp:] http://www.ohchr.org/EN/HRBBodies/CCPR/Pages/CCPRIndex.aspx, s. 2.

konieczności[161].

Zgodnie z polskim porządkiem konstytucyjnym, Międzynarodowy Pakt Praw Obywatelskich i Politycznych jest uznany za ratyfikowaną umowę międzynarodową, a tym samym stanowi część krajowego porządku prawnego i jest bezpośrednio stosowany. Dla skuteczności unormowań umowy międzynarodowej nie ma jednak znaczenia tryb jej ratyfikacji. Istotny on jest jednak przy określaniu zasad pierwszeństwa w przypadku kolizji z ustawą. Jak orzekł Naczelny Sąd Administracyjny, ratyfikowane umowy bez upoważnienia aktu rangi ustawowej w przypadku kolizji norm, ustępują ustawie, lecz mają pierwszeństwo przed innymi aktami normatywnymi[162]. W aktualnym stanie prawnym, MPPOiP jest aktem funkcjonującym w polskim porządku prawnym z pierwszeństwem przed krajowymi przepisami ustawy. Kwestią sporną w nauce jest natomiast to, na ile pierwszeństwo ma zastosowanie również w przypadku kolizji z regulacjami rangi konstytucyjnej. Zgodnie jednak z dominującym poglądem, ratyfikowane umowy międzynarodowe są usytuowane niżej od przepisów konstytucyjnych, z jakimi muszą być zgodne[163].

Bliższego przyjrzenia się wymaga także kwestia praktycznego wpływu przystąpienia Polski do MPPOiP w obszarze wzmocnienia ochrony praw podstawowych i wolności człowieka. W zakresie ochrony praw wynikających z art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych wypowiedział się Trybunał Konstytucyjny, a swoją uwagę zwrócił w szczególności na kolizję norm odnoszących się do ochrony dóbr osobistych, do których ma zastosowanie art. 23 kodeksu cywilnego, powiązany także ze sferą prywatności człowieka[164]. Wskazał na redakcję art. 17 Paktu, która nie przewiduje możliwości ograniczenia ochrony przed zamachami na cześć lub dobre imię ze względu na wolność prasy. Na tej podstawie uznano, że ochrona dóbr osobistych winna mieć pierwszeństwo przed ochroną powyższej wolności[165].

Problematyka związana z kolizją gwarancji poszanowania życia prywatnego i innych praw podstawowych jest w szczególności wyraźna w mediach elektronicznych. Ogólnoświatowy dostęp do Internetu wymaga, ażeby normy prawne były implementowane w sposób ponadregionalny. Z uwagi na to, że MPPOiP jest uznawany obecnie za

[161] Decyzja Komitetu Praw Człowieka z dnia 15 listopada 2004 r. w sprawie *Hulst vs. Holandia,* sygn. akt: 903/1999, s. 7.9.
[162] Wyrok NSA z dnia 29 grudnia 1999 r., sygn. akt: I SA/Po 3057/98, ONSA 2001, nr 1, poz. 34.
[163] Wyrok TK z dnia 11 maja 2005 r., sygn. akt: K 18/04, OTK-A 2005, nr 5, poz. 49.
[164] P. Machnikowski, *Komentarz do art. 23, Nb. 2,* [w:] *Kodeks cywilny. Komentarz,* red. E. Gniewek, P. Machnikowski, Warszawa 2017, s. 61.
[165] Należy jednak zauważyć, że w orzecznictwie polskich sądów powszechnych istnieje pogląd odmienny, który prowadzi do braku przyznania pierwszeństwa poszczególnym prawom zagwarantowanym w MPPOiP. Zob. Wyrok SA w Gdańsku z dnia 25 kwietnia 2006 r., sygn. akt: I ACa 1877/05, LEX 466363.

najpowszechniej stosowaną umowę międzynarodową, gwarantującą podstawowe prawa człowieka, jest słusznym wniosek, aby dokument ten stał się podstawą do dalszego rozbudowania środków prawnych dotyczących ochrony prywatności w cyberprzestrzeni. Komitet Praw Człowieka nie posiada uprawnień organu sądowego, stąd też jest to skomplikowane w przypadku realizacji tego zamiaru[166].

Ważnym aktem była też Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Niewątpliwie stanowiła rezultat dokonanego skodyfikowania fundamentalnych praw wyartykułowanych w Powszechnej Deklaracji Praw Człowieka na płaszczyźnie europejskiej[167]. Została ona podpisana w dniu 4 listopada 1950 roku, natomiast weszła w życie w dniu 3 września 1953 roku[168]. Artykuł 8 jest uznany za najbardziej rozbudowaną regulację omawianych zagadnień. Nierozerwalnie wiąże się także z innymi prawami wymienionymi w Konwencji[169]. Zgodnie z ustępem 1. „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji". W ustępie 2. zawarto natomiast postanowienie, że „Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne oraz dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób"[170]. Z treści tego przepisu wynika, że zakaz ingerencji władzy publicznej w korzystanie z prawa do prywatności ze względu na charakter społeczeństwa demokratycznego, ma niemałe znaczenie z punktu zrozumienia możliwości zastosowania środków ograniczających prawo do prywatności przez władzę publiczną. Pomimo tego, że prywatność jest wartością powszechnie objętą ochroną, to nie ma ona charakteru bezwzględnego[171]. Dokonując wykładni art. 8 Europejskiej Konwencji Praw Człowieka,

---

[166] A. Gliszczyńska-Grabias, K. Sękowska-Kozłowska, R. Wieruszewski, *Koncepcja Światowego Trybunału Praw Człowieka,* „Państwo i Prawo" 2011, nr 5, s. 5-6.

[167] A. Bisztyga, *Geneza Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz Europejskiego Trybunału Praw Człowieka,* „Prawa Człowieka-Humanistyczne Zeszyty Naukowe" 1994, nr 1(9), s. 31-51.

[168] Europejska Konwencja Praw Człowieka została podpisana po powołaniu Rady Europy. Po zakończeniu II wojny światowej przykuwano większą uwagę do zapewnienia ludzkości podstawowych praw człowieka. Podejmowano starania mające na celu utworzenie nowego porządku politycznego, co w szczególności było widoczne w Europie. W konsekwencji, utworzono Radę Europy, czyli organizację międzynarodową stojącą na straży przestrzegania i rozwoju praw człowieka i podstawowych wolności. Zob. art. 1 pkt 2 Statutu Rady Europy z dnia 5 maja 1949 r. (Dz. U. 1994 nr 118, poz. 565).

[169] M. Pryciak, *Prawo do prywatności,* „Studia…", s. 220.

[170] E.H. Morawska, K. Gałka, *Standardy ochrony praw człowieka w prawie europejskiej konwencji praw człowieka,* Ministerstwo Sprawiedliwości, Warszawa 2011, s. 44.

[171] Art. 8 w ustępie 2. doprecyzowuje przesłanki, dla których władza publiczna w demokratycznym państwie prawnym może ingerować w ściśle określonych ku temu przypadkach, m.in. dla bezpieczeństwa państwowego,

trzeba zauważyć, że sfery chronione tym przepisem krzyżują się wzajemnie, tworząc przy tym rozbudowany katalog praw i wolności jednostki i odpowiadające im obowiązki władzy publicznej[172]. L. Leszczyński z kolei podnosi, że art. 8 Europejskiej Konwencji Praw Człowieka, obok sfery prywatności traktowanej wprost, wymienia również sferę nawiązującą do stosunków rodzinnych, mieszkania i korespondencji[173]. Nie może obejść się bez komentarza to, że twórcy Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności nie wprowadzili jednolitej definicji prywatności, a jedynie dookreślili katalog wartości, przez które należy interpretować zakres tego terminu. Dodatkowo, art. 8 Europejskiej Konwencji Praw Człowieka nie chroni czci i dobrego imienia[174]. W tym miejscu nasuwa się pewna wątpliwość. Nie jest do końca wiadome, czy należy to traktować jako wyłączenie spod ochrony, czy raczej z uwagi na otwarty charakter katalogu wartości cechujących sferę prywatności, należy *a priori* przyjąć, że ochrona dobrego imienia także wchodzi w zakres gwarancji, pomimo niewskazania jej wprost w treści normy.

Pomimo wprowadzenia do Konwencji katalogu praw i wolności, z których korzystają wszyscy jej sygnatariusze, Europejska Konwencja Praw Człowieka została uzupełniona o ustanowienie Europejskiego Trybunału Praw Człowieka, który miał zagwarantować przestrzeganie zobowiązań wynikających z Konwencji[175]. Rozwinięta judykatura ETPCz przyczyniła się do ugruntowania prawnego rozumienia zakresu, granic i możliwości ograniczenia prawa do prywatności w kulturze prawnej państw jako stron Konwencji. Trybunał potwierdził, że prywatność jest pojęciem szerokim, gdzie wręcz niemożliwe jest stworzenie jej jednolitej struktury definicyjnej[176]. Zwrócono uwagę jednak na to, że obszar życia prywatnego związany jest z identyfikacją osoby, a mianowicie z jej imieniem, nazwiskiem, a nawet zdjęciem. Celem gwarancji przewidzianej w art. 8 Konwencji jest stworzenie niezachwianego rozwoju osobistego jednostki w ramach społeczeństwa, stąd też,

---

bezpieczeństwa publicznego, dobrobytu gospodarczego kraju, ochrony porządku, zapobieganiu zamieszkom lub przestępczości, ochrony zdrowia i moralności, ochrony praw i wolności innych osób. Jest to katalog dóbr taksatywnie wyliczonych, co oznacza, że inne względy poza wymienionymi tutaj nie mogą stanowić podstawy naruszenia tej charakterystycznej sfery życia ludzkiego. Zob. M. Safjan, *Prawo do ochrony życia prywatnego,* [w:] *Szkoła Praw Człowieka…,* s. 214.

[172] L. Garlicki, *Komentarz do art. 8, Nb. 1,* [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, tom I, Komentarz do artykułów 1-18,* red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010, s. 479.

[173] L. Leszczyński, B. Liżewski, *Ochrona praw człowieka w Europie-szkic zagadnień podstawowych,* Lublin 2008, s. 88.

[174] A. Siostrzonek-Sergiel, *Prawo do prywatności a bezpieczeństwo publiczne…,* s. 409.

[175] Na początku organ sądowniczy miał inną strukturę organizacyjną, aniżeli teraz. Oznacza to, że Konwencja przewidywała ukonstytuowanie dwóch instytucji odpowiedzialnych za rozpatrywanie skarg, tj. Europejską Komisję Praw Człowieka oraz Europejski Trybunał Praw Człowieka. Pierwsza z nich miała pochylać się nad skargami indywidualnymi oraz międzypaństwowymi, natomiast druga odnosiła się do spraw wyłącznie międzypaństwowych i tylko takich, gdzie niemożliwe było polubowne rozstrzygnięcie sporu.

[176] Wyrok ETPCz z dnia 2 września 2010 r. w sprawie *Uzun vs. Niemcy,* sygn. akt: 35623/05, § 43.

dlatego niektóre działania podejmowane przez jednostkę w domenie publicznej mogą zostać objęte ochroną przewidzianą dla czynności życia prywatnego[177]. Mimo tego, że głównym celem ochrony podejmowanej w art. 8 przedmiotowej Konwencji jest zapewnienie jednostce bezpieczeństwa przed nadużyciem ze strony aparatu państwowego, nie oznacza to jednak, że granice normy powinny sprowadzać się jedynie do nakazu powstrzymywania się organów państwowych od wszelkiego rodzaju ingerencji. Nie mniej ważną powinnością jest istnienie konieczności stosowania środków dążących do zapewnienia poszanowania życia prywatnego w relacjach horyzontalnych[178], natomiast zaś w gestii państwa leży objęcie ochroną integralności moralnej jednostki przed działaniami ze strony innych osób[179].

Europejski Trybunał Praw Człowieka poruszył również aspekty odnoszące się do ochrony prywatności w związku z przetwarzaniem danych osobowych. Zwrócił uwagę na jakość danych oraz ich przydatność do realizacji celu przetwarzania jako powód czy dane mogą być w dalszym ciągu poddawane procesowi przetwarzania w granicach prawa[180]. Zagadnienie to odnosiło się przede wszystkim do gromadzonych przez upoważnione organy danych w celu zapobiegania czynom zabronionym i zapewnienia porządkowi publicznemu ochrony. Natomiast w kolejnym zaś rozpatrywanym przez ETPCz przypadku prawnym jednoznacznie wskazano, że ustawodawca krajowy powinien brać pod uwagę takie regulacje prawne, gdzie przetwarzanie danych osobowych będzie realizowane w sposób zgodny z tymi istniejącymi na kanwie art. 8 Konwencji. Zakres zbieranych danych miał być dostosowany do zamierzonego celu, a sposób ich przechowywania zezwalał na ustalenie tożsamości podmiotu danych tylko przez taki czas, który był potrzebny z uwagi na cel przetwarzania[181]. Z judykatury Europejskiego Trybunału Praw Człowieka wynika również, że tak samo gromadzenie, jak i udostępnienie informacji przez władzę publiczną odnoszących się do życia prywatnego, a ponadto odmowa usunięcia tych danych powodują wkroczenie w gwarancje wynikające z art. 8 ust. 1 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności[182]. Nie oznacza to jednak, że każda ingerencja stanowi naruszenie zobowiązań konwencyjnych. Nie jest nią ta, która ma zastosowanie do przesłanek wynikających z art. 8 ust. 2 Europejskiej Konwencji Praw Człowieka, czyli zgodna z prawem i konieczna

[177] Wyrok ETPCz z dnia 7 lutego 2012 r. w sprawie *von Hannover vs. Niemcy,* sygn. akt: 40660/08 oraz 60641/08, § 95.
[178] Wyrok ETPCz z dnia 24 lutego 1998 r. w sprawie *Botta vs. Włochy,* sygn. akt: 21439/93, § 33.
[179] Wyrok ETPCz z dnia 24 lipca 2012 r. w sprawie *Đorđević vs. Chorwacja,* sygn. akt: 41526/10, § 152.
[180] Wyrok ETPCz z dnia 6 czerwca 2006 r. w sprawie *Segerstedt-Wiberg i in. vs. Szwecja,* sygn. akt: 62332/00.
[181] Wyrok ETPCz z dnia 4 grudnia 2008 r. w sprawie *S. i Marper vs. Wielka Brytania,* sygn. akt: 30562/04, 30566/04.
[182] Wyrok ETPCz z dnia 26 marca 1987 r. w sprawie *Leander vs. Szwecja,* sygn. akt: 9248/81; wyrok ETPCz z dnia 4 maja 2000 r. w sprawie *Rotaru vs. Rumunia,* sygn. akt: 28341/95, § 46.

w społeczeństwie demokratycznym. Wymagane jest zatem zbadanie łącznego występowania tych dwóch kryteriów, aby można było mówić o jakiejkolwiek ingerencji aparatu państwowego, przy czym należy pamiętać, że muszą być one interpretowane zawężająco ze względu na charakter przepisu prawnego, określającego ograniczenie uprawnienia gwarantowanego niniejszą Konwencją. Trybunał przy tym uznał, że wymagane jest, aby środki ograniczające prawo do prywatności wynikały nie tylko z powszechnie obowiązującego prawa, ale i były zgodne z zasadą rządów prawa[183]. W tym znaczeniu, krajowe regulacje muszą być zrozumiałe dla jednostki oraz zapewniać transparentność, postrzeganą jako należytą ochronę przed arbitralnością. Oznacza to, że kontrola nad działaniem uprawnionych organów powinna wynikać z przepisów prawa i nie może polegać na nieograniczonej swobodzie podejmowania decyzji[184]. Wymóg podyktowany koniecznością stosowania jakiegokolwiek ograniczenia, pociąga za sobą istnienie istotnej potrzeby społecznej, z kolei zastosowany środek musi być proporcjonalny do zamierzonego i uzasadnionego prawem celu, przy czym dobrze by było, gdyby uwzględniał naturę prawa, na które oddziałuje[185]. Biorąc pod uwagę dorobek orzeczniczy Europejskiego Trybunału Praw Człowieka, trzeba liczyć się ze stale rosnącą przewlekłością postępowania, mającą niekorzystny wpływ na przydatność skorzystania z drogi skargowej prowadzącej do ochrony praw i wolności osobistych. Każda idea zmierzająca do zagwarantowania ochrony praw podstawowych na poziomie międzynarodowym, powinna uwzględniać nie tylko dylematy orzecznicze i wypływające z nich skutki widoczne w krajowych systemach prawnych, ale również związane z dostępnością prawnych środków ochrony charakterystycznych dla okresu koniecznego do wydania prawomocnego wyroku. Pomimo wzrostu świadomości tego problemu, nie udało się jeszcze wypracować efektywnych reform. Wynika to prawdopodobnie z faktu, że do Europejskiego Trybunału Praw Człowieka napływa ciągle wysoka liczba skarg. Świadczy to o tym, że Trybunał pomimo tego, że uważany jest za jedną ze skuteczniejszych form ochrony praw człowieka, to nie ma wpływu na znalezienie złotego środka, polegającego na możliwości rozpatrywania spraw przez państwa – strony Konwencji na poziomach krajowych porządków prawnych w zakresie ochrony praw podstawowych z powodu braku mocno wykształconych instrumentów prawnych[186].

Europejska Konwencja Praw Człowieka nie normuje bezpośrednio relacji z krajowym

[183] Wyrok ETPCz z dnia 24 kwietnia 1990 r. w sprawie *Kruslin vs. Francja,* sygn. akt: 11801/85.
[184] Postanowienie ETPCz z dnia 29 czerwca 2006 r. w sprawie *Weber i Saravia vs. Niemcy,* sygn. akt: 54934/00, § 92-94.
[185] Wyrok ETPCz z dnia 14 września 1987 r. w sprawie *Gillow vs. Wielka Brytania,* sygn. akt: 9063/80, § 55.
[186] *Wprowadzenie, Nb. 10,* [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, tom I. Komentarz do artykułów 1-18,* red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010, s. 23.

porządkiem prawnym, stąd też problematyka ta pozostaje do rozwiązania przez państwa – strony Konwencji. Dominuje jednak system, zgodnie z którym Konwencja jako umowa międzynarodowa znajduje się w hierarchii aktów normatywnych pomiędzy Konstytucją a regulacjami rangi ustawowej. Takie rozwiązanie jest aktualne także w polskim systemie prawnym. Europejska Konwencja Praw Człowieka stanowi część krajowego porządku prawnego, a w sytuacji kolizji norm korzysta z pierwszeństwa przed ustawami zwykłymi jako ratyfikowana umowa międzynarodowa[187]. Tak też, na podstawie art. 46 Europejskiej Konwencji Praw Człowieka, kraje członkowskie są zobligowane do wypełniania ostatecznych orzeczeń Europejskiego Trybunału Praw Człowieka, gdzie posiadają status stron. Wyrok Trybunału zobowiązuje wręcz dane państwo do usunięcia stwierdzonego naruszenia Konwencji, ale sposób realizacji pozostaje w dyspozycji regulacji krajowych systemów prawnych. Jednakże, należy pamiętać, że wydany wyrok nie jest adresowany *erga omnes,* zatem nie odnosi się do spraw jednostkowych, zawisłych przed sądami krajowymi, jak też nie określa zakresu obowiązków w stosunku do innych państw, będących stronami Konwencji. Orzeczenia Europejskiego Trybunału Praw Człowieka mają charakter deklaratoryjny, a w zakresie stwierdzenia naruszenia Konwencji korzystają z powagi rzeczy osądzonej *res iudicata*[188]. W granicach, w jakich orzeczenie ETPCz ma moc wiążącą, państwo nie może kwestionować sytuacji, czy do naruszenia doszło, czy też nie. Oprócz tego, zobowiązane jest do podjęcia określonych kroków zmierzających do realizacji wyroku[189].

Warta uwagi jest również Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, która w skali międzynarodowej stanowiła pierwszy akt prawny odnoszący się do ochrony danych osobowych, więc siłą rzeczy także i do prywatności[190]. Stanowiła ona rezultat przyjęcia przez Komitet Ministrów Rady Europy rezolucji nr 73/22, a także 74/29 oraz była wynikiem rozwoju prawodawstwa krajowego wśród państw członkowskich Rady Europy. Pomimo tego, że została podpisana w 1981 roku, to jej okres *vacatio legis* trwał przez kolejne cztery lata[191]. Problematyka ochrony danych osobowych już wtedy była na tyle ważna, że zezwolono nawet państwom nienależącym do Rady Europy na przystąpienie do Konwencji, co miało potwierdzić potrzebę

[187] D. Miąsik, A. Wróbel, *Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności,* [w:] *Europeizacja prawa administracyjnego. System Prawa Administracyjnego,* red. R. Hauser, tom 3, Warszawa 2014, s. 277.
[188] Wyrok ETPCz z dnia 30 lipca 2009 r. w sprawie *VgT vs. Szwajcaria,* sygn. akt: 32772/02, § 61.
[189] Postanowienie SN z dnia 17 kwietnia 2007 r., sygn. akt: I PZ 5/07, „OSNAPiUS-Orzecznictwo Sądu Najwyższego" 2008, nr 13-14, poz. 196.
[190] Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. 2003 nr 3, poz. 25).
[191] Konwencja nr 108 Rady Europy weszła w życie w dniu 1 października 1985 roku.

wspólnego porozumienia w wypracowaniu standardów w zakresie przetwarzania danych osobowych[192]. To posunięcie uznano za krok milowy w historii rozwoju ochrony prywatności rozwijającej się w sieciach informatycznych. Choć z jednej strony, Konwencja nr 108 jako umowa międzynarodowa oznacza akt normatywny prawnie wiążący, a więc postanowienia w niej zawarte wręcz muszą zostać zaimplementowane w krajowych porządkach prawnych państw – sygnatariuszy, to z drugiej strony przyczyniło się to w znacznym stopniu do poszerzenia ochrony praw podstawowych, w tym ochrony prywatności w ten sposób, że Konwencja nr 108 nie określała jedynie nowych postanowień, ale rozszerzała dotąd już istniejące uprawnienia. Tak też, zgodnie z definicją wprowadzoną w art. 2 Konwencji nr 108 za dane osobowe należy traktować wszelkie informacje związane z osobą fizyczną o ustalonej albo dającej się zidentyfikować tożsamości[193].

Główne reguły ochrony danych zostały wyrażone w Rozdziale II Konwencji nr 108. Na ich podstawie, państwa, będące stronami Konwencji, powinny wdrożyć do swoich systemów prawnych takie rozwiązania, które gwarantowałyby podmiotom danych m.in. prawo do informacji w zakresie istnienia zbioru danych osobowych i celu jego powstania czy prawo do sprostowania lub usunięcia informacji, pod warunkiem, że zostały przetworzone z naruszeniem przepisów prawa wewnętrznego. Konwencję nr 108 można traktować jako pierwsze europejskie ramy prawne gwarantujące ochronę danych osobowych[194]. Oprócz tego, Konwencja, będąca zarazem umową międzynarodową, tak naprawdę zaliczana była do prawnie wiążących aktów normatywnych odnoszących się do ochrony danych, dopóki nie weszło w życie nowe Rozporządzenie 2016/679[195]. O znaczeniu Konwencji nr 108 świadczyło także przystąpienie do niej krajów spoza europejskiego kręgu kulturowego, w rezultacie czego stała się ona początkiem budowy ponadregionalnych standardów ochrony danych osobowych. Przedstawiona dotąd w pozytywnym świetle Konwencja, nie była natomiast pozbawiona luk. Po pierwsze, jej postanowienia adresowane były do państw, których rola polegała na przenoszeniu rozwiązań do krajowego porządku prawnego, dlatego przepisy umowy mogły być różnie interpretowane w poszczególnych państwach. Był to jeden z powodów, dla których Komisja Europejska podjęła decyzję w odniesieniu do przygotowania samodzielnego projektu regulacji w obszarze ochrony danych osobowych, którym miała być

[192] Polska ratyfikowała Konwencję w dniu 23 maja 2002 roku, a jej postanowienia weszły w życie do polskiego porządku prawnego w dniu 1 września 2002 roku.
[193] Jest to analogiczna definicja do tej przedstawionej w wytycznych Organizacji Współpracy Gospodarczej i Rozwoju.
[194] Grupa Robocza Artykułu 29 ds. Ochrony Danych, Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości, *Przyszłość prywatności,* [dostęp:] http://www.giodo.gov.pl/data/filemanager_pl/Dokument%20WP%20168%20wersja%20nieoficjalna.pdf, s. 6.
[195] *Podręcznik europejskiego prawa o ochronie danych,* Urząd Publikacji Unii Europejskiej 2014, s. 16.

Dyrektywa 95/46/WE[196]. Należy jednak dostrzec, że nawet po uwzględnieniu treści Protokołu Dodatkowego, Konwencja nr 108 jest niekompletna. Przejawia się to w braku postanowień trwale związanych z europejskim modelem ochrony danych, jak również prawodawstwem krajowym[197]. W 1999 r. określono zasady nowelizacji Konwencji nr 108, które miały ułatwić przystąpienie Unii Europejskiej do Konwencji[198]. Według danych na dzień 22 marca 2018 roku zaproponowane nowe postanowienia nie zostały zatwierdzone przez niektóre strony, do których przynależą też państwa członkowskie Unii Europejskiej[199].

Problemy zaczęły być także dostrzegane przez instytucje Rady Europy oraz sygnatariuszy Konwencji. W związku z tym, w 2010 roku podjęto szereg prac nad przygotowaniem projektu zmian, dostosowujących treść Konwencji do obecnych potrzeb w ramach obszaru ochrony danych. Najpierw prace były realizowane przez Komitet Doradczy. Na ich końcowym etapie, projekt przekazano Międzynarodowemu Komitetowi ds. Ochrony Danych[200] do dalszej analizy. W ostateczności Projekt Zmiany Konwencji[201] został przyjęty przez Komitet na posiedzeniu w dniach 15-16 czerwca 2016 roku[202]. Należy jeszcze zauważyć, że zakres postulowanych zmian dostosowywał wszelkie kwestie, a mianowicie definicje, uprawnienia podmiotów danych, obowiązki administratorów oraz reguły przetwarzania danych do tych akceptowanych przez unijny model ochrony danych, zwłaszcza wprowadzonych w późniejszym czasie w Ogólnym Rozporządzeniu o Ochronie Danych Osobowych.

1.2.4. Ochrona prawa do prywatności w prawie polskim

Zaczynając od dokonania analizy regulacji konstytucyjnych w przedmiocie ochrony

[196] Komunikat Komisji Europejskiej z dnia 13 września 1990 r. na temat ochrony jednostek w związku z przetwarzaniem danych osobowych we Wspólnocie oraz bezpieczeństwa informacji, COM (90) 314 final, CELEX: 51990DC0314, s. 3-4.
[197] Za przykład może posłużyć nieuwzględnienie w Konwencji nr 108 zgody podmiotu danych stanowiącej podstawę do gromadzenia i przetwarzania danych osobowych.
[198] Rada Europy, *Amendments approved by the Committee of Ministers,* Strasburg, [dostęp: 15.06.1999] http://rm.coe.int/168008c2b8.
[199] Zapewne było to spowodowane tym, że państwa te podjęły decyzję o budowie własnego systemu ochrony danych na podstawie aktów normatywnych na poziomie unijnym oraz w oparciu o instytucje sądowe. Źródło: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.
[200] *ad hoc*. Committee on Data Protection, CAHDATA 2016.
[201] Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, [dostęp:] https://rm.coe.int/16806a616c.
[202] M. Ciechomska, *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych,* „Monitor Prawniczy" 2017, nr 16, s. 877.

prawa do prywatności – w Konstytucji z okresu II Rzeczypospolitej Polskiej[203] i Polskiej Republiki Ludowej[204] należy podnieść, że nie znajdowało się w nich *expressis verbis* wyrażone sformułowanie, które odnosiłoby się bezpośrednio do prawa do prywatności[205]. Niemniej jednak, nie można stwierdzić, że nie było żadnych gwarancji związanych z przedmiotowym prawem. W tzw. Konstytucji Marcowej przewidziano kolejno w art. 97 – ochronę nietykalności osobistej, w art. 100 – ochronę miru domowego, a w art. 106 – zachowanie tajemnicy korespondencji. Zaś treść art. 68 ust. 2 Konstytucji Kwietniowej zakresem swej ochrony obejmowała następujące wartości, tj. wolność osobistą, wolność mieszkania i tajemnicę korespondencji. Mimo tego, Konstytucja Kwietniowa w znacznym stopniu powodowała ograniczenie praw i wolności osobistych w kontaktach z władzą publiczną. Potwierdzeniem tego był przepis art. 10 ust. 1, na podstawie którego żadna podejmowana czynność nie mogła pozostawać w sprzeczności z celami państwowymi, przejawiającymi się w ich prawach. Oprócz niniejszego art. 5 dyktował, że państwo zapewniało swoim obywatelom możliwość rozwoju osobistego, przyznawało wolność słowa, sumienia i zrzeszeń, jednakże ograniczane one były poprzez dobro powszechne. W Konstytucji PRL prawo do prywatności kształtowało się nieco odmiennie. Przejawiało się ono w regulacji odnoszącej się w art. 74 ust. 1 do nietykalności osobistej, natomiast nienaruszalność mieszkania i tajemnicę korespondencji, uregulowane w kolejnym ustępie, delegowano do regulacji ustawy zwykłej. Niemniej jednak poszanowanie tych wartości było znikome, a to z uwagi na brak przejawów szacunku do panujących zasad rządów prawa w okresie PRL.

Trybunał Konstytucyjny przyjrzał się prawnej regulacji ochrony prywatności w oparciu o nadal obowiązujące przepisy Konstytucji PRL. Podstawą rozważań był art. 1 Konstytucji[206], który charakteryzował Rzeczpospolitą Polską jako demokratyczne państwo prawne. W oparciu o to uznano, że z rzeczonej zasady niewątpliwie można wywieść istnienie samoistnego prawa do prywatności przejawiającego się w zachowaniu w tajemnicy informacji o swoim życiu prywatnym[207].

---

[203] Ustawa z dnia 17 marca 1921 r.-Konstytucja Rzeczypospolitej Polskiej (Dz. U. 1921 nr 44, poz. 267); Ustawa Konstytucyjna z dnia 23 kwietnia 1935 r. (Dz. U. 1935 nr 30, poz. 227).

[204] Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dniu 22 lipca 1952 r. (Dz. U. 1952 nr 33, poz. 232).

[205] K. Nowak, *Kompetencje głowy państwa w zakresie zwierzchnictwa nad siłami zbrojnymi i bezpieczeństwa państwa w okresie prowizorium konstytucyjnego Polski Ludowej (1944-1952),* „Ius et Administratio" 2013, nr 3, s. 111.

[206] Ustawa z dnia 19 grudnia 1989 r. o zmianie Konstytucji Rzeczypospolitej Ludowej (Dz. U. 1989 nr 75, poz. 444).

[207] Wyrok TK z dnia 24 czerwca 1997 r., sygn. akt: K 21/96…

Wraz z postępującymi przemianami politycznymi po 1989 roku oraz z wiążącym się z tym wzrostem znaczenia ochrony systemu praw człowieka, problematyka zakresu prawnej ochrony praw człowieka stała się przedmiotem analizy orzecznictwa. Z wejściem w życie Konstytucji RP w 1997 r. ochrona prywatności zyskała miano gwarancji konstytucyjnej. Normy kształtujące prawa podmiotowe i nakładające na państwo określone obowiązki składają się na zasadę ochrony prywatności[208]. Sfera prywatna jest otwarta na oddziaływanie z zewnątrz, zatem wkraczanie w nią przez władzę nie jest identyczne[209].

Konstytucja RP nie posługuje się pojęciem prawa do prywatności. Prawo do prywatności można określić przy pomocy analizy poszczególnych norm konstytucyjnych[210]. J. B. Young potwierdził, że „prywatność jest jak słoń – łatwiej ją rozpoznać niż opisać"[211]. Z całego katalogu praw człowieka, prawo do prywatności jest tym, które najtrudniej określić.

W artykule 47 Konstytucji RP wskazano obszary, które kojarzone są z życiem prywatnym. Postanowienia konstytucyjne gwarantujące ochronę życia prywatnego są ogólnikowe, nie do końca sprecyzowane. Tak też, można przyjąć, że dobra osobiste stanowiące składniki prywatności nie mogą być enumeratywnie wyliczone. Przepis ten nie zawiera w sobie katalogu zamkniętego. Dobra chronione służą jedynie ukazaniu przykładowych wartości. Jednak tam zamieszczone, winny być postrzegane jako standardy obowiązujące w polskim społeczeństwie[212].

Trybunał Konstytucyjny w jednym ze swoich orzeczeń wykroczył nieco poza zakres sformułowany w art. 47 Konstytucji RP. Do wartości w nim wyliczonych dodał jeszcze godność[213], podkreślając tym samym jej doniosłe znaczenie dla prywatności. Trybunał Konstytucyjny trafnie przyjął, iż „ochrona prywatności i autonomii informacyjnej jest konsekwencją ochrony przyrodzonej i niezbywalnej godności człowieka"[214]. We współczesnym świecie przejawem godności człowieka jest umiejętność bycia podmiotem dotyczących go danych[215]. Pozbawienie jednostki tego uprawnienia koliduje z wartościami demokratycznego państwa prawnego[216]. Aby można było mówić o zachowaniu przez

[208] K. Łakomiec, *Konstytucyjne gwarancje ochrony prywatności informacyjnej…,* s. 64.
[209] Wyrok TK z dnia 5 marca 2013 r., sygn. akt: U 2/11, OTK-A 2013, nr 3, poz. 24.
[210] M. Safjan, *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych,* „Kwartalnik Prawa Publicznego" 2002, z. 1, s. 233.
[211] J.B. Young, *Privacy,* Chichester 1978, s. 3.
[212] L. Garlicki, P. Sarnecki, *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Warszawa 2003, t. 3, s. 2.
[213] Wyrok TK z dnia 12 grudnia 2005 r., sygn. akt: K 32/04…
[214] Wyrok TK z dnia 30 lipca 2014 r., sygn. akt: K 23/11…
[215] R. Piotrowski, *Prawo do tożsamości informacyjnej i jego znaczenie w ustroju demokratycznym,* [w:] *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka,* red. J. Jaskiernia, Warszawa 2013, s. 479.
[216] R. Piotrowski, *Demokratyczne państwo prawne a lustracja,* „Państwo i Prawo" 2007, nr 6, s. 3-18.

człowieka godności, to wymagane jest przede wszystkim poszanowanie jego sfery osobistej. Człowiek nie może być przymuszony do przeżywania z innymi swoich wydarzeń, dzielenia się swoimi prywatnymi doznaniami o intymnym charakterze.

Preambuła Konstytucji RP nadaje normatywny charakter proklamowanym w art. 47 wartościom[217]. Te wartości winny stanowić punkt kulminacyjny przy dokonywaniu oceny poszczególnych norm konstytucyjnych. Według Leszka Garlickiego, przepisom szczegółowym należy nadawać znaczenie, które będzie odzwierciedleniem realizacji tychże zasad, a z drugiej zaś strony nie może im być nadawane takie znaczenie, które pozostałoby w sprzeczności z zasadami[218]. Joanna Braciak nadmienia, że analiza tego przepisu stanowi wskazówkę, w jaki sposób można stosować normy odnoszące się do poszczególnych dóbr związanych z życiem prywatnym.

Jak słusznie się zauważa, powstały dwa modele tego prawa. Pierwszy model jako „prawo do prywatności", „prawo do poszanowania prywatności", „prawo do ochrony życia prywatnego" lub pod inną tożsamą nazwą, został poddany ochronie w Konstytucji RP. Treść art. 47 ustawy zasadniczej w stosunku do innych ma charakter subsydiarny. To oznacza, iż „jeżeli jakaś materia nie została objęta szczegółowymi unormowaniami o konkretnych elementach prywatności, to gwarancje poszanowania życia prywatnego można wyprowadzić bezpośrednio z postanowień art. 47"[219]. Zatem inne prawa i wolności mieszczące się w sferze prywatności są rozwinięciem prawa do prywatności i zawierają się w przepisach szczególnych. W związku z tym, wszelkie mogące powstać kolizje pomiędzy chronionymi wartościami ze sfery prywatnej są rozpatrywane przez odwołanie się do klauzuli generalnej, czyli do prawa do prywatności. W drugim modelu, prawo do prywatności nie jest wyrażone w ustawie zasadniczej, co skutkuje „wyprowadzeniem tego prawa z postanowień konstytucyjnych chroniących inne prawa i wolności, a jego treść jest zasadniczo sumą tych praw"[220]. Dla skuteczności ochrony prywatności musi zaistnieć jej związek z innymi prawami.

W opinii M. Safjana ochrona prywatności posiada charakter samoistny. Dla jej skuteczności nie musi istnieć związek z innymi prawami jednostki[221]. Ten pogląd aprobuje również H. Szewczyk, podnosząc, że źródłem prywatności jest sama konstytucja, która obok proklamowania prawa do ochrony prywatności wyraża prawo do decydowania o swoich

[217] Wyrok TK z dnia 12 września 2005 r., sygn. akt: SK 13/05 (Dz. U. 2005 nr 186, poz. 1566).
[218] L. Garlicki, *Uwagi do wstępu do Konstytucji,* [w:] *Konstytucja RP. Komentarz,* red. L. Garlicki, t. 5, Warszawa 2007, s. 3.
[219] J. Braciak, *Prawo do prywatności…*, s. 164.
[220] M. Gdula, *Wprowadzenie do prawa do prywatności w prawie polskim…,* s. 38.
[221] M. Safjan, *Prawo do ochrony życia prywatnego…*, s. 127.

prawach osobistych. Stąd też można wysnuć wniosek, że jednostce przysługuje władztwo nad jej informacjami, które nie powinno jedynie polegać na wyrażaniu zgody na ich rozpowszechnianie, ale sprowadzać się do ich ochrony przed dostępem innych osób[222].

Analiza treści art. 47 ustawy zasadniczej nasuwa A. Mednisowi kilka refleksji. Jego zdaniem, ten przepis odnosi się do wartości obejmującej szerszy zakres od prywatności. Można przyjąć, że celem prawodawcy jest potwierdzenie, że zakres przedmiotowy ochrony obejmuje szeroko rozumianą autonomię woli jednostki. Ponadto, przepis ten akcentuje wąskie rozumienie pojęcia życia prywatnego, ograniczonego do ochrony tajemnicy sfery najbliższej jednostce. Definicja życia prywatnego nie obejmuje w związku z tym swobody decydowania o swoim życiu osobistym. Życie osobiste zostało potraktowane jako odrębna wartość. Niemniej jednak, nie ulega wątpliwości, że powodem umieszczenia w jednym przepisie wartości, jak ochrona życia prywatnego, rodzinnego, czci i dobrego imienia, jak też prawo do decydowania o swoim życiu osobistym jest wykazanie ich łącznych relacji. Tak też ograniczenie swobodnego decydowania o swoim życiu, będzie przejawem ograniczenia prywatności[223]. Prywatność postrzegana jako tajemnica życia osobistego jest ujęciem dokładniejszym, chociaż wyznaczenie linii granicznej pomiędzy prawem do nieujawniania informacji o swoim życiu osobistym a prawem do zachowania przez jednostkę autonomii nie jest możliwe, stąd też autonomia woli jednostki stanowi element prywatności[224].

Porównując zakres przedmiotowy z zakresem podmiotowym, to ten pierwszy jest znacznie szerszy od drugiego. Analizując orzecznictwo Trybunału Konstytucyjnego, nietrudno zauważyć, że stoi on na stanowisku, że w art. 47 Konstytucji RP zagwarantowane zostały dwie oddzielne sytuacje. Obie te normy konstytucyjne określa się mianem prawa do prywatności[225]. *Prima facie,* jest to prawo jednostki do ochrony prawnej wskazanych w nim wartości, a po drugie wolność podejmowania decyzji.

Pierwsza sfera powinna być precyzyjnie unormowana przez władzę państwową. Zatem można przyznać, że ma ona w swej istocie charakter prawny. Prawu jednostki winna towarzyszyć regulacja ustawowa, która obierze za swój cel ochronę prywatności, życia rodzinnego, czci i dobrego imienia. Stąd też konieczne jest zaistnienie unormowania prawnego, które pozwoli bronić wskazanych wartości[226]. Odpowiedzialność władzy publicznej nie zacieśnia się tylko do zobowiązań negatywnych, odnoszących się do

[222] H. Szewczyk, *Ochrona dóbr osobistych w zatrudnieniu,* Kraków 2007, s. 124.
[223] A. Mednis, *Prawo do prywatności…,* s. 113.
[224] *Tamże,* s. 115.
[225] Wyrok TK z dnia 5 marca 2013 r., sygn. akt: U 2/11…
[226] *Tamże.*

powstrzymywania się przed nieuprawnionym wkraczaniem w wartości chronione. Przejawia się także pod postacią realizacji przesłanek pozytywnych polegających na poszanowaniu prywatności w relacjach horyzontalnych. Środkiem spełnienia tego celu jest wdrożenie należytych mechanizmów prawnych. W przypadku naruszenia prawa do prywatności, każdemu powinna przysługiwać droga sądowa, a jej pominięcie jest wystarczające do uznania badanego przepisu za niezgodny z Konstytucją RP[227].

Po wtóre, zakazana jest ingerencja w wolność ukształtowania przez dany podmiot swojego życia osobistego wedle własnych upodobań. Innymi słowy, ustrojodawca wykluczył możliwość ingerowania w życie osobiste podmiotu[228]. Przedstawiciele nauki prawa konstytucyjnego zwracają uwagę na okoliczność, że prawo gwarantowane na mocy ww. przepisu jest prawem do ochrony sfery życia, niezwiązanej bezpośrednio z wykonywaniem przez uprawniony podmiot kompetencji organów władzy publicznej[229] oraz podejmowaniem się innych działań wraz z prowadzeniem działalności o publicznym zasięgu[230]. Ustawa zasadnicza zobowiązuje wręcz władze publiczne do nieangażowania się w określony przez prawo do prywatności obszar działań podejmowanych przez jednostkę. Zapewnia to ochronę przed wszelkimi jego naruszeniami. Co ważne, należy podkreślić, że nie można ograniczyć stosowania przepisów Konstytucji RP wyłącznie do stosunków zacieśniających się pomiędzy jednostką a władzą publiczną[231]. Adresatami jest państwo i jego obywatele[232].

Druga sfera odnosi się więc do wolności. Winna ona polegać na zakazaniu wkroczenia jakiejkolwiek zewnętrznej ingerencji w życie osobiste jednostki[233]. Wolność ta jest przejawem także wolności jako wartości ogólnej człowieka ugruntowanej na podstawie przepisu 31 ust. 1 Konstytucji RP oraz wolności osobistej w ścisłym tego słowa znaczeniu w świetle art. 41 ust. 1 Konstytucji RP[234]. Paweł Sarnecki uważa, że w tym wypadku lepiej używać sformułowania „wolność od ingerencji w sfery prywatne", niźli „prawo do prywatności"[235]. Znalazło to swoje odzwierciedlenie w jednym z wyroków Trybunału Konstytucyjnego, niemniej jednak

---

[227] Wyrok TK z dnia 18 lipca 2011 r., sygn. akt: K 25/09, OTK-A 2011, nr 6, poz. 57.
[228] P. Sarnecki, *Komentarz do art. 47 Konstytucji Rzeczypospolitej Polskiej,* [w:] *Konstytucja Rzeczypospolitej Polskiej, Komentarz, tom III,* red. L. Garlicki, Warszawa 2003, s. 1.
[229] R. Grabowski, S. Grabowska, A. Młynarska-Sobaczewska, W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej…,* s. 396.
[230] Wśród rodzajów działalności publicznej wymienia się działalność pisarską, dziennikarską, aktorską, charytatywną, leczniczą, nauczycielską oraz duszpasterską. Zob. P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.,* Warszawa 2000, s. 114.
[231] S. Rozmaryn, *Konstytucja jako ustawa zasadnicza PRL,* Warszawa 1967, s. 132.
[232] Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01…
[233] M. Jabłoński, *Klasyfikacja wolności i praw jednostki w Konstytucji RP,* [w:] *Wolności i prawa jednostki w Konstytucji RP. Idee i zasady przewodnie konstytucyjnej regulacji wolności i praw jednostki w RP, tom I,* red. M. Jabłoński, Warszawa 2003, s. 1.
[234] Wyrok TK z dnia 5 marca 2013 r., sygn. akt: U 2/11…
[235] P. Sarnecki, *Komentarz do art. 47 Konstytucji…,* uwaga 3, s. 1.

trzeba przyznać, że znacznie częściej posługuje się terminem „prawo do prywatności". Inni przedstawiciele nauki również twierdzili, że w tej sytuacji, a także analogicznej do niej, należy mówić o wolności, a nie o prawie[236]. Wiesław Skrzydło, choć nie rozwinął swojej myśli, stwierdził, że „generalne postanowienia art. 47 ustawy zasadniczej są na tyle ogólne, że pojawia się niewątpliwa konieczność bliższego określenia tego prawa i płynących stąd konsekwencji prawnych, czego zresztą Konstytucja RP nie zapowiada"[237]. Bogusław Banaszak zdefiniował życie prywatne jako „przymioty, wewnętrzne przeżycia osobiste (jednostkowe) człowieka i ich oceny, refleksje dotyczące wydarzeń zewnętrznych i jego wrażenia zmysłowe, a także stan zdrowia"[238].

Życie prywatne jest przeciwieństwem definicji życia publicznego, zwłaszcza politycznego. Trybunał Konstytucyjny doszedł do podobnego wniosku. Zdefiniował samą prywatność (nie życie prywatne) jako „prawo do życia własnym życiem, układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[239]. Życie publiczne obejmuje relacje człowieka ze współmieszkańcami w sposób anonimowy, niepołączony więzami osobistymi. W ramach tych relacji można wyróżnić stosunki społeczne oraz zawodowe. Na sferę życia prywatnego składają się relacje rodzinne[240] i przyjacielskie. Ogólny wniosek, który można wysnuć, sprowadza się do tego, że życie prywatne dzieli się na życie rodzinne (więzy małżeńskie oraz rodzinne) oraz życie osobiste (pozostałe przypadki niemające charakteru publicznego). Ochrona prawna, wynikająca z art. 47 ustawy zasadniczej, obejmuje wszelkie przejawy postępowania w wymienionych relacjach, tj. wypowiedzi, wyrażanie opinii, swojego światopoglądu, przekonań i innych[241]. Ochrona polega na ustalaniu gwarancji prawnych zapobiegającym ingerowaniu czynników zewnętrznych w sferę życia prywatnego[242].

Życie rodzinne jest szerszym pojęciem od życia prywatnego. Bierze ono swój początek w przeżyciach i wydarzeniach odnoszących się do najbliższych człowiekowi osób. W literaturze prawa konstytucyjnego podkreśla się, że nie jest wymagane prowadzenie wspólnego gospodarstwa domowego. Co więcej, do tego kręgu niekoniecznie muszą

[236] A. Mednis, *Prawo do prywatności…,* s. 79.
[237] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Warszawa 2013, s. 49-67.
[238] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Warszawa 2012, s. 295.
[239] Wyrok TK z dnia 11 października 2011 r., sygn. akt: K 16/10 (Dz. U. 2001 nr 240, poz. 1436).
[240] Zacieśniając bardziej tę definicję, życie rodzinne stanowią stosunki małżeńskie oraz te, które wynikają z więzów pokrewieństwa i powinowactwa-stąd też ochrona życia rodzinnego stanowi przejaw ochrony życia prywatnego.
[241] B. Szmulik, *Ochrona prawna,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz Encyklopedyczny,* red. W. Skrzydło, S. Grabowska, R. Grabowski, Warszawa 2009, s. 292.
[242] Z. Zawadzka, *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną. Problem rozstrzygania konfliktu zasad,* Warszawa 2013, s. 57.

wchodzić wszyscy posiadani krewni i powinowaci danej jednostki. Nieco odmienny komentarz można zauważyć u Pawła Sarneckiego. Nalega się, aby ugruntować jednolite stanowisko w kwestii, czy pomimo braku zażyłych relacji z jednym z członków rodziny nie powinno w ostateczności mówić się i tak o elemencie życia rodzinnego, chronionego na podstawie omawianej normy konstytucyjnej. Pytanie to raczej do dziś pozostaje otwarte. Dla innych, życie rodzinne odnosi się do szeregu relacji międzyludzkich, które wynikają z więzi krwi, bądź prawa – i tak znów Paweł Sarnecki w zaprezentowanej przez siebie argumentacji podał nieco odmiennie, że należy je rozumieć w świetle przyjętych norm i standardów w tym kręgu cywilizacyjnym, w którym człowiek na co dzień obcuje.

Zakres podmiotowy prawa do prywatności nie wydaje się budzić większych wątpliwości. Posłużenie się w art. 47 ustawy zasadniczej terminem „każdy" pozwala wnioskować, że prawo to odnosi się do wszystkich osób fizycznych i prawnych, które przebywają na terytorium Rzeczypospolitej Polskiej, a tym samym podlegają polskiemu prawu. Bogusław Banaszak doprecyzował, że omawiane prawo przysługuje wszystkim osobom fizycznym ze względu na zdolność do posiadania przez nie życia prywatnego, rodzinnego, czci i dobrego imienia[243]. Rodzi się jednak pytanie, czy zakres ten można rozszerzyć poza krąg osób fizycznych. Prawodawca, używając słowa „każdemu" i posługując się w ten sposób najszerszą z możliwych formułą, nie uczynił tego bez powodu. Nie sposób pominąć przepisów prawa cywilnego związanych z obszarem ochrony dóbr osobistych. Ustawa cywilna już w brzmieniu pierwotnym wprowadzała prawną ochronę czci i dobrego imienia, nietykalności mieszkania czy tajemnicy korespondencji. Obszar jej ochrony w znacznym stopniu wyczerpywał katalog elementów uwzględnionych w definicji życia prywatnego na gruncie międzynarodowych systemów praw człowieka. Zważyć należy jednak na pewne różnice. W art. 23 k.c. nie posłużono się wprost terminem ochrony życia prywatnego, dlatego przepisu tego nie można traktować jako wystarczające źródło ochrony jednostki przed ingerencją w sferę prywatności, która rozumiana jest jako prawo do bycia pozostawionym w spokoju w znaczeniu szerokim. Co prawda, tylko osoba fizyczna może posiadać życie prywatne, rodzinne i cześć. W przypadku dobrego imienia, czyli dbałości o pozytywną opinię społeczną, sprawa nie jest już na tyle łatwa. Warte podkreślenia jest, że ustrojodawca użył sformułowania zespolonego. Pomiędzy terminem „cześć" a „dobre imię" występuje koniunkcja. Nie przesądza to jednak o tym, że tworzy to tylko jedną normę prawną. W literaturze przedmiotu zdania w tej materii są podzielone[244]. Jedni uważają, że

[243] B. Banaszak, *Konstytucja Rzeczypospolitej…,* s. 294.
[244] Wyrok SN z dnia 10 listopada 2005 r., sygn. akt: V CK 314/05, Legalis 181192.

twórca Konstytucji RP miał na celu jedynie zabieg stylistyczny. Inni są zdania przeciwnego[245].

Cześć należy interpretować szeroko jako wewnętrzne przekonanie podmiotu o swojej wartości i wynikającym z niej szacunku do siebie samego. Dobre imię natomiast oznacza zabieganie jednostki o pozytywną opinię wyrażaną przez innych[246]. Oznacza to, że godzenie w cześć człowieka będzie dla niego boleśniejszym odczuciem ingerencji w jego prawo do prywatności, niźli miałoby to miejsce w przypadku dobrego imienia. Dobra te powinny *de facto* stworzyć reguły prawidłowego postępowania tak w sferze życia prywatnego, jak i publicznego. Sąd Najwyższy uznał, iż „cześć i dobre imię są pojęciami obejmującymi wszystkie dziedziny życia osobistego, zawodowego i społecznego. Naruszenie czci może nastąpić nie tylko przez pomówienie o ujemne postępowanie w życiu osobistym, ale także przez zarzucenie niewłaściwego postępowania w życiu zawodowym czy działalności publicznej, naruszające dobre imię danej osoby i mogące ją narazić na utratę zaufania potrzebnego do wykonywania działalności"[247]. Aczkolwiek, analizując szerzej orzecznictwo sądów powszechnych, można wysnuć wniosek, że niektóre sądy apelacyjne traktują, że cześć przejawia się zarówno w aspekcie zewnętrznym i wewnętrznym. Ten pierwszy odnosi się do dobrego imienia, drugi zaś do godności osobistej[248]. Naruszenie dobrego imienia może łączyć się z pomawianiem innej osoby o takie postępowanie, które doprowadzi do poniżenia jej w opinii publicznej, narazi na utratę zaufania potrzebnego dla danego stanowiska i zawodu. Obrazę stanowi naruszenie godności osobistej[249]. Cześć i dobre imię należy rozumieć tak samo albo co najmniej podobnie jak i w Konstytucji RP, tak i na gruncie przepisów ustawy cywilnej. Co prawda, można przyjąć, że dobre imię jest pojęciem węższym od czci, a zatem w niej się zawierającym. Z tego wynika, że tak naprawdę cześć i dobre imię stanowią jedną wartość. Aczkolwiek zdaniem Arwida Mednisa mają one niewiele wspólnego z prawem do prywatności. W jego ocenie z godzeniem w cześć lub dobre imię mamy do czynienia w momencie, kiedy do wiadomości osób trzecich napływają nieprawdziwe, sfałszowane informacje, natomiast elementy wspólne z prawem do prywatności wystąpią dopiero wówczas, gdy zauważalne będzie wtargnięcie się w sferę osobistą i integralność podmiotu. Twierdzenie to należy uznać za słuszne, bowiem nie zawsze naruszenie tych wartości będzie

[245] P. Sarnecki, *Komentarz do art. 47 Konstytucji…,* s. 4.
[246] 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. 19.
[247] Wyrok SN z dnia 9 października 2002 r., sygn. akt: IV CKN 1402/00, Legalis 59130.
[248] Wyrok SA w Białymstoku z dnia 13 września 2013 r., sygn. akt: I ACa 374/13, Legalis 743003.
[249] Wyrok SA w Rzeszowie z dnia 10 grudnia 2010 r., sygn. akt: I ACa 376/09, Legalis 526614.

wiązać się z wtargnięciem w prywatność, chronioną zresztą przez Konstytucję RP[250].

Należy wskazać, że w zakresie osób prawnych ujawnia się konieczność posługiwania się obiektywnym kryterium przy wyjaśnianiu istoty dobra osobistego i stopnia jego naruszenia. Dobra osobiste osób prawnych to wartości o charakterze niemajątkowym, dzięki którym osoba prawna ma możliwość funkcjonowania na podstawie zakresu swego działania[251]. Odnosząc się do osób prawnych, to przysługują im następujące dobra osobiste, tj. dobre imię, nazwa, tajemnica korespondencji i nietykalność pomieszczeń. W przywołanej powyżej sprawie zawisłej pod sygn. akt: V CK 314/05 chodzi jedynie o dobre imię osoby prawnej, a nie o cześć. Kwestionowane sformułowanie, że „wskutek braku gospodarności i należytego nadzoru ze spółdzielni wypływa rzeka pieniędzy" zawiera krytyczną ocenę działań organów osoby prawnej. Zarzuty kierowane wobec tych organów są zarzutami kierowanymi pod adresem samej osoby prawnej, godzącymi w dobre imię tej spółdzielni. Konkluzja ta jest tym bardziej uzasadniona, jeśli zważyć, że wypowiedź nie zawiera oskarżenia kierowanego do danego, wskazanego z imienia i nazwiska członka zarządu lub rady nadzorczej[252].

Poddanej w wątpliwość kwestii nie rozstrzyga do końca orzecznictwo Trybunału Konstytucyjnego. Wydając wyroki w sprawie zgodności aktów normatywnych z art. 47 Konstytucji RP wskazuje na jednostkę jako na adresata prawa do prywatności. Niemniej jednak, z orzeczeń TK wynika silne związanie czci i dobrego imienia, jak i prywatności z godnością człowieka[253]. Trybunał Konstytucyjny odmiennie niż poprzednio wskazał w nim, że pomówienie instytucji, osób prawnych i jednostek organizacyjnych niemających osobowości prawnej stanowi ingerencję w cześć osób fizycznych z nimi związanych. Według niego, pomówienie ww. organów o określone postępowanie lub właściwości odnosi się do działania, bądź zaniechania i cech konkretnych podmiotów. Byłoby niedorzeczne zabranianie pomawiania osób fizycznych, ale dopuszczenie robienia tego wobec instytucji, która stanowi ich miejsce zatrudnienia. Godzenie w dobra osobiste instytucji, osób prawnych i innych jednostek organizacyjnych jest bezwzględnie związane z pomówieniem osób fizycznych, choć ich dane osobowe nie muszą być wskazane wprost.

W judykaturze Sądu Najwyższego przyjęło się również, że „dobre imię stanowi dobro osobiste osoby prawnej, którego ochrony można dochodzić w oparciu o treść art. 23 k.c. Do kręgu dóbr osobistych osoby prawnej wchodzą dobra związane z jej identyfikacją, tj. nazwa

[250] Wyrok SA w Warszawie z dnia 30 listopada 2012 r., sygn. akt: VI ACa 728/12, Legalis 739296.
[251] Wyrok SN z dnia 14 listopada 1986 r., sygn. akt: II CR 295/86, OSNCP 1988, nr 2-3, poz. 40.
[252] Wyrok SN z dnia 10 listopada 2005 r., sygn. akt: V CK 314/05…
[253] Wyrok TK z dnia 30 października 2006 r., sygn. akt: P 10/06 (Dz. U. 2006 nr 202, poz. 1492).

lub firma, oraz dobre imię, tj. sława, reputacja, autorytet. Dobra osobiste osób prawnych to wartości niemajątkowe, dzięki którym osoba ta może funkcjonować zgodnie ze swoim zakresem działania"[254]. W tym kazusie, nieco inaczej ujmuje się pojęcia czci i dobrego imienia. Czyni się to w kontekście przyporządkowania tych cech osobom prawnym, a nie fizycznym. Podobne stanowisko zajął Europejski Trybunał Praw Człowieka. Uznał, iż skoro podmiotem ochrony z art. 8 EKPCz są osoby prawne, to ochrona ta dotyczy także ich siedziby[255]. Jakub Rzucidło zwraca jeszcze uwagę na art. 76 ww. Konwencji. W szczególny sposób nakłada na władze publiczne obowiązek, aby chroniły konsumentów, użytkowników i najemców przed działaniami, jakie naruszają ich prywatność[256]. W obowiązującym porządku prawnym znalazł wyraz pogląd, że przedmiotowa ochrona jest szczególną wartością konstytucyjną[257].

Stąd też biorąc powyższe pod uwagę, ujawniają się trzy podmioty, wpisujące się w zakres pojęcia „każdy" z art. 47 Konstytucji RP, którym prawodawca zagwarantował szerszy zakres ochrony. I o ile konsumentem może być jedynie osoba fizyczna, to tymi pozostałymi mogą być różne podmioty prawa. Choć Trybunał Konstytucyjny podkreślił, że wymienione pojęcia nie mogą być rozumiane jedynie tak, jak to zostało ujęte w prawie prywatnym, niemniej jednak nie wypracował innych w tym zakresie z punktu widzenia regulacji na gruncie Konstytucji RP[258].

Z praktycznego punktu widzenia, rzeczona wartość konstytucyjna należy do katalogu najbardziej zagrożonych dóbr. Prywatność nie jest doceniana ani przez obywateli, ani przez władze publiczne. Użytkownicy nowych technologii rezygnują z ochrony własnej prywatności na poczet uczestnictwa w postępującej cyfryzacji. Relacje interpersonalne wymagają notorycznego używania środków elektronicznych wykorzystywanych do przepływu informacji, a podmiot w sposób bardziej świadomy, bądź też nie, rezygnuje z przysługującego mu prawa do ujawniania informacji o swojej osobie, w tym władzom publicznym oraz podmiotom gospodarczym[259]. Ludzie coraz częściej wykorzystują prywatność, starając się tworzyć zbiory danych, bez jakich państwo dotychczas funkcjonowało, nie powodując tym samym zagrożenia przedmiotowej wartości

[254] Wyrok SN z dnia 17 lipca 2008 r., sygn. akt: II CSK 111/08, Legalis 133166.
[255] Wyrok ETPCz z dnia 16 kwietnia 2002 r. w sprawie *Set Colas Est and Others vs. Francja,* sygn. akt: 37971/97, § 4; L. Garlicki, *Komentarz do art. 8 EKPCz,* [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, tom I, Komentarz do artykułów 1-18,* Warszawa 2010, s. 538-539.
[256] J. Rzucidło, *Prawo do prywatności i ochrona danych osobowych…,* s. 161.
[257] Wyrok TK z dnia 26 września 2000 r., sygn. akt: P 11/99, OTK 2000, nr 6, poz. 187.
[258] Wyrok TK z dnia 13 września 2005 r., sygn. akt: K 38/04 (Dz. U. 2005 nr 186, poz. 1567).
[259] R. Piotrowski, *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne,* [w:] *Prywatność a jawność-bilans 25-lecia i perspektywy na przyszłość,* red. A. Mednis, Warszawa 2016, s. 25.

konstytucyjnej. Zbieranie danych o jednostce może spowodować powstawanie profili informacyjnych poszczególnych podmiotów, niekoniecznie wiążąc się z ich wolą i wiedzą. Nowe technologie wykorzystywane są w znacznym stopniu, a wdrażana informatyzacja za swój cel obiera gromadzenie danych, bez względu na rzeczywiste potrzeby praktyczne – tak też kształtuje się reżim informacyjny, gdzie zdolny do uzyskiwania informacji podmiot władzy wykonawczej będzie mógł posiadać wiedzę na temat wszystkich[260].

1.2.5. Konstytucyjne ograniczenia prawa do prywatności

Prawo do prywatności nie jest wolnością o charakterze absolutnym[261] – również wobec innych osób, poza publicznymi, z uwagi na potrzeby życia w zbiorowości. Konieczne jest jednak formułowanie ograniczeń w oparciu o wymagania konstytucyjne[262]. Można to uznać za swoistego rodzaju paradoks. Prawo do prywatności związane jest z wolnością jednostki, a człowiek w pełni wolny to taki, który będzie realizował swoje zamiary, zaś inni ludzie powinni je akceptować, nawet jeśli nie będą się z nimi zgadzać[263]. Dlatego nie można przyjąć w żaden sposób, że istnieje prawo do wolności absolutnej, ponieważ zawsze zostanie w większy lub mniejszy sposób ograniczona. Ograniczenia należy jednak pojmować bardziej jako wyjątek, aniżeli zasadę, ponieważ nie powinny one naruszać podstawowych wolności i praw.

Wprowadzanie ograniczeń praw i wolności konstytucyjnych ma o tyle większe znaczenie, ponieważ ustawa zasadnicza jest aktem najwyższego rzędu. Prawnomiędzynarodowa limitacja ingerencji w prawa podstawowe nie ma zastosowania do krajowych przepisów konstytucyjnych. Konstytucja jest najwyższym prawem Rzeczypospolitej Polskiej wobec wszystkich wiążących umów międzynarodowych, nie wyłączając przy tym prawa unijnego. W rezultacie korzysta ona z pierwszeństwa obowiązywania i stosowania na naszym terytorium[264].

Rozpatrując sposobność ograniczenia prawa do prywatności należy mieć na uwadze

---

[260] R. Piotrowski, *Prawo do tożsamości informacyjnej…,* s. 490.
[261] A. Szymanowska, M. Wierzbowski, *Granice ochrony danych osobowych,* [w:] *Prawne uwarunkowania wymiany informacji-nowe wyzwania,* red. K. Markowski, M. Wierzbowski, Warszawa 2009, s. 81.
[262] Wyrok TK z dnia 19 czerwca 1992 r., sygn. akt: U 6/92, OTK 1992, nr 1, poz. 13.
[263] A. Klich, *Boimy się wolności, marzymy o wspólnocie,* [dostęp: 18.01.2013] https://wyborcza.pl/magazyn/7,124059,13259382,boimy-sie-wolnosci-marzymy-o-wspolnocie.html?disableRedirects=true.
[264] Wyrok TK z dnia 11 maja 2005 r., sygn. akt: K 18/04…

zakaz naruszania istoty tego uprawnienia[265]. Absolut ten opiera się na założeniu, iż w granicach każdego prawa lub wolności (konstytucyjnie zagwarantowanych), można wyróżnić taką część, gdzie poprzez jej naruszenie nastąpi zakłócenie ich tożsamości[266]. W myśl przyjętej przez Trybunał Konstytucyjny linii orzeczniczej, dobra konstytucyjne mogą zostać ograniczone tylko „dla realizacji innej normy konstytucyjnej, poddającej pod ochronę dobro, które w danym przypadku posiada pierwszeństwo przed prywatnością. Ograniczenia są dopuszczalne, jeżeli umożliwiają ochronę bezpieczeństwa państwa, porządku publicznego, zdrowia, moralności publicznej, środowiska albo wolności lub praw innych osób. Muszą one być zgodne z zasadą proporcjonalności. Ustanowione ograniczenia spełniają ten ostatni wymóg, jeżeli wprowadzona regulacja ustawodawcza jest w stanie doprowadzić do zamierzonych przez nią skutków, tj. zasada przydatności i niezbędna dla ochrony interesu publicznego, z którym jest powiązana, tj. zasada konieczności, a ponadto jej efekty pozostają w proporcji do ciężarów nakładanych przez nią na obywatela, tj. zasada proporcjonalności *sensu stricto"*[267]. Ingerencja w życie prywatne może być jednak potrzebna w celu usunięcia zagrożeń wymierzonych w istotę demokratycznego państwa prawnego[268].

Prawo do prywatności podlega ograniczeniom wynikającym z treści przepisu art. 31 ust. 1 ustawy zasadniczej[269]. Ma ono swoje szczególne znaczenie, ponieważ oprócz tego, ograniczenia wolności i praw mogą być wprowadzane na podstawie art. 233 Konstytucji RP w kontekście stanów nadzwyczajnych. W odniesieniu do prawa do prywatności, zgodnie z art. 233 ust. 1 Konstytucji RP prawo to jest nienaruszalne, nawet w aktach ograniczających inne prawa w stanie wojennym i wyjątkowym, czy na podstawie przepisów szczególnych, które towarzyszą regulacji konkretnego prawa lub wolności. W ocenie Trybunału Konstytucyjnego oznacza to, że „nawet warunki tak wyjątkowe i ekstremalne nie zezwalają ustawodawcy na złagodzenie przesłanek, przy których spełnieniu można wkroczyć w sferę życia prywatnego, nie narażając się na zarzut niekonstytucyjnej arbitralności"[270]. Niniejsze doprowadziło do konkluzji, że wolność w postaci prawa do prywatności może być ograniczona w drodze ustawowej, zwłaszcza w realiach procesu karnego, który najgłębiej wnika w konstytucyjne wolności i prawa obywatelskie[271]. Prawo do prywatności leży u podnóża „kategorii praw

[265] D. Fleszer, *Godność i prywatność osoby w świetle Konstytucji Rzeczypospolitej Polskiej,* „Roczniki Administracji i Prawa" 2015, nr 15, s. 27.
[266] L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu,* Warszawa 2011, s. 103.
[267] Wyrok TK z dnia 20 czerwca 2005 r., sygn. akt: K 4/04…
[268] Wyrok TK z dnia 13 lutego 2001 r., sygn. akt: K 19/99, OTK 2001, nr 2, poz. 30.
[269] S. Jarosz-Żukowska, *Charakter i znaczenie wolności i praw jednostki wyrażonych w Rozdziale I Konstytucji RP,* [w:] *Prawa człowieka i system ich ochrony. Zarys wykładu,* Warszawa 2010, s. 135-138.
[270] Wyrok TK z dnia 20 czerwca 2005 r., sygn. akt: K 4/04…
[271] Wyrok TK z dnia 5 marca 2013 r., sygn. akt: U 2/11…

niederogowanych, tzn. takich, które w żadnym wypadku nie podlegają ograniczeniom w stanie wojennym i w stanie wyjątkowym"[272]. W ocenie Trybunału Konstytucyjnego zagwarantowana w ustawie zasadniczej ochrona życia prywatnego odnosi się również do ochrony danych osobowych, nazywanej autonomią informacyjną[273]. Koncepcja autonomii informacyjnej jest uogólnieniem prawa do prywatności. Obejmuje dane o charakterze *stricte* personalnym, jak i te, które odnoszą się do sfery ekonomicznej podmiotu – w tym sensie Trybunał Konstytucyjny dopuszcza jednak mniej restrykcyjne kryteria ograniczeń prawa do ochrony danych osobowych[274].

W ograniczenia prawa do prywatności wpisuje się również jego poszanowanie w kontekście osób pełniących funkcje publiczne, czy nawet szerzej rozumując – ubiegających się o ich pełnienie. Przejaw zainteresowania osób trzecich życiem prywatnym takich podmiotów jest poniekąd w pełni uzasadnione i normalne[275]. Zatem, osoba pełniąca funkcję publiczną jest niewątpliwie ograniczona w swym prawie do prywatności. Należy mieć na uwadze, że Konstytucja RP gwarantuje na mocy art. 61 ust. 1 Konstytucji RP prawo do ubiegania się o informacje o osobach pełniących funkcje publiczne i o działalności organów władzy publicznej, a każdy organ to *de facto* człowiek lub grupa osób, stąd też ich działalność nie podlega ochronie w takim zakresie jak działalność zawodowa pozostałych podmiotów. Zaś przepisy ustawy o dostępie do informacji publicznej[276] zobowiązują wręcz taki podmiot do udostępnienia określonych informacji, bez względu na to, czy ktokolwiek przejawia swoje zainteresowanie nimi[277]. *A contrario,* inne informacje udostępniane są na wniosek zainteresowanego. Prywatność osoby publicznej charakteryzuje się słabszą ochroną z uwagi na zakres przedmiotowy prawa do informacji, z którego nie są wyłączone te odnoszące się do pełnienia funkcji publicznych[278].

W ocenie Jana Bocia, wyłączenie spod ochrony art. 47 ustawy zasadniczej ma postać dwóch grup uwarunkowań. Chodzi o wyeliminowanie charakteru absolutnego ochrony z powodów publicznie ważnych, pomimo że w obowiązującym porządku prawnym nie są one skatalogowane. Z teoretycznego punktu widzenia odnosi się to do relacji pomiędzy interesem publicznym a prywatnym. Interes publiczny można zdefiniować jako obejmujący grupę niezindywidualizowanych odbiorców traktowanych jako wspólny podmiot. Ponadto, chodzi

[272] Wyrok TK z dnia 29 września 2008 r., sygn. akt: SK 52/05 (Dz. U. 2008 nr 178, poz. 1103).
[273] Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01…
[274] Wyrok TK z dnia 20 listopada 2002 r., sygn. akt: K 41/02, OTK-A 2002, nr 6, poz. 83.
[275] Wyrok TK z dnia 21 października 1998 r., sygn. akt: K 24/98…
[276] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2018, poz. 1669).
[277] Szerzej o upowszechnianiu wszelkich informacji bez wniosku zob. M. Bernaczyk, *Obowiązek bezwnioskowego udostępniania informacji publicznej,* Warszawa 2008, s. 26.
[278] Wyrok TK z dnia 11 maja 2007 r., sygn. akt: K 2/07 (Dz. U. 2007 nr 85, poz. 571).

o przyczyny wprowadzania takich stanów nadzwyczajnych, jakich skutkiem będzie ograniczenie również sfery życia prywatnego[279]. Co istotne, granice wkraczania w konstytucyjne prawa i wolności wyznacza zasada proporcjonalności. Posłużenie się stwierdzeniem, iż ograniczenia mogą być ustanawiane w demokratycznym państwie prawnym, rodzi konieczność poddaniu refleksji, czy regulacja ta jest niezbędna do ochrony interesu publicznego oraz czy owoce zastosowanej regulacji są wprost proporcjonalne do ciężarów ponoszonych przez nią na obywatela[280]. Zatem ograniczenie prawa lub wolności może nastąpić z uwagi na inną normę lub wartość konstytucyjną, a poziom tego ograniczenia powinien pozostać w prawidłowej proporcji do rangi interesu, jakiemu ograniczenie ma odpowiadać[281]. Niewykluczone, iż prywatność jednostki będzie przedmiotem ograniczeń koniecznych w demokratycznym państwie prawa. Oznacza to takie ukształtowanie systemu poprzez wykorzystanie poglądów większości parlamentarnej, która z kolei podlega ocenie większości składu orzekającego Trybunału Konstytucyjnego. Co ciekawe, Trybunał Konstytucyjny w jednym ze swych wyroków podkreślił, że prywatność „nie jest wartością konstytucyjną dorównującą w hierarchii prawu do traktowania humanitarnego, a więc w szczególności do wolności od tortur, które ma charakter absolutny i nie może być w żadnych warunkach ograniczone, a więc nie może podlegać ograniczeniom z uwagi na sprecyzowane przesłanki unormowane w art. 31 ust. 3 ustawy zasadniczej”[282]. Regulacje prawne traktujące o kompetencjach organów państwowych do wkraczania w sferę praw i wolności obywatelskich winny być dokonywane z uwzględnieniem wykładni zawężającej[283]. Zdanie odrębne w tej materii zgłosił sędzia Trybunału Konstytucyjnego Z. Czeszejko-Sochacki wskazując, aby wybór ten nie był swobodny, lecz nadzorowany za pomocą konstytucyjnie określonych środków ochrony praw i wolności[284].

Ograniczenie prawa do prywatności, w tym przede wszystkim ze względu na bezpieczeństwo państwa oraz porządek publiczny, może stać się problematyczne dla bezpieczeństwa demokratycznego państwa prawnego w tym sensie, że władzy wykonawczej i podporządkowanych jej podmiotom inicjującym czynności operacyjno-rozpoznawcze pozostają do dyspozycji środki, których zastosowanie daje możliwość stworzenia sytuacji,

[279] J. Boć, *Prawo do prywatności i jego ochrona w prawie konstytucyjnym,* [w:] *Przetwarzanie i ochrona danych osobowych,* red. G. Szpor, Katowice 1998, s. 1.4.-1.5.
[280] Wyrok TK z dnia 29 czerwca 2001 r., sygn. akt: K 23/00, OTK-ZU 2001, nr 5, poz. 124.
[281] A. Sakowicz, *Prawnokarne gwarancje prywatności,* Kraków 2006, s. 102.
[282] Wyrok TK z dnia 17 lipca 2008 r., sygn. akt: SK 25/07, OTK-A 2008, nr 6, poz. 119.
[283] Uchwała TK z dnia 16 stycznia 1996 r., sygn. akt: W 12/94, OTK 1996, nr 1, poz. 4.
[284] Wyrok TK z dnia 24 czerwca 1997 r., sygn. akt: K 21/96…

gdzie dojdzie do destrukcji instytucji demokratycznych i eliminacji praw obywatelskich[285]. Zagrożenie dla zasady demokratycznego państwa prawnego może mieć swój początek w zbytnio uzewnętrznianych względach ideologicznych czy politycznych w działalności egzekutywy. W ocenie Trybunału Konstytucyjnego, pomimo że środki ochrony bezpieczeństwa przejawiające się w legalnie dopuszczalnej działalności operacyjnej powodują zagrożenie dla wolności, to niemniej jednak bezpieczeństwo publiczne jako dobro przyznające ustawodawcy kompetencje do kreowania ograniczeń w korzystaniu z wolności obywatelskich wymaga zachowania zasady proporcjonalności wkroczenia w imię ochrony bezpieczeństwa, a także należytego systemu kontroli ocalenia tej zasady w praktyce[286].

Warte uwagi jest także inne ograniczenie przedmiotowego prawa, a mające swój wyraz w art. 45 Konstytucji RP. Na jego mocy zagwarantowane jest prawo do sądu, w tym jawne rozpatrzenie sprawy. Sąd Najwyższy podniósł, iż „w demokratycznym państwie prawa zasadą jest, że jednostka winna być chroniona, a sądy mają w tym zakresie szczególną rolę, przed wszelkimi nieuzasadnionymi ograniczeniami wolności ustanawianymi przez władze publiczne. Wolności obywatelskie są zatem elementem wspólnego, demokratycznego i legalistycznego porządku, przeto mogą być również z uwagi na wspólne dobro i interesy w rozsądny i odpowiadający prawu sposób ograniczone, przy uwzględnieniu służącego każdemu obywatelowi prawa do prywatności chroniącego indywidualną sferę jego osobistego życia”[287].

Charakterystyczną cechą prawa do sądu jest jawność, która może mieć charakter wewnętrzny. Wtedy oznaczać będzie dostęp stron do udziału w czynnościach procesowych, w tym możliwość zaznajomienia się z aktami sądowymi. Może przybrać też charakter zewnętrzny, tj. prawo wstępu publiczności na rozprawę[288]. Inną kwestią pozostaje ocena zabiegu tego rodzaju sytuacji, bowiem tak naprawdę osoba kierująca sprawę na drogę postępowania sądowego, musi liczyć się z tym, że z częścią jej prywatności, z którą związany jest spór, zapozna się nieograniczony krąg osób. Źródłem pojmowanej w ten sposób prywatności jest Konstytucja RP, która proklamuje też prawo do decydowania o swoich prawach osobistych. Wówczas zaś można wnioskować, że skoro podmiotowi przysługuje takie prawo, to i przysługuje mu również władztwo nad dotyczącymi go informacjami. Chodzi o szczególny rodzaj informacji. Nie wystarczy udzielenie samej zgody na ich rozpowszechnienie. Takie informacje objęte są specyficzną ochroną, bowiem zazwyczaj nie

[285] Wyrok TK z dnia 12 grudnia 2005 r., sygn. akt: K 32/04…
[286] *Tamże*.
[287] Wyrok SN z dnia 8 kwietnia 1994 r., sygn. akt: III ARN 18/94, OSNP 1994, nr 4, poz. 550.
[288] B. Banaszak, *Prawo konstytucyjne,* Warszawa 2008, s. 102.

są normalnie chronione przed dostępem innych osób[289].

Wyjątki od tej zasady mogą wystąpić z uwagi na taksatywnie wyliczony katalog wartości materialnych wskazanych w art. 31 ust. 3 Konstytucji RP, tj. moralność, bezpieczeństwo państwa, porządek publiczny, ochronę życia prywatnego stron lub inny ważny interes prywatny. Niemniej jednak, musi to nastąpić w formalnej drodze ustawy[290]. Konstytucja RP posłużyła się zasadą, zgodnie z którą ustalenie granic praw i wolności ciąży na prawodawcy[291]. Niniejsze w swoim orzeczeniu podkreślił Trybunał Konstytucyjny, zwracając tym samym uwagę na to, że ograniczenia te nie mogą naruszać istoty wolności i praw[292]. Przez to sformułowanie można rozumieć m.in. uprawnienie do zachowania tożsamości informacyjnej, a zatem prawo do zebrania wszystkich informacji dotyczących danej osoby, sprawowania nad nimi pieczy i zarządzania nimi w granicach określonych w Konstytucji RP. Zebranie wszystkich danych o jednostce bez jej woli i wiedzy oznacza odebranie jej dobra w postaci prawa do prywatności. Powoduje utratę przez nią prawa do autonomii informacyjnej, co można uznać za tożsame z naruszeniem istoty prawa do prywatności i ochrony danych osobowych[293]. Za zgodne ze standardem ograniczania praw i wolności można przyjąć te, które są proporcjonalne i niearbitralne, a zatem wprowadzane ustawą, poddane kontroli sądowej i oparte na przesłankach wyrażonych w Konstytucji RP, co więcej – respektujące istotę prawa do prywatności, a tym samym zasadę godności.

1.3. Regulacja konstytucyjna prawa do informacji

1.3.1. Prawo do autonomii informacyjnej na gruncie przepisów Konstytucji RP

Generalnie zasadę autonomii informacyjnej po raz pierwszy rozwinięto w Niemczech. Orzeczenie Federalnego Sądu Konstytucyjnego z dnia 15 grudnia 1983 roku dotyczyło kontrowersyjnych przepisów ustawy z dnia 25 marca 1982 r. o powszechnym spisie ludności, przewidujących gromadzenie w okresie spisu szczegółowych informacji o obywatelach, tj. imię, nazwisko, adres, przynależność wyznaniową, wykształcenie, wykonywaną profesję oraz sytuację mieszkaniową. Analizując zakwestionowane przepisy, Federalny Sąd Konstytucyjny

[289] H. Szewczyk, *Ochrona dóbr osobistych…,* s. 124.
[290] Wyrok TK z dnia 23 lutego 2010 r., sygn. akt: K 1/08, OTK-A 2010, nr 2, poz. 14.
[291] B. Banaszak, *Prawo konstytucyjne,* Warszawa 2010, s. 471.
[292] Wyrok TK z dnia 29 czerwca 2001 r., sygn. akt: K 23/00…
[293] R. Piotrowski, *Prawo do tożsamości informacyjnej...,* s. 480.

wywiódł z ogólnego prawa osobowości wynikającego z ustawy zasadniczej RFN[294] przysługujące jednostce prawo do samookreślenia informacyjnego. Federalny Trybunał Konstytucyjny wyraził stanowisko, że w warunkach zmodernizowanego przetwarzania danych, Konstytucja RFN obejmuje ochroną jednostkę przed nieograniczonym gromadzeniem, przechowywaniem, wykorzystywaniem i przekazywaniem dotyczących jej danych osobowych. Służyło to zapewnieniu jednostce swobodnego rozwoju własnej osobowości. Ponadto w Konstytucji RFN zagwarantowano prawo do samodzielnego ujawniania i używania danych osobowych. Ochrona sfery prywatności, a także zagwarantowanie jednostce wiedzy o tym, które informacje na jej temat są dostępne w środowisku, stanowią niezbędne elementy korzystania z przysługujących jednostce praw oraz całkowitego uczestnictwa w życiu społecznym i politycznym[295].

Ochrona danych osobowych w Polsce, zawierająca się w autonomii informacyjnej, posiada krótką historię. Została uregulowana w art. 51 Konstytucji RP. Na prawo do ochrony danych osobowych składają się fundamentalne zasady, tj. wolność jednostki do ujawnienia informacji związanych z jej osobą (kontrola danych znajdujących się w posiadaniu innych osób jest związana z uprawnieniem do decydowania o tym, czy i komu podmiot wyjawi określone informacje), uprawnienie władzy publicznej w zakresie pozyskiwania, gromadzenia i udostępniania informacji o obywatelach, prawo dostępu do dokumentów urzędowych oraz zbiorów danych, a tym samym prawo żądania sprostowania bądź usunięcia informacji tam zawartych[296]. Nie prowadzi to jednak do wniosku, iż wcześniej nie istniała ochrona danych osobowych.

W przypadku polskiej ustawy zasadniczej, przez autonomię określa się samodzielne stanowienie o swoich sprawach oraz niezależne od innych podejmowanie decyzji. Aksjologicznych podstaw autonomii informacyjnej powinno upatrywać się na gruncie wolności jednostki[297] i traktować jako urzeczywistnienie prawa do ochrony życia prywatnego w obszarze obejmującym rozporządzanie informacjami o sobie samym. Oddaje to „złożony, hybrydowy charakter tej koncepcji, łączącej elementy o charakterze wolnościowym z konkretnymi uprawnieniami o funkcji ochronnej"[298]. Jednostka, korzystając z przysługującej jej wolności, może swobodnie dysponować wiadomościami o sobie,

[294] Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, Bundesgesetzblatt nr I, s. 1.
[295] G. Hornung, Ch. Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination,* "Computer Law&Security Report" 2009, nr 1, s. 85-86.
[296] J. Braciak, *Prawo do prywatności…,* s. 157-160.
[297] D. Błoński, M. Florczak-Wątor, *Problem horyzontalnej skuteczności prawa do ochrony danych osobowych w świetle przepisów konstytucyjnych Polski i Szwajcarii,* „Przegląd Sejmowy" 2015, nr 1 (126), s. 95.
[298] K. Grzybowski, *Autonomia informacyjna jednostki a zgoda na przetwarzanie przez pracodawcę danych osobowych,* „Przegląd Sejmowy" 2020, nr 6 (161), s. 52.

a państwo z kolei powinno powstrzymywać się od nieuzasadnionego wkraczania w tę sferę aktywności ludzkiej.

W dobie społeczeństwa informacyjnego, aspekt wolnościowy autonomii informacyjnej nabiera takiego znaczenia, że czasem aż bywa utożsamiany z samą esencją tejże koncepcji. W jednym ze swoich orzeczeń, Trybunał Konstytucyjny przyjął, iż „istota autonomii informacyjnej każdego człowieka sprowadza się do pozostawienia każdej osobie swobody w określeniu sfery dostępności dla innych wiedzy o sobie”[299].

Autonomia informacyjna posiada także nie mniej ważny walor ochronny, scharakteryzowany w konkretnych uprawnieniach, które prawodawca winien zagwarantować jednostce, ustanawiając przy tym należyte środki prawne ich przymusowego egzekwowania. Konstytucyjna ochrona autonomii informacyjnej wymaga od państwa aktywności w celu zapewnienia skutecznych narzędzi pozwalających na zidentyfikowanie, jakie informacje o jednostce znajdują się w posiadaniu innych podmiotów oraz umożliwiają sprawowanie umotywowanej kontroli nad tymi informacjami. Przy analizowaniu aspektu wolnościowego autonomii informacyjnej co do zasady zwraca się uwagę na możliwość odmowy udzielenia poszczególnych informacji o sobie, definiując ten wymiar autonomii informacyjnej mianem wolności od ujawniania informacji[300]. Założenie autonomii informacyjnej wyraża jednak zdecydowanie bogatszą treść. Posiadanie informacji nie polega jedynie na zachowaniu ich w tajemnicy, lecz również na dzieleniu się nimi. Autonomia informacyjna w kontekście wolnościowym wyraża się zarówno poprzez wolność od ujawniania informacji – możliwość zachowania tajemnicy, jak też wolność ujawniania informacji – możliwość ich przekazania.

Koncepcja autonomii informacyjnej jednostki ugruntowała się w dorobku orzeczniczym polskiego sądu konstytucyjnego. Jedno z głównych założeń zostało już scharakteryzowane w wyroku Trybunału Konstytucyjnego w dniu 24 czerwca 1997 r. (sygn. akt: K 21/96). Podkreślało ono rangę prawa do prywatności, regulowanego na podstawie przepisów obowiązujących przed dniem wejścia w życie Konstytucji RP z dnia 2 kwietnia 1997 r. Trybunał Konstytucyjny wyjaśnił wówczas, iż „prywatność odnosi się też do ochrony informacji dotyczących danej osoby i gwarantuje m.in. pewien stan niezależności, w ramach którego jednostka może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu”. Wolność podmiotu od ujawniania informacji związanych z jego osobą jest definiowana przez doktrynę jako prawo bądź zasada samodzielnego podejmowania przez każdego decyzji o ujawnieniu dotyczących go

[299] Wyrok TK z dnia 12 listopada 2002 r., sygn. akt: SK 40/01, OTK-A 2002, nr 6, poz. 81.
[300] Wyrok TK z dnia 14 lipca 2015 r., sygn. akt: K 2/13, OTK-A 2015, nr 7, poz. 100.

informacji. Prawo to związane jest z wszelkim rodzajem informacji. Zaś zobowiązanie danej osoby do ujawnienia informacji na jej temat ma charakter wyjątkowy, znajdujący swoją podstawę w ustawie[301]. Przez informację należy rozumieć dane, które można przetwarzać. Przybierają one charakter liter, cyfr, impulsów elektrycznych[302]. Co istotne, terminologia danych różni się od informacji. Dane są elementami łatwymi do przesyłania, interpretacji czy przetwarzania metodami ręcznymi albo automatycznymi. Są przechowywanymi w bazie wartościami. Z kolei informacja to dane przetworzone pod taką postacią, ażeby zaprezentować znaczenie tych danych[303].

Jednak zasadnicze założenia autonomii informacyjnej, które utrwaliły się we współczesnym porządku konstytucyjnym zostały przedstawione nieco później w wyroku z dnia 19 lutego 2002 r. w sprawie zawisłej pod sygn. akt: U 3/01[304]. W treści uzasadnienia tego orzeczenia TK zidentyfikował uprawnienia podmiotu wyznaczających jego autonomię w sferze informacyjnej. Uprawnienia te sprowadzają się do prawa do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, które znajdują się w posiadaniu innych jednostek. Jednocześnie Trybunał Konstytucyjny określił miejsce autonomii informacyjnej w sferze konstytucyjnych gwarancji ochrony prywatności, podkreślając, że stanowi ona istotny element składowy prawa do ochrony życia prywatnego wyrażonego w art. 47 ustawy zasadniczej, niemniej jej podstaw i gwarancji trzeba doszukiwać się przede wszystkim w przepisach art. 51 Konstytucji RP. Tak ukształtowana koncepcja znalazła potwierdzenie w wielu kolejnych wyrokach wydawanych przez Trybunał Konstytucyjny dotyczących przetwarzania danych osobowych przez podmioty publiczne[305]. Prawo do ochrony danych osobowych jest szczególnym instrumentem prowadzącym do ochrony życia prywatnego. Oznacza to, że chroni te same wartości, które objęte są zakresem ochrony prawa do prywatności. Prywatność zapewnia pewien stan niezależności, gdzie dany podmiot może podejmować decyzje o zakresie i zasięgu ujawniania innym osobom informacji o swoim życiu[306]. W ocenie Trybunału Konstytucyjnego nie jest prawidłowe twierdzenie, że pomiędzy wspomnianymi prawami zachodzi stosunek krzyżowania się. Jednakże są one od siebie zależne, co zresztą widać na pierwszy rzut oka. Takie stanowisko nie prowadzi do polepszenia

[301] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz,* Warszawa 2007, s. 115.
[302] T. Burczyński, *Elektroniczna wymiana informacji w administracji publicznej,* Wrocław 2011, s. 30.
[303] B. Stefanowicz, *Informacja,* Warszawa 2004, s. 14.
[304] Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01…
[305] Wyrok TK z dnia 19 czerwca 2018 r., sygn. akt: SK 19/17, OTK-A 2018/42; Wyrok TK z dnia 20 stycznia 2015 r., sygn. akt: K 39/12, OTK-A 2015, nr 1, poz. 2.
[306] Wyrok TK z dnia 12 listopada 2002 r., sygn. akt: SK 40/01…

roli ochrony danych osobowych, bowiem są one odrębną instytucją od prawa do prywatności. Z drugiej zaś strony, prawo do prywatności nie jest jedynie utożsamiane z ochroną danych osobowych z uwagi na szerszy zakres swojego pojęcia[307].

Regulacja wyrażona w art. 51 Konstytucji RP wiąże się z ujawnieniem wszelkich informacji, będących odzwierciedleniem zarówno osobistego, jak i publicznego postępowania jednostki. Jej przejawem jest wolność od ujawniania organom władzy publicznej swojego światopoglądu, przekonań religijnych, czy wyznania[308]. Wszystko to składa się na element ochrony danych osobowych. Władza publiczna nie może dysponować informacjami o obywatelach, innymi niż te, które są niezbędne w demokratycznym państwie prawa. Za takie informacje należy uznać te, które są konieczne w granicach kompetencji władz i przyświecają realizacji ich zadań. Zatem informacje mają być zebrane nie z uwagi na obywateli, a ze względu na funkcje i zadania wykonywane przez organy władzy publicznej. Za informacje niezbędne uznano dane umożliwiające funkcjonowanie jednostki w społeczeństwie, a których ujawnienie nie jest postrzegane jako naruszenie sfery prywatności. Doprecyzowując, są to takie dane, bez jakich istnienie państwa byłoby nader utrudnione. Niemniej jednak, nie mogą one przesądzać o przewadze informacyjnej nad obywatelem[309]. Sformułowanie informacji niezbędnych należy interpretować nieostro. Gwarancje określone w ust. 2 przywołanego wyżej przepisu są niejako skonkretyzowaniem prawa do prywatności, analogicznie do ochrony danych osobowych. Niniejsze potwierdza szczególne znaczenie prawa do prywatności, a oprócz tego ukazuje od niego zależność ochrony danych osobowych. Będąca przedmiotem analizy wolność jednostki, oznacza również zakaz podejmowania przez określone w aktach rangi ustawowej podmioty, jakichkolwiek prób zmierzających do pozyskania tego rodzaju informacji poprzez rozpytanie. Obowiązek informacyjny może być nałożony w sposób bezpośredni lub pośredni, uszczegółowiony w aktach normatywnych niższego rzędu. Nie może być jednak oparty wprost wyłącznie na nich[310]. Zadaniem Trybunału Konstytucyjnego jest orzekanie w sprawach zgodności ustaw z Konstytucją RP, a tym samym ustaw regulujących m.in. zasady ochrony danych osobowych. Celem ustawodawcy, jaki mu przyświecał było stworzenie gwarancji jednostce prawa do prywatności i ochrony danych osobowych.

---

[307] M. Jabłoński, K. Wygoda, *Dostęp do informacji…,* s. 240.
[308] P. Sarnecki, *Konstytucja Rzeczypospolitej Polskiej. Komentarz do Art. 51,* III, red. L. Garlicki, Warszawa 2003, s. 1-2.
[309] I. Lipowicz, *Konstytucyjne podstawy ochrony danych osobowych,* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia,* red. P. Fajgielski, Lublin 2008, s. 49.
[310] I. Lipowicz, *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku,* red. J. Boć, Wrocław 1998, s. 99.

W ustępie 3. art. 51 Konstytucji RP, ustrojodawca ogólnikowo uregulował dostęp jednostki do dokumentów urzędowych, przez co należy rozumieć podejmowanie przez władze odpowiednich działań. Oprócz tego, zdawkowo odniósł się do zbiorów danych, które określono jako zbiór informacji, „uzyskanych przez dany czynnik władzy publicznej”[311]. Z przepisu tego wynika, że jednostka ma dostęp jedynie do dokumentów i zbiorów danych o charakterze urzędowym. Nie przysługują jej uprawnienia wglądu do tego rodzaju dokumentów, ale o charakterze prywatnym, nawet gdy pozyskują informacje o danej osobie.

Pojęcie dokumentu urzędowego oraz zbioru danych w Konstytucji RP nie zostało zdefiniowane. Zbiorem danych są wszystkie dostępne źródła informacji, które posiadane są przez władze publiczne. Ważnym elementem jest określenie dysponenta tegoż dokumentu. Należałoby zwrócić uwagę, że nie każdy dokument znajdujący się w posiadaniu władzy publicznej można przyporządkować do kategorii dokumentu urzędowego. Zbiór informacji będzie także zbiorem danych. Niemniej jednak, Trybunał Konstytucyjny podniósł, iż dokumenty urzędowe i zbiory danych różnią się od informacji[312]. Wskazane powyżej uprawnienie stanowi podstawę udostępnienia akt sprawy toczącej się przed organem administracji publicznej bądź przed sądem powszechnym. Postępowanie sądowe należy połączyć z art. 45 Konstytucji RP, gdzie zagwarantowane zostało prawo do sądu, z art. 77 i 79 Konstytucji RP[313].

Występujące w art. 51 ust. 1 i 3 zwroty „informacji dotyczących jego osoby” oraz „dotyczących go dokumentów i zbiorów danych” odnoszą się jedynie do osób fizycznych[314]. Znajduje to swoje uzasadnienie w tym, że prawo do ochrony danych osobowych jest ściśle związane z prawem do prywatności, które przysługuje jednostce, a nie innym podmiotom[315]. Jeżeli jednak przyjąć, iż w oparciu o treść art. 51 ust. 1 i 3 Konstytucji RP chronione są tylko dane osób fizycznych, to o tyle nie można wyeliminować tej ochrony na podstawie art. 47 Konstytucji RP co najmniej w takim zakresie, w jakim chroni dobre imię podmiotów prawa – innych niż osoby fizyczne[316]. Zaś w art. 51 ust. 4 omawianego przepisu krąg adresatów zdefiniowany jest jako „każdy”, ale nie przypisuje już każdemu takich cech, które bez jakiegokolwiek cienia wątpliwości pozwalałyby wykazać, że odnosi się on jedynie do osoby

[311] P. Sarnecki, *Konstytucja Rzeczypospolitej Polskiej…,* s. 5.
[312] Wyrok TK z dnia 26 października 2005 r., sygn. akt: K 31/04, OTK ZU 2005, nr 9, poz. 103.
[313] H. Knysiak-Molczyk, *Granice prawa do informacji w postępowaniu administracyjnym i sądowoadministracyjnym,* Warszawa 2013, s. 77.
[314] P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej…,* s. 69.
[315] A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy,* Warszawa 2008, s. 46.
[316] M. Jabłoński, *Zasada różnicowania zakresu realizacji konstytucyjnych wolności i praw jednostki w oparciu o kryterium obywatelstwa polskiego,* [w:] *Wolności i prawa jednostki w Konstytucji RP,* red. M. Jabłoński, tom I, Warszawa 2010, s. 529.

fizycznej. Można domniemywać, że skoro cała ta regulacja skierowana jest do osób fizycznych, to i ust. 4 także. Jednakże, na gruncie prawa do dobrego imienia można przyjąć, że jej adresatami oprócz osób fizycznych są także inne podmioty prawne[317]. W ustępie 4. art. 51 ustawy zasadniczej sformułowano prawo żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z aktem o randze ustawy. Adresatem tego prawa jest każdy podmiot twierdzący, że informacje go dotyczące są niepełne czy błędne. Co istotne, z omawianego przepisu wynika, że jednostka wyposażona jest w prawo do żądania, a nie prawo do samodzielnego sprostowania i usunięcia. Nie świadczy to jednak o osłabieniu omawianej gwarancji. Prawo to odnosi się do wszelkich informacji, którymi władze publiczne dysponują o jednostce. Obejmuje także te zebrane w związku z prowadzoną działalnością operacyjną (m.in. przez policję, CBA, CBŚ). Prawo to w dużej mierze podlega pewnym ograniczeniom. Rodzi obowiązek władz publicznych do rozpatrzenia i uwzględnienia żądania wyrażonego w ust. 4, niemniej jednak w granicach wyznaczonych przez art. 31 ust. 3 Konstytucji RP. W ustępie 5. określono zasady i tryb gromadzenia oraz udostępniania zebranych informacji.

Nieco inaczej przedstawia się sprawa ograniczeń prawa do ochrony danych osobowych. Podlegają tym samym regułom w oparciu o treść art. 31 ust. 3 Konstytucji RP – podobnie jak w przypadku prawa do prywatności. Niemniej jednak, nie można zapominać o regulacji art. 51 ust. 2 Konstytucji RP. Statuuje on bowiem o przysługującym władzy publicznej uprawnieniu do pozyskiwania, gromadzenia i udostępniania informacji o obywatelach. Terminologia tych sformułowań nie jest konkretyzowana ani w przepisach ustawy zasadniczej, ani w judykaturze Trybunału Konstytucyjnego. Ich interpretacja dokonywana jest w oparciu o słownikowe wyjaśnienie tych definicji. Zatem pozyskanie oznacza zdobycie czegoś, gromadzenie to składanie w jednym miejscu tego, co zostało zdobyte, natomiast udostępnianie to ułatwienie skorzystania z czegoś[318]. Konstytucja RP wprowadza ograniczenia dwojakiego rodzaju. Pierwsze ograniczenie odnosi się co do formy – obowiązek udostępnienia danych powinien być określony przez ustawę. Drugie ograniczenie zaś przybiera postać udostępnienia danych jedynie w sytuacji, kiedy jest to niezbędne w demokratycznym państwie prawa[319]. Kwestią problematyczną może być określenie informacji, które należy uznać za niezbędne. Można przyjąć, że będą to takie informacje, dzięki którym władze publiczne będą zdolne do sfinalizowania działań w granicach

[317] Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01…
[318] *Słownik Języka Polskiego PWN,* [dostęp: 20.06.2014] http://sjp.pwn.pl/slownik/2507328/pozyskać; http://sjp.pwn.pl/szukaj/gromadzić; http://sjp.pwn.pl/szukaj/udostępnić.
[319] Wyrok TK z dnia 20 listopada 2002 r., sygn. akt: K 41/02…

przyznanych im kompetencji. Trybunał Konstytucyjny nawiązał do wartości wymienionych w art. 31 ust. 3 ustawy zasadniczej i w ramach tego, podniósł, że „ocena zachowania przez ustawodawcę zwykłej zasady proporcjonalności w aspekcie możliwości pozyskiwania przez władze publiczne informacji o obywatelach może i powinna być przeprowadzana na podstawie współstosowanych przepisów art. 51 ust. 2 oraz art. 31 ust. 3 Konstytucji RP. Poza koniecznością wskazania interesu mieszczącego się w katalogu zawartym w art. 31 ust. 3 Konstytucji RP przesłanką legalności wkroczenia w zakres autonomii informacyjnej jednostki jest stwierdzenie, że wprowadzona regulacja ustawodawcza jest w stanie doprowadzić do zamierzonych przez nią skutków (zasada przydatności), jest niezbędna do ochrony interesu publicznego, z którym jest powiązana (zasada konieczności), a jej efekty pozostają w proporcji do ciężarów nakładanych przez nią na obywatela (zasada proporcjonalności *sensu stricte*)”[320].

Przewidziane są też przypadki, gdzie można skorzystać z instytucji ograniczenia autonomii informacyjnej jednostki na poziomie każdego z jej aspektów. W wymiarze wolnościowym daje się zaobserwować dwutorowy przebieg tego procesu. Stosowane ograniczenia są ukierunkowane na zobowiązanie jednostki do ujawnienia określonych informacji jej dotyczących – ingerencja w sposobność zachowania danych w tajemnicy lub na limitowanie wolności przekazywania innym uczestnikom obrotu takich informacji celem ich zgodnego z prawem wykorzystania w określony sposób – ingerencja w sposobność dzielenia się informacjami. W sferze ochronnej autonomii informacyjnej ograniczenia doprowadzają do ingerencji w uprawnienia umożliwiające jednostce sprawowanie kontroli nad występującymi w obrocie o niej informacjami. Ograniczone może też zostać prawo do informacyjnego samostanowienia. Wskazuje się tu na sytuację, w której przeważał interes ogółu, przy zachowaniu oczywiście zasady proporcjonalności. Trybunał zwrócił uwagę, że jednostka nie znajduje się w bezwzględnej dyspozycji swoim prawem[321]. Poglądy te w dużej mierze zostały przyjęte przez ustawodawcę na gruncie przepisów prawa polskiego.

Autonomia informacyjna ma wymiar personalny, jak i ekonomiczny[322]. Przedmiotem ochrony są informacje osobowe. Bez znaczenia jest, jakiego rodzaju są to informacje. Mogą to być zarówno te, które narażają podmiot na uczucie ośmieszenia, ale też wręcz przeciwnie – te, które niekoniecznie rozpatrywane są w kategoriach moralności. Trybunał Konstytucyjny podjął się próby określenia, co jest przedmiotem ochrony autonomii informacyjnej. W jednym

[320] Wyrok TK z dnia 17 czerwca 2008 r., sygn. akt: K 8/04, OTK-A 2008, nr 5, poz. 81; wyrok TK z dnia 21 listopada 1995 r., sygn. akt: K 12/95, OTK 1995, nr 1, poz. 15.
[321] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2013, s. 21.
[322] Wyrok TK z dnia 17 czerwca 2008 r., sygn. akt: K 8/04…

z jego orzeczeń można zauważyć, że „przedmiotem ochrony są bowiem na tle nowoczesnych ujęć prywatności wartości akcentujące możliwość prowadzenia swych spraw, decydowania o swym życiu i o rodzajach więzi personalnych z innymi z maksymalną swobodą, a zarazem z najmniejszym stopniem ingerencji świata zewnętrznego w tę sferę, która jest domeną własnej aktywności jednostki. Ów wspólny korzeń aksjologiczny prawa do życia prywatnego oraz do ochrony danych osobowych decyduje w dużym stopniu o potrzebie poszukiwania wspólnego uzasadnienia dla uznania za dopuszczalną ingerencji zewnętrznej w świat odosobnienia jednostki”[323].

Nauka prawa oraz judykatura rozpatrywała kwestie dotyczące ochrony jednostki z uwagi na dotyczące jej dane osobowe, ale przez pryzmat uprzednio wspomnianych przepisów prawa cywilnego – art. 23 i 24 k.c. Te klasyczne środki ochrony dóbr osobistych w dobie postępującej komputeryzacji okazały się bezskuteczne. Konstrukcja prawa do ochrony danych osobowych ze swej natury ma zapewniać uprawnienia o charakterze prewencyjnym, których celem będzie niedopuszczenie do powstawania zagrożeń[324]. W konstytucjach, w których nie zagwarantowano bezpośrednio prawa do ochrony danych osobowych, ich ochrona realizowana jest poprzez wykładnię norm odnoszących się do ochrony dóbr osobistych lub prywatności[325]. Nieuchronność zagwarantowania ochrony danych osobowych pojawiła się wraz z rozwojem technik informacyjnych. W ocenie M. Safjana, istniały dwie fundamentalne przyczyny, dla których tworzono mechanizmy ochrony danych. Pierwszą z nich była nieudolność tradycyjnego aparatu ochrony prywatności, który swoje zastosowanie znalazł w nauce prawa cywilnego i karnego. Za drugą przyczynę natomiast uznano potraktowanie środków publicznoprawnych za podstawowy budulec ochrony danych osobowych[326]. Uregulowanie ochrony danych osobowych w Konstytucji RP spowodowało podniesienie znaczenia tego zagadnienia, a to z uwagi na miejsce, jakie zajmuje ustawa zasadnicza w polskim systemie prawa[327]. Konstytucjonalizacja ochrony danych osobowych odgrywa ogromną rolę w kształtowaniu sytuacji prawnej jednostki. Taki też cel przyświecał ustrojodawcy, który pośród wolności i praw osobistych

[323] Wyrok TK z dnia 12 listopada 2002 r., sygn. akt: SK 40/01…
[324] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej,* „Państwo i Prawo” 1997, z. 6, s. 30.
[325] P. Sobczyk, *Ochrona danych osobowych jako element prawa do prywatności,* „Zeszyty Prawnicze” 2009, nr 1, s. 300.
[326] M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informacyjnym,* „Państwo i Prawo” 2002, nr 6, s. 7.
[327] G. Koksanowicz, *Ochrona danych osobowych w świetle Konstytucji oraz Ustawy o ochronie danych osobowych,* [w:] *Konstytucyjny ustrój państwa. Księga jubileuszowa Profesora Wiesława Skrzydły,* red. T. Bojarski, E. Gdulewicz, J. Szreniawski, Lublin 2000, s. 93.

sformułował prawo do prywatności i związane z nim prawo do ochrony danych osobowych. W zasięgu rozwijającej się informatyzacji życia społecznego i postępującej globalizacji, jakakolwiek aktywność podmiotu nie ma szansy zaistnieć bez ingerencji w strefę jej prywatności[328].

Aktualnie ciężar ochrony prywatności jednostki coraz bardziej przesuwa się w stronę środków publicznoprawnych. Ochrona jest realizowana nie tylko poprzez przepisy prawa prywatnego, ale dokonywana jest także w prawie publicznym. Na państwo nałożony jest obowiązek zorganizowania życia społecznego, aby została zapewniona efektywna realizacja wzajemnych relacji praw i wolności. Wynika to z konieczności równoważenia interesu jednostki (ochrony jej autonomii informacyjnej) z interesem publicznym, którego zabezpieczenie też może wymagać przetwarzania danych osobowych. Służą temu środki publicznoprawne (stosunki jednostka – państwo), jak i cywilnoprawne (relacja jednostka – jednostka). W literaturze przedmiotu przyjęło się, że prawo do ochrony danych osobowych ma dwa aspekty – prywatnoprawny i publicznoprawny[329]. Pierwszy charakteryzuje się osobistym stosunkiem, powstałym między osobą fizyczną a danymi do niej się odnoszącymi. W tym przypadku zatem dane osobowe podlegają ochronie, podobnie jak dobra osobiste. W szerokim znaczeniu, autonomia informacyjna zaliczana jest do kategorii dóbr osobistych i przy każdym restrykcyjnym założeniu należy przyjąć, iż chronione są dane osobowe. Zaś w wąskim znaczeniu, do naruszenia dobra osobistego dochodzi w wypadku, gdyby nieuprawnione wtargnięcie się doprowadziło do zakłócenia spokoju fizycznego osoby, będącej jednocześnie ofiarą naruszenia. Możliwa jest jeszcze inna wykładnia danych osobowych, tym razem nie rozumiana jako dobro osobiste, ale rozpatrywana w kategoriach własnościowych. Za przedmiot ochrony należy wówczas uznać dane osobowe, których właścicielem jest człowiek na podstawie faktu związania z tymi danymi. Inne stanowisko kształtuje się tak, że przedmiotem ochrony jest władztwo sprawowane nad danymi przez osobę, której dane dotyczą, nierzadko połączone z zasadą poufności. Analizując te koncepcje, należy raczej przyjąć model powszechnej ochrony dóbr osobistych i to w ujęciu *sensu stricte* – jest to prawo niemajątkowe, ściśle połączone z podmiotem. Prowadzi to do wniosku, że wyłączona jest możliwość zrzeczenia się tego uprawnienia, uczynienia go przedmiotem dziedziczenia. Niemajątkowy aspekt tego prawa nie uniemożliwia jednak czerpania korzyści

[328] M. Krasińska, S. Mizerek, *ABC wybranych zagadnień ustawy o ochronie danych osobowych,* Warszawa 2007, s. 6.

[329] Zauważalne jest zjawisko przybierania przez stosunki regulowane przez prawo cywilne charakteru publicznego. Występuje to chociażby w sferze pomiędzy przedsiębiorcami jako administratorami baz danych osobowych a konsumentami, których te dane dotyczą. Zob. M. Kępiński, *Ocena stanu przepisów prawa cywilnego ujętych w kodeksie cywilnym po roku 1997,* „Przegląd Legislacyjny" 2001, nr 3, s. 169.

majątkowych przez jego wykonywanie.

Konieczność prawnej regulacji zagadnienia ochrony danych osobowych nie powinna być przedmiotem dyskusji. Problematyczne jednak pozostają założenia, na których opierać się mają konkretne rozwiązania prawne. Zbliżają się one do modelu własnościowego, gdzie każdą osobę należy traktować jak właściciela danych jej dotyczących lub też zmierzają do traktowania tego zagadnienia przez pryzmat ochrony praw osobistych jednostki, jej prywatności oraz godności. Charakterystyczną cechą przepisów z zakresu ochrony danych osobowych jest to, że uważają one osobę, której dane dotyczą za słabszy podmiot różnych stosunków prawnych, przez co traktowana jest za taką, która wymaga podwyższonych standardów ochrony[330].

W obliczu tak szybko zmieniających się uwarunkowań technologicznych, ekonomicznych i społecznych problemem staje się automatyczne przetwarzanie danych. Obserwowane jest zjawisko nieprzewidywalności skali tego przetwarzania z punktu widzenia podmiotu danych. Do ważnych zagadnień współczesnej ochrony danych osobowych należą profilowanie osób, Internet przedmiotów, przetwarzanie danych w chmurze, przetwarzanie danych na portalach społecznościowych, przetwarzanie danych osobowych w związku z geolokalizacją lub też z wykorzystaniem metod Big Data, ochrona danych biometrycznych, a co najistotniejsze realizacja „prawa do bycia zapomnianym". Żadne z tych zagadnień nie istniało u progu kształtowania się prawa do ochrony danych osobowych. „Prawo do bycia zapomnianym" pojawiło się dopiero w odpowiedzi na rewolucję cyfrową i szybki rozwój Internetu oraz e-usług[331]. Internet nie służył do tego, aby chronić prywatność, ponieważ cele, które w swoich początkach miał realizować, nie zakładały potrzeby ochrony danych prywatnych. Dopuszczalna jednak była taka możliwość i każdy wówczas mógł zdecydować, w którym miejscu będą przechowywane jego dane. Wszystko się zmieniło wraz z umasowieniem usług komunikacyjnych związanych z siecią[332]. W momencie udostępniania informacji prywatnych, a nawet intymnych, znaczącą kwestią jest to, czy podmioty danych robią to świadomie, czy faktycznie przekazanie tych danych jest ich założeniem lub jest co najmniej brane przez nich pod uwagę. Google czy Facebook wykorzystują spersonalizowane

[330] M. Sakowska-Baryła, *Prawo do ochrony danych…,* s. 42-43.
[331] Zanikła granica pomiędzy „człowiekiem i maszyną, rzeczywistością realną i wirtualną". Zob. M. Herma, *Za prywatność w internecie trzeba płacić,* [dostęp:28.12.2014]https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1603593,1,za-prywatnosc-w-internecie-trzeba-placic.read.
[332] K. Szymielewicz, A. Walkowiak, *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem,* „Monitor Prawniczy" 2014, nr 9, s. 29.

działania w myśl reguły: „Dostajesz bezpłatny serwis w zamian za informacje o sobie”[333].

Wyszukiwarki internetowe wpłynęły na intensywny rozwój Internetu, umożliwiając dostęp do informacji z sieci. Google nie służy jedynie za wyszukiwarkę – to też wiele innych usług z nią powiązanych, które w większości przypadków są bezpłatne dla podmiotów niekomercyjnych. Dokonywanie przez Google działań opierających się na profilowaniu internautów można uznać za cenę za dostęp do nich. Umotywowane jest zatem postulowanie, aby regulacje prawne uwzględniały rolę wyszukiwarek w gospodarce, ponieważ tylko wtedy będzie można wykonywać konkurencyjność poprzez zwiększanie innowacyjności gospodarki, a tym samym przeciwdziałać naruszeniom prywatności informacyjnej jednostki[334]. Kolejnym przykładem z zakresu ochrony danych osobowych jest działanie aplikacji instalowanych na urządzeniach mobilnych. Aplikacje monitorujące stan zdrowia, dietę lub zakupy gromadzą dane, które rozejdą się po różnych podmiotach. Pozornie infantylna aplikacja Brightest Flashlight, pozwalająca zamienić smartfon w latarkę, nie tylko zbiera informacje o położeniu dzięki czujnikowi GPS, lecz daje także prawo wglądu w dane znajomych, którzy w ostatnim czasie telefonowali[335].

W dobie rewolucji cyfrowej dane osobowe są jednym z najdroższych dóbr, które powinny podlegać ochronie w postaci zabezpieczeń technicznych i gwarancji prawnych. Naprzeciw temu zagadnieniu wychodzi europejska inicjatywa reformy prawa ochrony prywatności oraz przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych.

1.3.2. Prawo do informacji jako prawo człowieka

W literaturze proponuje się różne interpretacje samego pojęcia informacji. Zauważa się, że pojęcie informacji wywodzi się z dziedziny cybernetyki i teorii informacji[336], którego używają przedstawiciele różnych dyscyplin naukowych[337]. Badaniem natury informacji zajmuje się nauka o informacji – zapoczątkowało ją bibliotekoznawstwo, a rozwija się dzięki

[333] M.-Th. Tinnefeld, *Jak Internet zmienia prawne ramy prywatności,* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* red. G. Szpor, W. Wiewiórowski, Warszawa 2012, s. 3.
[334] Ł. Goździaszek, *Prawo do bycia zapomnianym w wyszukiwarce internetowej-glosa do wyroku Trybunału Sprawiedliwości z 13.05.2014 r. w sprawie C-131/12 Google Spain SL i Google Inc. przeciwko Agencia de Protección de Datos (AEPD) i Mario Costeja González,* „Europejski Przegląd Sądowy” 2015, nr 2, s. 41.
[335] Na podobnych zasadach działa wiele innych darmowych aplikacji. Zob. M. Herma, *Za prywatność w internecie trzeba płacić…*
[336] T. Górzyńska, *Prawo do informacji i zasada jawności administracyjnej*. *Orzecznictwo Sądu Najwyższego, Naczelnego Sądu Administracyjnego i Trybunału Konstytucyjnego,* Kraków 1999, s. 86.
[337] G. Szpor, *Pojęcie informacji a zakres ochrony danych,* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia,* red. P. Fajgielski, Lublin 2008, s. 7-8.

informatyce[338]. Ta dyscyplina naukowa zajmuje się zapewnianiem efektywnego dostępu do informacji w warunkach niekontrolowanego rozrostu zasobów informacyjnych[339]. Pojęcie informacji jest wykorzystywane prawie we wszystkich sferach życia codziennego, wiedzy i nauki, także prawa. W każdej z tych dziedzin może być ono rozumiane inaczej[340]. Każda z definicji wskazuje na inny aspekt informacji. Do informacji można zaliczyć zarówno przedmiot materialny, jak i ideę oraz myśl. Z uwagi na digitalizację informacją staje się obecnie dokument, usługa, praca, a nawet rozrywka[341].

W podejmowanych próbach wyjaśniania definicji informacji pojawiają się dwa odmienne założenia. W kontekście tradycyjnym, typowym dla nauk społecznych i prawnych, przyjmuje się, że w terminie „informacja" zawiera się redukcja niepewności[342]. Informacją jest taki przekaz, który może zostać użyty przez jego adresata przy założeniu, że adresatem jest człowiek. Bogdan Michalski zauważa, że informację stanowi „suma wiadomości o sytuacjach, stanach rzeczy, wydarzeniach i osobach. Może być ona przedstawiona w formie pisemnej (…) i każdej innej możliwej do odbioru za pomocą zmysłów"[343]. W aspekcie tradycyjnym przyjmuje się, że informację stanowią treści intelektualne przetworzone w formę zrozumiałą dla odbiorcy, które mają dla niego wartość rzeczywistą, w toku samego poznania, jak i w procesie podejmowania decyzji[344].

Wykładnia stanowisk prezentowanych w nauce prowadzi do konkluzji, że określenie terminu „informacja" zależy od dyscypliny naukowej, niemniej jednak nawet w ramach jednej dziedziny można spotkać odmienne definicje[345]. W ślad za interpretacją w znaczeniu szerokim, pojęcie informacji mogłoby obejmować stany wiedzy i świadomości, a zatem również te komunikaty, które są utrwalone wyłącznie w pamięci człowieka. Mariusz Maciejewski proponuje, aby przyjąć, iż „informacja to utrwalony w dowolny sposób (także w pamięci człowieka) komunikat (wiedza, świadomość) o jakimś fakcie (rozumianym jako atrybut zachowania i inne). Komunikat może być utrwalony w sposób materialny (również elektroniczny na nośniku danych) i możliwy do odczytania przez inne osoby oraz w sposób niematerialny, *a contrario* niemożliwy do odczytania przez inne osoby w pamięci

[338] J. Janowski, *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniach administracji,* Warszawa 2009, s. 74.
[339] *Tamże,* s. 74.
[340] M. Mucha, *Obowiązki administracji publicznej w sferze dostępu do informacji,* Wrocław 2002, s. 22.
[341] J. Janowski, *Technologia informacyjna dla prawników…,* s. 82.
[342] T. Goban-Klas, *Media i komunikowanie masowe. Teorie i analizy prasy, radia, telewizji i Internetu,* Warszawa-Kraków 1999, s. 190.
[343] B. Michalski, *Prawo dziennikarza do informacji,* Kraków 1974, s. 9-10.
[344] J. Janowski, *Technologia informacyjna dla prawników…,* s. 92.
[345] P. Fajgielski, *Informacja w administracji publicznej-prawne aspekty gromadzenia, udostępniania i ochrony,* Warszawa 2007, s. 13.

człowieka”[346]. Grażyna Szpor stoi na stanowisku, że informacja rozumiana jako dobro niematerialne pozwala na wykorzystanie tego pojęcia w ustawowej definicji danych osobowych. Podkreśla ona, że cechą charakterystyczną danych osobowych jest ich nieprzenoszalność, co innymi słowy oznacza niedopuszczalność posłużenia się nimi przez inne osoby jako danymi identyfikującymi[347].

Definiowanie informacji nie przynosi oczekiwanych rezultatów ani przy zastosowaniu metody pozytywnej, ani wtedy, gdy podejmowane są próby wskazywania w negatywny sposób tych zjawisk i przedmiotów, które nie są informacją. Andrzej Adamski zaproponował odróżnienie terminu informacji od pojęcia danych, wskazując, że dane są nośnikiem informacji i mogą być jej źródłem[348]. Według Pawła Fajgielskiego w takim ujęciu „dane stanowią zakodowany zapis informacji – ich treść można odczytać wówczas, gdy znane są konwencje wykorzystane do ich zakodowania”[349]. Pojęcie informacji w języku prawnym jest używane w dwóch odmiennych funkcjach – jako zwrot dookreślający albo jako wyraz zasadniczy. Informacja w funkcji dookreślającej inne pojęcie jest interpretowana w sposób tradycyjny, bliski językowi potocznemu[350].

Definicja prawa do informacji też nie ma ujednoliconego charakteru. Modyfikacje dotyczą zakresu podmiotowego i przedmiotowego, trybu uzyskiwania dostępu do informacji, a także środków ochrony. Jednakże mimo pojawiających się rozbieżności w porządkach prawnych państw europejskich, można zagwarantować ochronę i poszanowanie aktywności człowieka przejawiających się w poszukiwaniu informacji, pozyskiwaniu danych i poszerzaniu wiedzy[351].

Prawo do informacji początkowo było jedynie przedmiotem orzecznictwa sądowego. Aktualnie, wykracza poza ramy jednego przepisu prawa. Prawo do informacji obejmuje wiele unormowań znajdujących się w dokumentach mających niejednolitą moc prawną. Fundamentem szczegółowych uregulowań są rozwiązania o powszechnym charakterze, nawiązujące do wspólnych wartości, a tym samym urzeczywistniające prawo do informacji

---

[346] M. Maciejewski, *Prawo informacji-zagadnienia podstawowe,* [w:] *Prawo informacji, prawo do informacji,* red. W. Góralczyk, Warszawa 2006, s. 31.
[347] G. Szpor, *Pojęcie informacji a zakres…,* s. 17.
[348] A. Adamski, *Prawo karne komputerowe,* Warszawa 2000, s. 37.
[349] Terminem danych ustawodawca posługuje się niejednokrotnie. Z reguły nie dokonuje rozróżnienia pomiędzy informacjami a danymi, a czasem nawet „definiuje dane z wykorzystaniem pojęcia informacji”. Zob. P. Fajgielski, *Informacja w administracji publicznej…,* s. 15-16.
[350] Zjawisko to jest widoczne zwłaszcza w regulacjach zapewniających ochronę danych osobowych, gdzie dane osobowe definiowane są jako informacje.
[351] J. Taczkowska-Olszewska, *Dostęp do informacji publicznej w polskim systemie prawnym,* Warszawa 2014, s. 20-21.

jako jedno z podstawowych praw człowieka[352]. Systematyka praw człowieka znacząco wpływa na jego rozwój. Prawo do informacji zaliczane jest do tzw. praw nowoczesnych, które podlegają szczególnej ochronie z uwagi na rozwój nowych technologii informacyjnych, w tym nowych wyzwań społecznych (walka z terroryzmem, handel narkotykami, choroby zakaźne)[353]. Prawa podstawowe z jednej strony są traktowane jako podmiotowe, natomiast z drugiej przyznaje się im wyższą moc prawną. Wypływa to z faktu, że służą nie tylko podmiotom jednostkowym, ale i kształtują ustrój polityczny[354].

Prawo do informacji ma wytworny charakter. Przejawia się to w pokonywaniu barier technicznych i językowych. Do prawa do informacji sięgają głównie specjaliści z różnych gałęzi działalności Unii Europejskiej, zaś procedura uzyskania określonej informacji zmusza do posiadania wiedzy z tego zakresu i używania zasobów informacyjnych. Negatywnie może oddziaływać czasochłonna procedura sądowa, która prowadzi do zaniku prawa do informacji poprzez długoletni czas oczekiwania na prawomocne orzeczenie. Niejednokrotnie zwraca się także uwagę na niebezpieczeństwo dla suwerenności państwa. Wynika ono z uzależnienia procesów informacyjnych od podmiotów zewnętrznych. Utrata niezależności państwa następuje poprzez przejęcie przez źródła zewnętrzne kontroli nad przepływem i badaniem jakości informacji. Po przekroczeniu granicy w drastycznym stopniu następuje zanik podejmowania decyzji politycznych, społecznych i ekonomicznych w sposób samodzielny[355].

Prawo do informacji wypływa z katalogu wartości uznawanych za wspólne dziedzictwo narodów wymagające prawnej ochrony przez poszczególne państwa, jak również organizacje międzynarodowe, których są one członkami. Na płaszczyźnie europejskiej, prawo do informacji zostało ustanowione, aby tworzyć jeszcze bliższe związki pomiędzy narodami Europy, w których decyzje podejmowane są tak otwarcie, jak to tylko możliwe[356]. Doprowadza to do wykreowania polityki przejrzystości, która przejawia się w szacunku dla praw podstawowych. Prawo do informacji ma za zadanie służyć bowiem realizacji zasad otwartości i bliskości, przejrzystości oraz poufności. Multicentryczność systemu prawa, co oznacza krzyżowanie się reguł obowiązujących w porządkach prawnych różnych państw,

---

[352] Odmienną opinię w tym przedmiocie wyraża I. Kondak, *Kto chce, ten wie,* „Rzeczpospolita" z dnia 10.06.2002 r., s. C3.
[353] F. Jasiński, *Karta Praw Podstawowych,* Warszawa 2003, s. 203.
[354] B. Banaszak, *Ogólne wiadomości o prawach człowieka,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2002, s. 22.
[355] J. Oleński, W. Jaworski, *Uwarunkowania patologii informacji i drogi jej zwalczania,* [w:] *Prawo informacji, prawo do informacji,* red. W. Góralczyk, Warszawa 2006, s. 300.
[356] Punkt 1 Preambuły Rozporządzenia (WE) Nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz. Urz. UE L 145, 31/05/2001, P. 0043-0048).

opartych na tych samych wartościach[357], nakłada powinność dokonywania interpretacji prawa do informacji nie tylko przez instytucje krajowe, ale też przez te o charakterze międzynarodowym, tj. Europejski Trybunał Praw Człowieka czy Trybunał Sprawiedliwości Unii Europejskiej.

Gwarancje zapewniające prawo do informacji zaliczają się do katalogu norm w prawie ponadnarodowym, które zostały ustanowione, aby zintegrować wspólnoty[358]. Ich zasadniczym celem nie jest ochrona praw podmiotowych jednostki. Prawo do informacji ma służyć interesom wspólnoty – ponadnarodowej strukturze opartej na scentralizowanej władzy i skoncentrowanej na wypracowywaniu standardów w polityce zagranicznej i bezpieczeństwa oraz we współpracy sądowo – policyjnej[359]. Prawo do informacji zostało wyartykułowane w prawie pierwotnym Unii Europejskiej[360]. Zakres prawa do informacji jest skutkiem nie tylko unormowań traktatowych, ale także konsekwencją przyjętej przez Trybunał Sprawiedliwości rozszerzającej wykładni zapisów Traktatu. Przy wyrokowaniu, Trybunał uwzględnia cel ustanowienia Unii Europejskiej, jak i regulacje prawnomiędzynarodowe, do których się odwołuje. Pod jurysdykcję Trybunału Sprawiedliwości została poddana kontrola poszanowania praw człowieka jako zasadniczej zasady prawa unijnego[361].

Ekspansja katalogu wspólnie wypracowanych wartości, które objęte są ochroną w oparciu o akty prawa pierwotnego Unii Europejskiej i uregulowania prawnomiędzynarodowe, doprowadza do podejmowania prób ich uporządkowania, a czasem również i do ustalania rangi oraz relacji panujących między wartościami uznawanymi za podstawowe. Traci na aktualności koncepcja o aksjologicznej neutralności praw podstawowych[362]. Zbiór praw jest dynamiczny. Nie wyklucza się dodawania nowych praw albo odwrotnie – usamodzielniania się elementów do tej pory chronionych praw w autonomiczne prawa ludzkie. Do wspólnych wartości zalicza się prawo praw człowieka, które należy respektować w każdym społeczeństwie, mimo zróżnicowanych warunków

[357] H. Izdebski, *Doktryny polityczno-prawne. Fundamenty współczesnych państw,* Warszawa 2015, s. 16.
[358] I.C. Kamiński, *Słuszność i prawo. Szkic prawnoporównawczy,* Kraków 2003, s. 61-62.
[359] C. Brewin, *Europe,* [w:] *Foreign Policy and Human Rights. Issues and Responsem,* red. R.J. Vincent, Cambridge 1986, s. 195.
[360] Na gruncie prawa unijnego przez długi czas nie podejmowano prób definicji prawa do informacji. Traktaty założycielskie nie zawierały w swej treści postanowień odnoszących się do wolności i praw jednostki. Doprowadziło to do ukształtowania się tzw. prawa pretoriańskiego, którego podstawowym założeniem było oparcie działań organów Unii Europejskiej na standardach wynikających z judykatury Europejskiego Trybunału Praw Człowieka, kształtowanych na zasadzie Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności jako aktu prawa międzynarodowego. Zob. J. Taczkowska-Olszewska, *Dostęp do informacji…,* s. 48.
[361] F. Benoit-Rohmer, H. Klebes, *Prawo Rady Europy. W stronę europejskiej przestrzeni prawnej,* przekł. M.A. Nowicki, Warszawa 2006, s. 148.
[362] T. Jasudowicz, *Administracja wobec praw człowieka,* Toruń 1996, s. 30.

życiowych[363]. Na prawa człowieka składa się zespół norm identyfikujących wolności i prawa przynależne człowiekowi tylko z uwagi na to, że jest człowiekiem. Zalicza się je do praw pierwszej generacji („wolność od")[364]. Drugą generację stanowią prawa społeczne i ekonomiczne, które powinny być realizowane przez władze publiczne. Aktualnie w nauce prawa wykształciły się także prawa trzeciej generacji odnoszące się do ogółu społeczności[365].

Prawo do informacji zalicza się do praw drugiej generacji. Prawo do informacji nie zostało wprost wyrażone w regulacjach o charakterze międzynarodowym. Zanim uregulowano je wprost w aktach normatywnych, to utożsamiano go z wolnością wypowiedzi[366], czyli w katalogu praw i wolności zaliczanych do klasycznych praw wolnościowych[367]. Wolność wypowiedzi jest prawem negatywnym. W systematyce praw podstawowych posiada wysoką rangę. Zazwyczaj powoływane jest wówczas, gdy ocenie podlega zakres i sposób realizacji prawa do informacji. Z wolnością wypowiedzi, a inaczej z wolnością wyrażania poglądów, łączy się wolność w przedmiocie komunikowania, pozyskiwania i rozpowszechniania informacji. Wolność wypowiedzi nie ma racji bytu bez wolności komunikowania. Jednakże trzeba zaznaczyć, że informacja a komunikacja to odrębne pojęcia. Informacja jest jedynie elementem komunikacji[368]. W literaturze przedmiotu przyjmuje się, iż prawo do informacji nie tylko wywodzi się z wolności wypowiedzi, ale jest też jej częścią składową. Nie ma mowy o swobodzie rozpowszechniania informacji, jeżeli nie jest ona związana z wcześniejszym uzyskaniem informacji. Wolność wypowiedzi może zaistnieć jedynie w przypadku wolności informacji, składającej się z wolności poszukiwania, otrzymywania i przekazywania informacji[369].

Na kontynencie europejskim, prawo do informacji powstało w oparciu o Europejską Konwencję o Ochronie Praw Człowieka i Podstawowych Wolności[370]. Niniejsza Konwencja zawiera w sobie katalog praw i wolności oraz ustanawia zasady kontroli ich respektowania. Kontrola przejawia się w podporządkowaniu krajów – sygnatariuszy Konwencji pod jurysdykcję Trybunału Praw Człowieka, czyli organu posiadającego uprawnienia do

---

[363] A. Łopatka, *System Międzynarodowej Ochrony Praw Człowieka,* [w:] *Ochrona praw człowieka w świecie,* red. L. Wiśniewski, Bydgoszcz-Poznań 2000, s. 70.
[364] H. Izdebski, *Fundamenty współczesnych państw,* Warszawa 2007, s. 20.
[365] L. Wiśniewski, *Prawo a wolność człowieka-pojęcie i konstrukcja prawna,* Warszawa 1997, s. 21.
[366] Uzasadnienie do projektu Konwencji Rady Europy o dostępie do dokumentów urzędowych (CM/Del/Dec2008) 1025/4.3, [dostęp: 04.04.2008] http://assembly.coe.in.
[367] R. Mizerski, *Wolność ekspresji,* [w:] *Prawa człowieka i ich ochrona. Podręcznik dla studentów prawa i administracji,* Toruń 2005, s. 330.
[368] J. Sobczak, *Prawo prasowe. Podręcznik akademicki,* Warszawa 2000, s. 34.
[369] *Tamże,* s. 73.
[370] W treści samej Konwencji prawo do informacji zostało pominięte. Dopiero interpretacja pojęcia wolności wypowiedzi pozwoliła na jego dookreślenie.

rozwiązywania sporów na tle przestrzegania wolności i praw człowieka[371]. Trybunał Praw Człowieka kreował treść prawa do informacji[372]. W swoich rozważaniach powoływał się także na gwarancje ochrony wolności wypowiedzi i życia prywatnego. Dokonując wykładni zakresu wolności wypowiedzi, Trybunał przyjął, że nie obejmuje ona dostępu do dokumentów urzędowych oraz nie nakłada na władze publiczne pozytywnych obowiązków w aspekcie przekazywania informacji[373].

Aktualnie prawo do informacji może być realizowane odrębnie od norm, na podstawie których zagwarantowana jest wolność wypowiedzi i ochrona prywatności. Wynika to z tego, że ochrona wolności wypowiedzi wiązała się bezpośrednio z podmiotowością człowieka[374], ochrona prawa do informacji wypływa z pobudek ogólnospołecznych[375]. Prawo do informacji przejawia się, wobec tego nie tylko w indywidualnym interesie osoby ubiegającej się o informację, ale również w interesie całego społeczeństwa, a co więcej całego kraju[376]. Powyższe wskazuje na dwoistość celów tego uprawnienia. Prawo do informacji jest publicznym prawem podmiotowym. Oznacza to, że może ono przysługiwać każdemu, a jego urzeczywistnienie następuje z uwagi na interes państwa i społeczeństwa. Obywatel nie musi przy tym udowadniać, że działa we własnym interesie faktycznym, bądź prawnym[377]. Prawo do informacji jako jedno z praw człowieka może zostać ograniczone. Następuje to tylko po spełnieniu przesłanek przewidzianych dla pozostałych wolności i praw człowieka, zwłaszcza dla ograniczenia wolności wypowiedzi[378]. O zjawisku ingerencji w prawa człowieka można mówić, gdy jest zgodna z prawem, konieczna w demokratycznym państwie prawa i proporcjonalna w stosunku do zaimplementowanej sankcji.

Rozbieżności w określaniu prawa do informacji wynikają z różnic w identyfikowaniu źródeł prawa do informacji, jak i celów, jakim prawo to powinno służyć. Jeśli przyjmie się, że

---

[371] R. Hliwa, *Model ochrony praw człowieka w systemie Rady Europy. Mechanizmy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności,* [w:] *Ochrona praw człowieka w świecie,* red. L. Wiśniewski, Poznań 2000, s. 193.

[372] Zdaniem ETPCz zakresem autonomii informacyjnej objęte są tylko te informacje, które pochodzą ze źródeł ogólnodostępnych.

[373] I. Kondak, *Prawo do informacji publicznej w świetle standardów Rady Europy,* „Państwo i Prawo" 2007, nr 3, s. 72.

[374] A. Frankiewicz, *Regulacje wolności wypowiedzi w polskim porządku prawnym,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2002, s. 362.

[375] Mechanizmy umożliwiające dostęp do informacji umacniają zaufanie obywateli do organów sprawujących władzę. Gwarancje dostępu do informacji służą celowi publicznemu. Prawo do informacji łączy się czasem z zasadą jawności, na mocy której jest zapewniony dostęp do dokumentów urzędowych.

[376] M. Leciak, *Kultura jawności-Klauzula tajności. Dziennikarskie prawo do informacji a prawnokarna ochrona tajemnicy państwowej. Zarys problematyki,* [w:] *Znaczenie informacji w społeczeństwie obywatelskim. Wybrane aspekty prawne,* red. J. Marszałek-Kawa, B. Chludziński, Toruń 2007, s. 125.

[377] W. Jakimowicz, *O publicznych prawach podmiotowych,* „Państwo i Prawo" 1999, nr 1, s. 37.

[378] W. Sadurski, *Prawo przed sądem. Studium sądownictwa konstytucyjnego w postkomunistycznych państwach Europy Środkowej i Wschodniej,* Warszawa 2008, s. 365.

źródłem prawa do informacji jest wolność wypowiedzi, to na jego treść składać się będzie realizacja wartości, którymi są integralność osoby ludzkiej, jej rozwój, a także zaspokajanie potrzeb osobistych. Przyjęcie założenia, jakoby celem przyświecającym jest ochrona demokratycznego systemu Unii Europejskiej, doprowadza do wniosku, że posiada ono cechy prawa reglamentowanego i nie należy go utożsamiać w większym stopniu z naturą praw człowieka jako wartości niederogowanych, czyli takich, których wykonywania państwo nie może zaprzestać[379]. Karta Praw Podstawowych Unii Europejskiej jako część prawa pierwotnego wpisuje się nieco w realizację koncepcji kultury otwartego zarządzania, wobec czego coraz częściej kwestionowane jest identyfikowanie prawa do informacji z prawami człowieka w ich pierwotnym założeniu.

W porządkach prawnych państw europejskich, prawo do informacji zyskało samoistny status prawny. Informacja stała się niezależna od gwarancji wolności wypowiedzi. Prawo do informacji przestało być prawem jedynie wolnościowym[380]. Wobec tego zyskało miano nie tylko prawa podmiotowego, ale i zostało zaliczone do kategorii praw publicznych[381].

1.3.3. Publicznoprawny charakter prawa do informacji

Prawo do informacji zostało stworzone w interesie publicznym[382]. System demokratyczny państwa prawnego jest wartością, jaka poddana jest ochronie w oparciu o normy zapewniające obywatelom dostęp do informacji[383]. Fundamentalne zasady odwołujące się do informacji o charakterze publicznym zostały określone w porządku prawa ponadnarodowego, a konkretnie w Traktacie o Funkcjonowaniu Unii Europejskiej i w Karcie Praw Podstawowych Unii Europejskiej. Na podstawie art. 15 ust. 3 TFUE każdy obywatel Unii Europejskiej i każda osoba fizyczna lub prawna posiada prawo dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy[384]. Zostało to zaakcentowane w art. 42 KPP UE. Oznacza to wzmocnienie pozycji dostępu do dokumentów

[379] R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne,* Warszawa 2003, s. 25.
[380] Prawo do informacji działa dwustopniowo *in abstracto* (wykonywanie prawa jest potencjalnie możliwe po spełnieniu przez podmiot koniecznych przesłanek) oraz *in concreto* (dany podmiot nabył potrzebne uprawnienia). Por. K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP,* Kraków 1999, s. 26.
[381] J. Boć, *Prawo administracyjne,* Wrocław 2007, s. 501.
[382] T. Górzyńska, *Geneza i rozwój prawa do informacji,* [w:] *Prawo do informacji,* red. W. Góralczyk, Warszawa 2006, s. 23.
[383] Projekt Rezolucji Parlamentu Europejskiego z dnia 20 listopada 2008 r., pkt C.
[384] Regulacje dotyczące prawa dostępu do dokumentów są przejawem zasady otwartości. Oznacza to, że każda instytucja, organ i jednostka organizacyjna powinna deklarować przejrzystość swoich prac i opracowywać przepisy szczególne nt. dostępu do jej dokumentów w swoim regulaminie wewnętrznym.

i potwierdzenie jego rangi w postaci umieszczenia w katalogu praw fundamentalnych[385]. Powszechny dostęp do dokumentów jest zasadą prawną i możliwość jego odmowy jest uprawnieniem wyjątkowym[386]. Prawo do informacji jest tworem nie tylko unormowań traktatowych, ale również efektem dokonywanej przez Trybunał Sprawiedliwości wykładni przepisów Traktatu *sensu largo*[387]. Trybunał w procesie orzekania kieruje się celem funkcjonowania Unii Europejskiej poprzez uwzględnianie treści preambuły Traktatów, jak i przepisami prawnomiędzynarodowymi, do których odwołuje się ta preambuła. Trybunał Sprawiedliwości zwraca uwagę na postanowienia Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[388].

Podstawą orzekania Trybunału Sprawiedliwości w sprawach o udostępnienie informacji było także Rozporządzenie (WE) nr 1049/2001. To właśnie w nim państwo członkowskie Unii Europejskiej mogło zażądać od instytucji nieujawnienia dokumentu pochodzącego od tego państwa bez wyrażenia przez niego wcześniejszej zgody. Warunek ten zgodnie z przekonaniem Trybunału pozostaje *lex specialis* wobec pozostałych regulacji i skierowany jest do instytucji, aby nie ujawniała prawidłowego dokumentu. Dana organizacja nie posiada uprawnienia, aby sprawdzać, czy nieudostępnienie jest zasadne przy zastosowaniu kryterium publicznego[389].

Trybunał Praw Człowieka nie uznaje prawa do informacji jako prawa o charakterze publicznoprawnym, biorąc łącznie pod uwagę językową, jak i celowościową interpretację. Prawo do pozyskiwania informacji zostało ustanowione na rzecz każdego człowieka, aby objąć ochroną jego interesy przed ingerencją ze strony władz publicznych. Uprawnienie to reguluje zatem stosunki prywatnoprawne.

Parlament Europejski w Dyrektywie 2003/98/WE z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystania informacji sektora publicznego[390] wskazał na nałożony na każde z krajów członkowskich UE obowiązek określenia ogólnych warunków

---

[385] M. Szwarc-Kuczer, *Komentarz do art. 42 Karty Praw Podstawowych,* [w:] *Karta Praw Podstawowych. Komentarz,* red. A. Wróbel, Warszawa 2013, s. 1123.
[386] Wyrok SPI z dnia 8 listopada 2007 r., sygn. akt: T-194/04, *The Bavarian Lager Co Ltd. V. Komisja Wspólnot Europejskich,* Zbiór Orzeczeń 2007, s. II-4523.
[387] F. Benoit-Rohmer, H. Klebes, *Prawo Rady Europy…,* s. 148.
[388] W tej sytuacji zauważa się zagrożenie konkurencyjnym systemem ochrony praw człowieka. Jest to związane najpierw z uchwaleniem, a potem z wejściem w życie Karty Praw Podstawowych, która przejęła postanowienia Konwencji. Doprowadziło to niejako do wyodrębnienia się dwóch systemów ochrony w Europie. Wobec tego podjęto kroki, aby zapewnić przestrzeganie postanowień Konwencji w stosunku do każdej osoby będącej pod jurysdykcją Unii Europejskiej.
[389] Wyrok SPI z dnia 30 listopada 2004 r., sygn. akt: T-168/02, *IFAW Internationale Tierschutz-Fonds GmbH i in. przeciwko Komisji Wspólnot Europejskich*, Zbiór Orzeczeń 2004, s. II-4134, pkt 58-59.
[390] Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystania informacji sektora publicznego (Dz. Urz. UE L nr 345 z 31.12.2003, s. 90).

regulujących ponowne wykorzystanie informacji sektora publicznego. Parlament Europejski zwrócił uwagę na to, że informacja sektora publicznego jest istotnym materiałem wyjściowym dla produktów i usług związanych z zasobami cyfrowymi. Sektor publiczny zbiera, produkuje, reprodukuje i rozpowszechnia szeroki zakres informacji w wielu obszarach działalności, takiej jak społeczna, ekonomiczna, geograficzna, turystyczna czy edukacyjna. Zalecenia zawarte w Dyrektywie mają służyć „rozwojowi rynku informacyjnego". Prawo człowieka i obywatela do pozyskiwania informacji w przedmiocie spraw publicznych jest rezultatem postępujących zmian, jakie zachodziły na płaszczyźnie prawa międzynarodowego, prawa unijnego oraz w systemach prawa poszczególnych państw[391].

W regulacjach konstytucyjnych niejednokrotnie następuje krzyżowanie się informacji z pojęciami o szerszym zakresie. Częstokroć ustrojodawca traktuje informację jako element innego dobra chronionego przez Konstytucję RP[392]. Ochrona wolności informacji posiada pierwszeństwo wobec ochrony innych dóbr, których jest fragmentem. Głębsza ocena stosunków panujących pomiędzy wolnością informacji a innymi wolnościami i prawami gwarantowanymi konstytucyjnie pozwala zauważyć ich bezpośrednią relację, a z drugiej strony wskazuje na związki pośrednie w odniesieniu do wolnościowych i demokratycznych zasad ustroju państwa[393]. Prawo do informacji w generalnej postaci jest zawarte w art. 54 ustawy zasadniczej jako wolność poglądów i prawo do pozyskiwania oraz rozpowszechniania informacji. W tym przepisie brak jest ograniczeń w związku z publicznym charakterem informacji, natomiast sformułowane określenie „każdy" powoduje, że z uprawnienia tego korzysta nie tylko człowiek i obywatel, ale też każdy podmiot mający osobowość prawną[394].

Prawo do informacji o charakterze podmiotowym[395] zostało zawarte w kilku postanowieniach Konstytucji RP. Zostało ono uwzględnione w ramach ochrony prywatności w art. 51 ust. 3 Konstytucji RP (jako prawo do autonomii informacyjnej), jak też w art. 61 Konstytucji RP (jako prawo do informacji o działalności organów władzy publicznej) oraz

---

[391] B. Gronowska, *Systematyka międzynarodowo chronionych praw człowieka,* [w:] *Prawa człowieka w sytuacjach nadzwyczajnych,* red. T. Jasudowicz, Toruń 1997, s. 186.

[392] Informacja może podlegać ochronie na zasadzie regulacji gwarantujących ochronę takim dobrom, jak wolność wypowiedzi (art. 14 Konstytucji RP), sfera życia prywatnego (art. 47 Konstytucji RP), autonomia informacyjna (art. 51 Konstytucji RP), jawność życia publicznego (art. 61 Konstytucji RP), bezpieczeństwo ekologiczne (art. 74 Konstytucji RP).

[393] W. Sokolewicz, *Wprowadzenie do rozdziału II Konstytucji RP,* [w:] *Konstytucja Rzeczypospolitej Polskiej,* red. L. Garlicki, Warszawa 2005, s. 9.

[394] P. Winczorek, *Opinia w sprawie dostępu do informacji w Kancelarii Sejmu,* „Przegląd Sejmowy" 2003, nr 1, s. 69.

[395] Prawo podmiotowe definiowane jest jako „złożone sytuacje prawne wyznaczane jakimś podmiotom przez obowiązujące normy ze względu na uznawane przez prawodawcę społecznie uzasadnione interesy tych podmiotów". Zob. S. Wronkowska, Z. Ziembiński, *Zarys teorii prawa,* Poznań 2001, s. 109.

w art. 74 ust. 3 Konstytucji RP (jako prawo do informacji o stanie i ochronie środowiska).

W regulacjach dotyczących autonomii informacyjnej znaleźć można aż czterokrotne odwołanie do ustaw zwykłych. Odesłanie to limituje administracyjne władztwo w kontekście czynności oddziałujących na prywatne życie obywateli. Na podstawie regulacji konstytucyjnych organy władzy publicznej mogą żądać od obywateli udzielania informacji, wyłącznie w oparciu o przepisy aktów rangi ustawowej. Tylko ustawa umożliwia organom władzy publicznej skorzystanie z przysługujących jej kompetencji ograniczania obywatelom dostępu do dotyczących ich danych. Działania administracji, które są sprzeczne z ustawą mogą powodować powstanie obowiązku prostowania informacji. Należy zwrócić uwagę, że nawet działalność polegająca na zbieraniu informacji o obywatelach i ich udostępnianiu wymaga zgodności z regulacją ustawową[396].

Delegacja do uregulowania w trybie ustawy zwykłej zasad udzielania informacji pojawia się również w odniesieniu do prawa do informacji publicznej oraz prawa do informacji o stanie i ochronie środowiska. W odniesieniu do informacji publicznych, ustawodawca zwykły nie powinien wykroczyć poza regulowanie proceduralnego aspektu korzystania z prawa do informacji[397]. Ustawa zasadnicza dla określenia przedmiotu informacji publicznej podlegającej udostępnieniu posługuje się kryterium podmiotowym, zapewniając dostęp do informacji o działalności organów władzy publicznej, osób pełniących funkcje publiczne, jak również osób wykonujących zadania publiczne lub gospodarujących mieniem komunalnym lub majątkiem Skarbu Państwa (art. 61 ust. 1 Konstytucji RP). Z tego wynika, że prawo do informacji publicznej ma charakter zakresowo nieograniczony, ponieważ uzależniony jest od dynamiki i efektywności działań podmiotów publicznych. Wojciech Sokolewicz zwraca uwagę na fakt, że między regulacjami ustawowymi i konstytucyjnymi zauważalny jest brak spójności[398].

Odbiorcą obowiązku polegającego na udostępnieniu informacji są organy władzy publicznej. Inaczej jednak zakreślany jest krąg podmiotów upoważnionych do jej otrzymania, a także inny jest schemat udostępniania. Analiza regulacji Konstytucji RP, doktryna, jak też poglądy wyrażone w judykaturze traktują, iż normy prawne mogą obejmować informacje tego samego typu lub te same, jednakże z powołaniem się na różne podstawy prawne. Odnosi się

[396] J. Taczkowska-Olszewska, *Dostęp do informacji…,* s. 75.
[397] M. Zubik, *Opinia w sprawie dostępu do informacji w Kancelarii Sejmu,* „Przegląd Sejmowy" 2003, nr 1, s. 58.
[398] „W ustawie bowiem na plan pierwszy wysuwa się dla zdefiniowania informacji publicznej kryterium przedmiotowe, w dodatku sformułowane nieprecyzyjnie, co prowadzi do wniosków odmiennych od tych, jakie przynosi wykładnia odpowiednich przepisów Konstytucji". Zob. W. Sokolewicz, *Komentarz do art. 61 Konstytucji,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, Warszawa 2005, s. 21-22.

to do informacji o charakterze publicznym, których przekazanie może następować w ramach realizacji autonomii informacyjnej. Zakres informacji udzielanej zgodnie z art. 51 ust. 3 ustawy zasadniczej może pokrywać się z tą informacją publiczną, którą wyrażono w art. 61 Konstytucji RP. Element odróżniający te dwa przepisy od siebie nie zawsze jest wyartykułowany w sposób wyraźny, w szczególności w sytuacji, w której dokumentacja działania władzy publicznej posiada informacje osobowe. Orzecznictwo raczej rozstrzyga tego typu wątpliwości na rzecz ochrony danych osobowych[399]. Dokonując interpretacji tegoż stwierdzenia, udostępnienie informacji o charakterze osobowym następuje nie tylko tym osobom, które posiadają uprawnienie w oparciu o treść regulacji o ochronie autonomii informacyjnej, ale także tym podmiotom, do których dane te nie odnoszą się bezpośrednio, niemniej jednak domagają się one ich ujawnienia powołując się na realizację prawa dostępu do informacji publicznych.

Na temat trybu dostępu do informacji określonego w Konstytucji RP negatywnie odniosła się T. Górzyńska, która uważa, że nie jest w żaden sposób umotywowane, aby prawo do informacji było regulowane w przepisach kilku artykułów tym bardziej, iż uprawnienie dostępu nie jest polityczne ze względu na typ informacji (np. informacji dotyczącej działalności władz publicznych) przez sam fakt znajdowania się w kilku przepisach Konstytucji RP[400]. Aczkolwiek trzeba zauważyć, że usystematyzowanie prawa do informacji w jednym przepisie, pośród jednej kategorii albo też umiejscowienie wśród zasad ustrojowych w rozdziale pierwszym Konstytucji RP nie powodowałoby samo przez się jego jednoznacznej interpretacji. Wręcz przeciwnie, mogłoby doprowadzić do sporu, na ile prawo do informacji może być powszechne. Pozostawienie wolności informacji jako zasady ustrojowej, a jednocześnie wyłącznej gwarancji dostępu do informacji, mogłoby doprowadzić do odmówienia mu charakteru prawa podmiotowego. Zasady ustrojowe, choć kreują po stronie władz publicznych obowiązek ich realizacji, to nie tworzą jednostce bezpośrednich roszczeń. O ile zatem racjonalne zdają się być wskazówki dotyczące konieczności rekonstrukcji prawa do informacji publicznej na podstawie wielu przepisów Konstytucji RP, o tyle zabieg ten znajduje uzasadnienie z powodu rodzaju dóbr i interesów, których ochronie służy[401].

W literaturze przedmiotu wskazuje się, że sformułowane w art. 61 Konstytucji RP prawo do informacji publicznych (jako prawo polityczne), stanowi wydźwięk realizacji

[399] W. Sokolewicz, *Komentarz do art. 61 Konstytucji…,* s. 24.
[400] T. Górzyńska, *Prawo do informacji i zasada jawności…,* s. 92.
[401] J. Jendrośka, M. Stoczkiewicz, *Ustawa o dostępie do informacji publicznej a regulacje szczególne,* „Państwo i Prawo" 2003, z. 6, s. 91.

zasady zwierzchniej władzy narodu, jawności życia publicznego i zasady demokratycznego państwa prawnego[402]. Ochronie prywatności, traktowanej w kategoriach dobra osobistego, służy gwarantowane w art. 51 Konstytucji RP prawo dostępu do dokumentów urzędowych i zbiorów danych, jak też prawo do prostowania zawartych w nich informacji. Obowiązek udostępniania informacji, o których mowa w art. 51 oraz art. 61 ustawy zasadniczej spoczywa w pierwszej kolejności na organach władzy publicznej[403]. Odmienne zagadnienie adresata normy prawnej ustrojodawca ustanowił w art. 54 Konstytucji RP, gdzie udzielił gwarancji wolności informacji. Mają one bowiem wymiar powszechny, są skierowane do wszystkich podmiotów oraz przysługują im w jednakowym stopniu[404]. Obowiązek władz publicznych jest wynikiem generalnej wykładni norm konstytucyjnych w zakresie, w jakim regulują one prawa wolnościowe. Leszek Garlicki przyjął w dominującym stopniu koncepcję dwuwarstwowego pojmowania praw i wolności zawartych w Konstytucji RP. Każdy przepis konstytucyjny wyrażający prawo lub wolność powinien być rozumiany jako prawo podmiotowe (konkretne uprawnienie przysługujące jednostce), ale także jako wskazówka działania dla całego systemu władz publicznych[405]. Obowiązkiem nałożonym na władze publiczne jest nie tyle udostępnianie informacji, co zapewnienie jej swobodnego przepływu między podmiotami reprezentującymi władzę publiczną, jak i w ramach komunikacji prywatnej. Artykuł 61 Konstytucji RP stanowi jedynie fragment prawa do pozyskiwania informacji, natomiast art. 54 ustawy zasadniczej pozwala na udostępnianie informacji w szerszym zakresie niż byłoby to możliwe z powołaniem się na regulacje wyłącznie wynikające z art. 61 Konstytucji RP[406].

Nadmienić należy, że brak jest zgodności poglądów co do oceny relacji zachodzących między postanowieniami Konstytucji RP zapewniającymi prawo do informacji. Konstytucyjna wolność informacji z art. 54 ustawy zasadniczej powiązana jest z innymi prawami, m.in. do informacji publicznej z art. 61 Konstytucji RP, do dostępu osoby zainteresowanej do danych osobowych w dokumentach urzędowych z art. 51 ust. 3

[402] P. Winczorek, *Prawo obywatela do informacji,* „Rzeczpospolita" 24.02.2000 r., s. A12.
[403] A. Łabno-Jabłońska, *Zasada bezpośredniego obowiązywania konstytucyjnych praw i wolności jednostki. Analiza prawnoporównawcza,* [w:] *Podstawowe prawa jednostki i ich sądowa ochrona,* red. L. Wiśniewski, Warszawa 1997, s. 72.
[404] S. Wach, *Administracyjno-prawne ograniczenia wolności jednostki w Polsce,* [w:] *Prawne aspekty wolności. Zbiór studiów,* red. E. Cała-Wacinkiewicz, D. Wacinkiewicz, Toruń 2008, s. 38.
[405] L. Garlicki, *Polskie prawo konstytucyjne…,* s. 106.
[406] J. Sobczak, *Prawo do prywatności a wolność słowa i druku,* [w:] *Podstawowe problemy stosowania Konstytucji Rzeczypospolitej Polskiej. Raport wstępny,* red. K. Działocha, Warszawa 2004, s. 195.

Konstytucji RP[407], zaś elementem pozwalającym na odróżnienie prawa od wolności jest to, czy symetryczne obowiązki podmiotów trzecich przejawiają się głównie w działaniach, czy zaniechaniach. Najczęściej formułowany jest pogląd, że regulacje zawierające się w art. 54 Konstytucji RP są uzupełniane postanowieniami z art. 61 Konstytucji RP, te zaś dopełniają prawa gwarantujące dostęp do informacji szczególnych, określonych w art. 51 ustawy zasadniczej.

Ciężko też zgodzić się z poglądem, że pomiędzy art. 61 Konstytucji RP a art. 51 Konstytucji RP nie zachodzi żadna zależność, ponieważ ustrojodawca wyodrębnił dwie sfery. Sferę prywatności odnoszącą się do ochrony życia prywatnego oraz danych osobowych (chronioną regulacją prawną z art. 47 i art. 51 ustawy zasadniczej) oraz sferę działalności publicznej. Kontrowersyjne jest twierdzenie, że w ustawie zasadniczej nie ma kolizji między prawem do informacji publicznej a m.in. prawem do prywatności. Prawdopodobnie wynika to z przekonania, że podanie informacji do wiadomości publicznej pozbawia ją prywatnego elementu. Ujawnienie informacji prywatnej, umotywowane nawet względami interesu publicznego, może być jedynie oceniane w oparciu o kryterium legalności. Nie będzie więc działaniem bezprawnym ujawnienie informacji, która w dalszym ciągu pozostanie prywatną. Zgoła odmienna interpretacja prowadziłaby do konkluzji, że życie prywatne uzależnione jest od statusu podmiotu, którego dotyczy[408]. Prywatność powinna być rozumiana w sposób jednoznaczny, niemniej jednak prywatność osób pełniących funkcje publiczne może ulec zakłóceniu[409].

Obowiązkiem organu, który posiada żądaną informację nie jest tylko sprawdzenie czy jakkolwiek mieści się ona w charakterystyce informacji publicznej, ale także czy złożony wniosek winien być rozpoznawany w trybie mającym na uwadze zasady prywatności zgodnie z art. 51 Konstytucji RP. Organ władzy publicznej powinien zbadać charakter danych oraz udostępniać te, które odpowiadają wymogom ustawy. Zważając na art. 51 Konstytucji RP, organ nie ma możliwości odmowy dostępu do dokumentów i zbiorów danych, w szczególności tym osobom, których informacje te dotyczą. Należy zważyć, że ustalenie tożsamości osoby wnioskującej wpływa na zakres upowszechnionej informacji.

Przyjmując, że do informacji publicznej mogą zostać niekiedy przyporządkowane informacje o charakterze prywatnym, to sytuacja ta motywuje zastosowanie każdej

[407] Krytyce poddaje to m.in. Kamila Tarnacka, podnosząc, iż wymienione postanowienia Konstytucji RP trzeba interpretować jako samodzielne prawa podmiotowe. Zob. K. Tarnacka, *Prawo do informacji w Polsce,* „Państwo i Prawo" 2003, nr 5, s. 69-70.
[408] E. Kulesza, *Prawo obywateli do informacji o działalności podmiotów publicznych,* [w:] *Wolności i prawa jednostki oraz ich gwarancje w praktyce,* red. J. Wiśniewski, Warszawa 2006, s. 183.
[409] Wyrok TK z dnia 20 marca 2006 r., sygn. akt: K 17/05, OTK-A 2006, nr 3, poz. 30.

z konstytucyjnych regulacji w zakresie dostępu do informacji. Określenie informacji jako publicznej sprawi, że dojdzie do kolizji przepisów Konstytucji RP o dostępie do informacji różnego rodzaju. Prawdziwe zdaje się być stwierdzenie, że w jednakowym stopniu udzielenie informacji uzasadniać będą postanowienia art. 61 Konstytucji RP, jako regulującego w ogólnikowy sposób zakres dostępu do informacji publicznych, jak i te z art. 51 ust. 3 Konstytucji RP w takim zakresie, w jakim obejmują one dostęp do informacji publicznych. Na gruncie ustawy zasadniczej dochodzi do zbiegu podstawowych praw człowieka, tj. mając tu na myśli ochronę prywatności, w tym dane osobowe i wolność wypowiedzi, w tym prawo do otrzymywania i rozpowszechniania informacji[410]. W momencie wystąpienia kolizji interesów, to na organie państwowym lub na sądzie ciąży obowiązek zbadania danej sprawy, a tym samym dookreślenie, jakie dobra należy uwzględnić, a jakie ograniczyć. Sprzeczność praw człowieka różni się od konfliktu praw człowieka z dobrami społecznymi. K. Wojtyczek uzasadnia to w ten sposób, że „realizacja praw człowieka jest podstawowym celem państwa, prawa człowieka mają pierwszeństwo przed innymi wartościami konstytucyjnymi, przyznanie pierwszeństwa tym ostatnim jest możliwe tylko w szczególnych okolicznościach. W przypadku kolizji dwóch praw człowieka brak jest ogólnej jednej zasady, wskazującej, które z kolidujących wartości stoją wyżej w hierarchii i mają pierwszeństwo”[411]. Występujące kolizje można rozstrzygać na różne sposoby. Jednym z nich jest przyznawanie pierwszeństwa prawu na podstawie rangi aktu prawnego, w którym wyartykułowane są ograniczenia wykonywania tego prawa. Innym jest przyznanie pierwszego miejsca temu mniej ograniczonemu uprawnieniu. Jeśli chodzi o sądy powszechne, to nie opierają się na żadnej z tych zasad. Zawsze jednak badają, jakie prawo zostało naruszone i z jaką intensywnością. Wymiar sprawiedliwości wychodzi z założenia, że ustalanie ograniczeń zależy od konkretnej sytuacji i nie można stosować metod o ogólnym charakterze[412].

Prawa człowieka zagwarantowane konstytucyjnie mają pierwszeństwo przed prawem pozakonstytucyjnym. Rozstrzyganie zbiegu przepisów prowadzi do poświęcenia tego dobra, które zajmuje niższy poziom w subiektywnie przyjętej hierarchii wartości. Umożliwia to ochronę innych praw, aniżeli jedynie prawa do informacji. Rozwiązywanie kolizji może opierać się na generalnej systematyce ustawy zasadniczej oraz interpretacji konstytucyjnych regulacji wraz z uwzględnieniem charakteru informacji, która ma podlegać rozpowszechnieniu. Zbieg przepisów jest nie do uniknięcia z uwagi na naturę informacji

[410] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…,* s. 205.
[411] K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka…,* s. 198.
[412] B. Banaszak, *Zagadnienia podstawowe. Terminologia,* [w:] *System ochrony praw człowieka*, red. B. Banaszak, A. Bisztyga, K. Complak, M. Jabłoński, R. Wieruszewski, K. Wojtowicz, Kraków 2003, s. 51.

jawiącą się jako dobro niematerialne, gdzie jej ochrona jest stopniowalna i zależy od podmiotu i interesu, jakiemu służy. Nie każda informacja publicznie dostępna może zostać scharakteryzowana jako informacja publiczna. Jej dostępność umożliwiają postanowienia Konstytucji RP inne niż te z art. 61 ustawy zasadniczej. Ujawnieniu podlegają zatem informacje o charakterze publicznym, podczas gdy pozostałe określane są jako informacje prywatne. Publiczne udostępnienie informacji o charakterze prywatnym nie powinno być wynikiem swobodnego uznania, lecz następstwem zgody udzielonej przez jej dysponenta.

Prawo do uzyskiwania informacji jest wiążące dla organów władzy w zakresie podejmowania oznaczonych czynności faktycznych. Zauważa się, iż obowiązek działania administracji ma dwojaki charakter, tj. czynne oraz bierne informowanie. Informowanie czynne polega na tym, że to po stronie administracji leży zapewnienie obywatelom dostępu do informacji. Informowanie bierne sprowadza się do tego, że organ administracji jedynie odpowiada, przekazuje informacje żądanej treści. Z tego wynika, że obowiązek informacyjny sprowadza się zarówno do działania, jak i powstrzymywania się przed działaniem poprzez znoszenie ingerencji z zewnątrz, jeżeli obywatel wyrazi wolę skorzystania z przysługującego mu prawa do informacji[413]. Istotą obowiązku informacyjnego jest więc bezwzględność, co oznacza, że nie aktualizuje się on dopiero w chwili zgłoszenia przez uprawnioną osobę należytego żądania. Obowiązek ten jest jednocześnie przejawem bezpośredniego zastosowania norm Konstytucji RP w sferze wolności i praw człowieka[414]. Uzyskanie informacji może nastąpić w drodze powołania się na regulacje różnych ustaw, ale też i przepisów konstytucyjnych. Zawierają one szczegółowe, a zarazem inne unormowania dotyczące trybu dostępu do informacji, zaś w przypadku prawa do autonomii informacyjnej odmienne regulacje w zakresie przedmiotowym udostępnianych informacji. Stąd nie można przyjąć, że dostęp do informacji jest regulowany w oparciu o jedno ogólne prawo podmiotowe, które zostało określone w art. 61 Konstytucji RP. Chybione wydaje się również stwierdzenie, że art. 51 Konstytucji RP stanowi jedynie uzupełnienie generalnego prawa do informacji, ponieważ raczej posiada równorzędną moc prawną[415].

Dostęp do informacji jest postrzegany jako instytucja prawna, której odzwierciedleniem są prawa podmiotowe w Konstytucji RP, uzupełniane w ustawodawstwie

[413] M. Mucha, *Obowiązki administracji publicznej…,* s. 91.
[414] A. Błaś, *Rodzaje źródeł prawa administracyjnego,* [w:] *Prawo administracyjne,* red. J. Boć, Wrocław 2010, s. 63.
[415] A. Szmyt, *W sprawie interpretacji art. 61 Konstytucji RP z 2 kwietnia 1997 roku,* „Przegląd Sejmowy" 1999, nr 6, s. 68.

zwykłym. Prawo do informacji wymaga szeroko pojętej działalności prawodawczej[416]. Umiejscowienie dostępu do informacji w ustawie zasadniczej wskazuje na znaczenie, jakie ustrojodawca nadał temu prawu w systematyce praw i wolności. Skupił się na okolicznościach faktycznych i prawnych, w których może znajdować się osoba żądająca udzielenia informacji. Rozwiązania konstytucyjne rodzą potrzebę odrębnego unormowania w ustawodawstwie zwykłym tych sytuacji, gdzie obywatel zajmuje przeciwstawne miejsce w stosunku do władzy publicznej z uwagi na podejmowane przez niego prawo do informacji.

Nieco inaczej kształtuje się możliwość ograniczenia prawa dostępu do urzędowych dokumentów i zbiorów danych, wykonywanego przez osobę, której to dotyczy, zagwarantowanego w art. 51 ust. 3 Konstytucji RP. Prawo przysługujące każdej jednostce do uzyskania dostępu do informacji z nią związanych, będących w posiadaniu osób postronnych, które przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową albo dla realizacji celów statutowych, stanowi jeden z aspektów prawa do ochrony prywatności. Zwraca się uwagę, iż składa się ono na realizację prywatności informacyjnej, która to oznacza uprawnienie jednostki do kontrolowania treści i obiegu informacji z nią związanych[417]. Prawo do informacji o zawartych w zbiorach urzędowych danych dotyczących konkretnego podmiotu zalicza się do kategorii prawa do informacji publicznej tejże osoby, w takim jednak zakresie, w jakim zbiory te prowadzone są przez organy o charakterze publicznym. Teza ta może budzić wątpliwości, ponieważ gromadzenie i przetwarzanie informacji przez organy władzy publicznej nie prowadzi do przyjęcia stanowiska, że każda informacja znajdująca się w posiadaniu tych organów jest publiczna. Możliwe natomiast będzie żądanie przez osobę, której informacja dotyczy dostępu do niej na podstawie art. 51 ust. 3 Konstytucji RP, jak też domaganie się sprostowania i usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą, co z kolei zagwarantowane jest w ust. 4. O ile adresatem żądania dostępu do informacji lub dokonania jej korekty jest organ władzy publicznej, prawo do informacji będzie przybierać charakter publicznego prawa podmiotowego, którego nie należy utożsamiać z dostępem do informacji publicznych w rozumieniu art. 61 ustawy zasadniczej. Informacje, których zdobycie zapewniają normy art. 51 Konstytucji RP z reguły nie stanowią informacji o charakterze publicznym. Przyjęcie bowiem takiego założenia niewątpliwie przeczyłoby zasadzie racjonalności tych przepisów

[416] A. Bałaban, *Opinia w sprawie interpretacji art. 61 Konstytucji RP z 2 kwietnia 1997 r.,* „Przegląd Sejmowy" 1999, nr 6, s. 64.
[417] P. Litwiński, *Zasada autonomii informacyjnej w orzecznictwie Trybunału Konstytucyjnego a stosowanie przepisów o ochronie danych osobowych,* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia,* red. P. Fajgielski, Lublin 2008, s. 170.

Konstytucji RP, których celem jest ochrona prywatności jednostki, a zatem realizacji postanowień z art. 51 Konstytucji RP.

Informacje zawarte w urzędowych dokumentach i zbiorach danych, do których dostęp na podstawie regulacji art. 51 Konstytucji RP uzyskuje osoba zainteresowana, mogą wchodzić w zakres informacji publicznych, gdy nie tylko w aspekcie podmiotowym[418], ale także i przedmiotowym[419] wypełniają przesłanki z art. 61 Konstytucji RP. Na tej podstawie nie można zaprzeczyć, że informacje zawarte w urzędowych dokumentach i zbiorach będą podlegać udostępnieniu nie tylko tym osobom, których informacje te dotyczą, ale także zostaną udostępnione innym osobom jako informacje o sprawach publicznych.

Mając na uwadze, że Konstytucja RP nie rozstrzyga w jednoznaczny sposób o prymacie prawa do informacji nad innymi wartościami prawnie chronionymi, wykorzystywanie regulacji z zakresu dostępu do informacji wymaga określenia charakteru udostępnionej informacji oraz możliwości jej udostępnienia w oparciu o treść regulacji ustawowych i konstytucyjnych, a zarazem wymaga rozważenia interesów, którym służy. Prawo do informacji kwalifikuje się do publicznego prawa podmiotowego, nie dlatego, że jego wykonanie opiera się na przymusie państwowym, a podmiotem zobowiązanym są organy władzy publicznej, lecz dlatego że udostępnienie informacji leży w interesie publicznym[420].

1.4. Oddziaływanie prawa do prywatności na autonomię informacyjną jednostki

1.4.1. Związek zakresu podmiotowego prawa do ochrony danych osobowych z prawem do prywatności

W rozdziale drugim Konstytucji RP, w którym zawarto prawo do ochrony danych osobowych wskazano, że uregulowane tam prawa, wolności i obowiązki przysługują człowiekowi lub obywatelowi[421]. Rozróżnienie to jest przemyślanym zabiegiem, który ma na celu odróżnić prawa przysługujące każdemu człowiekowi bez względu na jego przynależność państwową czy pozycję społeczną od uprawnień przyznanych obywatelowi państwa polskiego. Inaczej mówiąc, pozwala na dostrzeżenie rozbieżności w zestawieniu z prawami

[418] Zostały zgromadzone lub podlegają przetworzeniu przez organ władzy publicznej.
[419] Nawiązują do działalności organów władzy publicznej oraz osób pełniących funkcje publiczne.
[420] J. Taczkowska-Olszewska, *Dostęp do informacji…,* s. 98.
[421] A. Młynarska-Sobaczewska, *Konstytucyjne wskazania podmiotów praw człowieka,* „Studia Prawno-Ekonomiczne" 2004, tom 70, s. 49.

o charakterze publicznym, określających relacje między jednostką a państwem[422]. Terminologia zastosowana w ustawie zasadniczej pozwala na odróżnienie praw człowieka od praw obywatela. Jeżeli realizacja danego uregulowania zależna jest od posiadania obywatelstwa polskiego, to Konstytucja RP posługuje się terminem „obywatel" lub „obywatel polski". Dualizmowi konstytucyjnemu praw i wolności trzeba nadać głębszy sens. W oparciu o kryterium podmiotowe, ustrojodawca wyraźnie wskazał istnienie przysługujących każdemu człowiekowi powszechnych partykularnych praw (wolności) oraz praw (wolności) obywatelskich w tym sensie, że są one skierowane nie do każdego człowieka, lecz tylko do tego, który ma polskie obywatelstwo[423].

Uniwersalne założenia co do podmiotowego zakresu prawa do ochrony danych osobowych, zwykło się wywodzić z systematyki tego prawa pośród konstytucyjnych praw i wolności osobistych, które mają służyć wszystkim podmiotom bez względu na posiadaną przez nich przynależność państwową[424]. Do analogicznej konkluzji skłania świadomość zależności zachodzącej pomiędzy art. 47 a 51 Konstytucji RP, która zakłada, że autonomia informacyjna jest jednym z komponentów prawa do prywatności w szerokim tego słowa znaczeniu[425], a prawo to zostało ukształtowane jako prawo należne każdemu, niezależnie od obywatelstwa lub innego kryterium wyodrębnienia jednostki ze zbiorowości ludzkiej. Należy mieć jednak na uwadze, iż art. 51 ustawy zasadniczej ustanawia partykularne uprawnienia wobec prawa do prywatności, stanowiąc konkretyzację tego prawa w kategoriach proceduralnych, dlatego też krąg adresatów może kształtować się zgoła odmiennie[426]. Poprzez wykorzystanie terminu „nikt" dla określenia zakresu podmiotowego przepisu, art. 51 ust. 1 Konstytucji RP zapewnia każdej jednostce, bez względu na jej obywatelski status, uprawnienie do samodzielnego i autonomicznego decydowania o ujawnianiu informacji o sobie[427]. Polski ustrojodawca, odnosząc się do zagadnienia ochrony danych osobowych, nie posłużył się bezpośrednio takim zwrotem, lecz określeniem „informacje dotyczące osoby". Informacja dotycząca osoby fizycznej zachowuje swój osobowy charakter do momentu, dopóki jest możliwe ustalenie tożsamości konkretnej osoby, której dotyczy informacja.

Równie szeroko, krąg uprawnionych podmiotów zarysowano w sytuacji art. 51 ust. 3

---

[422] W. Skrzydło, *Konstytucyjny katalog wolności i praw jednostki,* [w:] *Konstytucyjne wolności i prawa w Polsce. Zasady ogólne,* red. M. Chmaj, tom I, Kraków 2002, s. 53.
[423] A. Wróbel, *Obywatelstwo polskie a prawa i wolności konstytucyjne,* [w:] *Konstytucyjne wolności i prawa w Polsce. Zasady ogólne,* red. M. Chmaj, tom I, Kraków 2002, s. 154.
[424] B. Banaszak, *Prawo konstytucyjne,* Warszawa 2001, s. 428.
[425] Wyrok TK z dnia 20 listopada 2002 r., sygn. akt: K 41/02…
[426] Wyrok TK z dnia 19 maja 1998 r., sygn. akt: U 5/97…
[427] M. Wyrzykowski, *Status informacyjny obywatela,* [w:] *Prawo i ład społeczny. Księga ku czci profesor Anny Turskiej,* Warszawa 2000, s. 249.

i 4 Konstytucji RP, gdzie posłużono się pojęciem „każdy", co jest odpowiednikiem terminu „człowiek" dla wskazania podmiotu, który ma odpowiednio prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, jak też do zgłoszenia żądania sprostowania i usunięcia informacji niezgodnych z prawdą, niepełnych, bądź zebranych w sposób sprzeczny z aktem rangi ustawowej.

Nieco inaczej jest w przypadku zakresu art. 51 ust. 2 Konstytucji RP, na podstawie którego władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach, aniżeli te, które są niezbędne w demokratycznym państwie prawa. W związku z tym, można byłoby przyjąć, że władzom publicznym przysługuje prawo poddawania procesowi przetwarzania takich informacji, które dotyczą osób innych niż obywatele, przy czym dane te nie muszą jednocześnie wypełniać kryterium niezbędności w demokratycznym państwie prawnym[428]. Zastanawiając się nad powodem tego rozróżnienia, można przyjąć, że ustrojodawca miał na celu zawężenie kręgu podmiotów tego prawa do określonej kategorii osób fizycznych, gdyż to właśnie potraktował obywatela jako uprzywilejowanego z uwagi na ograniczenie możliwości pozyskiwania, gromadzenia i udostępniania informacji na jego temat za pośrednictwem władzy publicznej[429]. Definicja obywatelstwa poddana została w doktrynie prawa publicznego, w szczególności międzynarodowego, konstytucyjnego i administracyjnego szerszej analizie[430]. Obywatelstwo można określić tradycyjnie jako węzeł prawny łączący osobę fizyczną z krajem, w którym duży nacisk kładzie się na prawną przynależność jednostki do państwa albo inaczej jako status prawny jednostki, z jakim wiąże się posiadanie zespołu praw i obowiązków[431]. Konkretyzując, trzeba uznać, że obywatelstwo jest takim stosunkiem prawnym, który łączy daną osobę z państwem, a z jego posiadaniem wiążą się określone prawa i obowiązki publicznoprawne[432]. Na marginesie, obywatelstwo nie jest tożsame z przynależnością narodową, ponieważ obywatelem polskim może być osoba niepolskiej narodowości, a osoba narodowości polskiej może być obywatelem obcego kraju[433].

Na tle art. 51 ust. 2 Konstytucji RP, w doktrynie prawa pojawiły się dwa odmienne poglądy. Według Ewy Kuleszy, w nawiązaniu do prawa do ochrony danych osobowych,

[428] K. Wygoda, *Ochrona danych osobowych i prawo do informacji…,* s. 404.
[429] M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice…,* s. 222.
[430] M. Banaś, A. Krzywonos, *Prawo do obywatelstwa,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* Warszawa 2002, s. 157.
[431] B. Stępień-Załucka, *Wolności i prawa człowieka oraz obywatela w Konstytucji RP z dnia 2 kwietnia 1997 r. Zagadnienia wybrane,* Rzeszów 2021, s. 77.
[432] L. Garlicki, *Uwaga 5 do art. 34 Konstytucji,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, tom 3, Warszawa 2003, s. 4.
[433] A. Wróbel, *Obywatelstwo polskie…,* s. 411-412.

gwarancje zawarte w art. 51 ustawy zasadniczej, powinny odnosić się do wszystkich osób, a nie jedynie do obywateli Rzeczypospolitej Polskiej, gdyż nie ma podstaw do różnicowania prawa do ochrony danych osobowych od posiadanego obywatelstwa przez osobę przebywającą na terytorium RP, zwłaszcza, że prawo do ochrony danych osobowych wywodzące się z prawa do prywatności nie jest prawem związanym wyłącznie z obywatelstwem. Zasada, że prawo do ochrony danych przysługuje każdemu potwierdzona została w większości sformułowań użytych w art. 51 Konstytucji RP[434]. Stanowisko to wydaje się logiczne. Posługując się terminem „obywatel", podkreślono jedynie znaczenie danego prawa, nie odbierając go pozostałym osobom fizycznym[435].

Zgodnie z drugim z poglądów, wyrażonym przez Mirosława Wyrzykowskiego, mamy do czynienia z co najmniej kilkoma adresatami treści zawartych w art. 51 Konstytucji RP. Pierwszym z nich jest każdy, bez względu na posiadane obywatelstwo. Jednostce tej przysługuje prawo do nieujawniania informacji jej dotyczących, chyba że taki obowiązek wynika z aktu prawnego rangi ustawowej. Drugim z nich na podstawie ust. 2 art. 51 Konstytucji RP jest obywatel polski, o którym władze publiczne mogą pozyskiwać, gromadzić i udostępniać informacje niezbędne w demokratycznym państwie prawnym. Skutkiem tego pogrupowania jest nieumiejętność wskazania zakresu informacji, którymi mogą dysponować władze publiczne. Pojawia się pytanie, czy władze publiczne posiadają prawo do pozyskiwania, gromadzenia i upowszechniania informacji o osobach, które nie są obywatelami państwa polskiego. Tego przepisu Konstytucji RP nie można interpretować jako zakazu pozyskiwania, gromadzenia i udostępniania informacji przez stosowne władze publiczne o innych obywatelach niż obywatele polscy. Jednocześnie nasuwają się pewne wątpliwości, czy można gromadzić informacje o osobach innych niż obywatele, ponieważ treść art. 51 ust. 2 Konstytucji RP może wskazywać na dopuszczalność pozyskiwania, gromadzenia i udostępniania danych tylko o obywatelach polskich oraz niemożność takiego działania w stosunku do obywateli państw obcych[436].

W obu powyżej wyrażonych stanowiskach poruszono jedynie część tego zagadnienia.

---

[434] Autorka wprawdzie odnosi się do tego, że art. 51 ust. 2 Konstytucji RP posługuje się zwrotem „informacje o obywatelach", ale żadne demokratyczne państwo nie ma prawa w dowolny i w nieuzasadniony sposób gromadzić oraz wykorzystywać danych osób niebędących obywatelami. W związku z tym, propaguje ona, aby w przyszłości zmodyfikować art. 51 ust. 2 Konstytucji RP i rozstrzygnąć w niewątpliwy sposób wszystkie regulacje w ramach ochrony danych osobowych każdego podmiotu przebywającego na terytorium RP. Zob. E. Kulesza, *Konstytucyjne prawo do ochrony danych osobowych i jego ustawowa realizacja,* „Human Rights HZN" 2000, nr 7, s. 106.

[435] Z. Kędzia, *Pojęcie „prawa i wolności obywatelskie" (Uwagi na tle ustawy o Rzeczniku Praw Obywatelskich),* „Państwo i Prawo" 1989, z. 3, s. 26-27.

[436] M. Wyrzykowski, *Ochrona danych osobowych,* Warszawa 1999, s. 25.

Pierwsze pomija zasadę racjonalności prawodawcy, a ingerencja państwa w sferę praw człowieka powinna się na niej opierać i dążyć do jej realizacji[437]. Abstrahuje się w nim od poszukiwania uzasadnienia dla zasadności użycia w treści art. 51 ust. 2 Konstytucji RP terminu „obywatel". Wyeksponowany jest zaś postulat zharmonizowania konstytucyjnej terminologii tak, aby nie było żadnych wątpliwości co do szeroko zarysowanego kręgu podmiotów, którym służą gwarancje z art. 51 Konstytucji RP. Dualizm praw konstytucyjnych, oparty na podmiotowym kryterium, został wprowadzony przez ustrojodawcę w sposób świadomy, ponieważ jego zamiarem było zawężenie kręgu podmiotów prawa do określonej grupy osób, w tym przypadku do obywateli, zaznaczając to w treści przepisu[438]. Drugi zaś z przytoczonych poglądów może prowadzić do zbyt daleko posuniętych wniosków. Wiele zadań podejmowanych przez państwo wymaga pozyskiwania, gromadzenia i udostępniania danych osób niebędących obywatelami polskimi. Prawo do przetwarzania danych przez polskie władze publiczne znajduje podstawę w przepisach prawa i służy interesowi osób, których dane dotyczą. Podczas wykładni art. 51 ust. 2 Konstytucji RP nie może zabraknąć odwołania do ust. 5, który uważa się za integralną część konstytucyjnej regulacji prawa do ochrony danych osobowych. Umiejscowienie przepisu o tym brzmieniu na końcu art. 51 ustawy zasadniczej oznacza, że jego postanowienia należy odnosić do wszystkich poprzednich ustępów. Ustęp 5 art. 51 ustawy zasadniczej pozostaje niejako zbieżny z pozostałymi uregulowaniami, a nawet je dookreśla.

Nawiązując do konstytucyjnego standardu ochrony danych osobowych z art. 51 ustawy zasadniczej, można zauważyć, że wprost wskazano na aspekt ochrony danych osobowych, rozumiany jako jeden z kilku, poprzez który zapewnione jest prawo do prywatności regulowane w art. 47 Konstytucji RP. Art. 51 Konstytucji RP gwarantuje zabezpieczenie ochrony danych osobowych na szczeblu konstytucyjnym. Gwarancje wskazane na gruncie tego przepisu odnoszą się do wszystkich osób fizycznych, a nie tylko do obywateli polskich, z wyjątkiem unormowań z art. 51 ust. 2 ustawy zasadniczej. Pogląd ten jest szczególnie uzasadniony w sytuacji, jeżeli te gwarancje zinterpretuje się w powiązaniu z art. 47 Konstytucji RP, dotyczącym prawa do prywatności przysługującego wszystkim osobom fizycznym[439]. O tym, iż gwarancje ochrony danych osobowych z art. 51 ustawy zasadniczej dotyczą wszystkich osób fizycznych przesądza okoliczność dwukrotnego użycia

[437] J. Wróblewski, *Teoria racjonalnego tworzenia prawa,* Wrocław-Warszawa-Kraków-Gdańsk-Łódź 1985, s. 134.
[438] K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka…,* s. 137.
[439] A. Zwara, A. Mednis, M. Pisz, *RODO. Przewodnik dla adwokatów i aplikantów adwokackich,* Warszawa 2018, s. 6-7.

przez ustrojodawcę sformułowania „każdy". Regulacje, sformułowane w oparciu o ten przepis i odczytywane w powiązaniu z ogólnymi gwarancjami prawa do prywatności z art. 47 Konstytucji RP, powinny być rozpatrywane w kategoriach praw i wolności człowieka i obywatela. Jak łatwo zauważyć, tym określeniem nie posłużono się w całym artykule. Wskazując na krąg podmiotów, które mogą być obowiązane w inny sposób niż na podstawie ustawy do ujawniania informacji dotyczących osoby, użyto wprost sformułowania „nikt". Może być ono rozumiane jako „każdy", a więc skierowane do wszystkich osób fizycznych.

Ze względu na swój charakter, regulacje wynikające z art. 51 Konstytucji RP dotyczą jedynie osób fizycznych. Niezależnie od tego, art. 51 Konstytucji RP nie ogranicza się tylko do gwarancji ochrony danych osobowych, ale też zapewnia ochronę prywatności w szerszym zakresie.

W związku z tymi ustaleniami, odróżnienia praw i wolności człowieka od praw i wolności obywatela należy dokonywać ze względu na podmiot uprawniony. Założenie to nie należy do prostych i oczywistych, ponieważ z jednej strony bierze się pod uwagę, że przyrodzona i niezbywalna godność człowieka jest źródłem praw i wolności człowieka i obywatela, z drugiej zaś strony, szukanie zasadniczej różnicy pomiędzy prawami i wolnościami człowieka a obywatela może z czasem okazać się zbyt problematyczne i czasochłonne. Konstytucja RP nie daje powodów do przyjmowania wewnętrznej hierarchii praw i wolności. Dla tych praw i wolności wspólne jest to, że wyrastają z godności człowieka, która jest dla nich ostatecznym uzasadnieniem, jak i to, że podmiotem tych praw i wolności jest człowiek, lecz w odniesieniu do praw i wolności obywatelskich, człowiek ze względu na swój status obywatela[440]. Z tego też wynika, że prawodawca dostrzega potrzebę zaakcentowania, że określone w art. 51 ust. 2 Konstytucji RP zasady przetwarzania danych osobowych powinny odnosić się przede wszystkim do obywateli, ale w żadnym wypadku nie oznacza to, że konstytucyjne prawo do ochrony danych osobowych nie przysługuje cudzoziemcom, bowiem wręcz przeciwnie, im także to prawo jest zapewniane. Wskazane jest zwrócenie uwagi na odnoszący się bezpośrednio do obywateli art. 51 ust. 2 ustawy zasadniczej, lecz należy przy tym pamiętać, że ograniczenia dotyczące cudzoziemców mogą być wprowadzane wyłącznie w drodze ustawy i mają za zadanie mieścić się w granicach wyznaczanych przez art. 31 ust. 3 Konstytucji RP. Za znacznie poważniejszy problem uchodzi zagadnienie związane z tym, czy do cudzoziemców mogą być odnoszone reguły postępowania, o których mowa w art. 51 ust. 2 Konstytucji RP. Zdaniem specjalistów

[440] A. Wróbel, *Obywatelstwo polskie a prawa i wolności konstytucyjne…,* s. 154.

z zakresu ochrony danych osobowych, nie istnieją żadne przeciwwskazania do stosowania tych postanowień, również do informacji o cudzoziemcach, tym bardziej, że o końcowej ochronie w stosunku do tej kategorii podmiotów decydują przepisy aktu prawnego rangi ustawowej, które siłą rzeczy muszą mieścić się w założeniach art. 31 ust. 3 i art. 51 ust. 2 Konstytucji RP[441]. Przypadek, w którym konkretne prawo należy do grupy praw i wolności obywatela, nie może być traktowany na równi z tym, że ustawodawca nie ma uprawnień do rozszerzenia jego zakresu podmiotowego na cudzoziemców[442]. Pozostaje to w zgodzie z respektowanymi przez współczesne kraje demokratyczne założeniami opierającymi się na tezie, że osobom nieposiadającym danego obywatelstwa przysługują takie same prawa i obowiązki, jak obywatelom, a jakiekolwiek odstępstwa od tej zasady są jedynie wyjątkami. Zatem zauważa się zanik różnicowania statusu obywatela i cudzoziemca. Przy stosowaniu prawa do ochrony danych osobowych nie ma to większego znaczenia. Ochrona danych osobowych odchodzi w kierunku uniwersalnej kategorii praw i wolności człowieka. Analiza art. 51 Konstytucji RP prowadzi do wniosku, że regulacje wynikające z tego przepisu mają zastosowanie wobec wszystkich osób znajdujących się pod władztwem Rzeczypospolitej Polskiej i nie są uzależnione od spełnienia przez osobę fizyczną jakichkolwiek warunków[443].

Należy równocześnie zwrócić uwagę, że art. 51 ustawy zasadniczej obejmuje szeroki zakres podmiotów zobowiązanych do urzeczywistnienia gwarancji ochrony danych osobowych i nawiązuje nie tylko do władz publicznych, ale też do podmiotów niepublicznych, inaczej mówiąc – prywatnych. Istotny z punktu widzenia tego zagadnienia jest wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2002 roku, gdzie wywiedziono, że „prawodawca konstytucyjny w art. 51 ustawy zasadniczej kładzie nacisk przede wszystkim na ochronę jednostki wobec władz publicznych. W ustępie 2 jako podmiot zobowiązany do realizacji prawa wskazano władzę publiczną. 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 konstytucyjny dotyczy wszelkich przypadków, w których jednostka zobowiązana zostaje do ujawniania informacji o sobie innym podmiotom, a więc także podmiotom prywatnym. W świetle art. 47 Konstytucji RP nie ulega jednak wątpliwości, że ustawodawca ma konstytucyjny obowiązek zapewnić jednostce odpowiednią ochronę sfery prywatności nie tylko przed ingerencją ze strony podmiotów publicznych, ale również przed ingerencją ze strony innych jednostek i podmiotów

[441] M. Sakowska-Baryła, *Prawo do ochrony danych…,* s. 109.
[442] B. Banaszak, *Prawo konstytucyjne,* Warszawa 2004, s. 460.
[443] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…,* s. 95.

prywatnych”[444].

1.4.2. Relacje zachodzące pomiędzy prawem do ochrony danych osobowych a prawem do prywatności

Zagadnienie dóbr podlegających ochronie z punktu widzenia stosowania przez administrację zbiorów danych osobowych jest związane z ochroną prawa podmiotowego, jakim jest prawo do prywatności oraz ochrona dóbr osobistych na gruncie prawa cywilnego. Zdaniem A. Mrozka, każdemu przysługuje prawo do tworzenia obrazu własnej osoby i decydowania o tym, jakie informacje dotyczące siebie pragnie rozpowszechnić[445]. Elektroniczne gromadzenie danych umożliwia korzystanie z informacji o życiu osobistym człowieka. W literaturze podnoszono, że działania podejmowane przez administrację są celowe, niezbędne dla należytej organizacji i funkcjonowania życia społecznego. Nie powinny one jednak wykraczać poza granice uzasadnionych potrzeb oraz funkcji, które spełniają, natomiast możliwość zastosowania należytego roszczenia wywodzącego się z prawa cywilnego i ochrony prywatności nie może budzić wątpliwości[446].

Prawo do prywatności można porównać do prawa do bycia pozostawionym w spokoju. Przejawia się ono w ten sposób, że każdemu przysługuje prawo do tego, aby nie być niepokojonym w życiu prywatnym przez podmioty publiczne i niepubliczne. Zakazana ingerencja w życie prywatne ma najczęściej miejsce w momencie niedozwolonego gromadzenia i dysponowania danymi dotyczącymi jednostki, niezależnie od przyjętej formy. Naruszenie prawa do prywatności ma miejsce, gdy dane osobowe są w sposób zabroniony gromadzone, nawet jeżeli są one prawdziwe. Prawo do prywatności i prawo do informacji rodzą pewien paradoks współczesnego świata. Człowiek siłą rzeczy jest coraz większym konsumentem informacji. Mimo to, mając na uwadze coraz to większą dostępność do informacji, chce bardziej chronić obszar swojej prywatności[447].

Prawo do ochrony danych osobowych rozwija prawo do prywatności, jest jego pochodną. Przyjęcie, że ochrona danych osobowych wywodzi się z prawa do prywatności jest zjawiskiem dość powszechnym. Nie jest to pozbawione podstaw, bowiem zważając na szerokie rozumienie terminologii prawa do prywatności, można z całą stanowczością

[444] Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01…
[445] A. Mrózek, *Prawno-polityczne problemy funkcjonowania banków danych w państwach burżuazyjnych,* „Państwo i Prawo” 1976, nr 8-9, s. 33.
[446] K.W. Kubiński, *Ochrona życia prywatnego człowieka…,* s. 68.
[447] M. Safjan, *Ochrona danych osobowych-granice autonomii informacyjnej,* [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa 1999, s. 11.

sformułować przekonanie, że zagadnienie ochrony danych osobowych wchodzi w zakres tego pierwszego prawa. Wobec tego, wszelkie naruszenia danych osobowych godzą także w chronione dobro, jakim jest prywatność. Zagrożenia te wyodrębniły się w dobie postępującego procesu cywilizacji i przejawiają się w niebezpieczeństwie dla sfery prywatności w postaci prywatności informacyjnej.

W art. 47 Konstytucji RP ustrojodawca obejmuje ochroną życie prywatne, rodzinne i osobiste. Dopiero w następnych przepisach konkretyzuje gwarancje ochrony prawa do prywatności ogólnie uregulowanego[448]. Związek, jaki istnieje pomiędzy prawem do prywatności a ochroną danych osobowych kształtuje się jako związek materialny. Ochrona prywatności w dużej mierze jest współzależna od ochrony danych osobowych, które dotyczą jednostki. W judykaturze Trybunału Konstytucyjnego prawo do autonomii informacyjnej z art. 51 ustawy zasadniczej jest uszczegółowioną konstrukcją, jaka służy ochronie tych samych wartości, które zostały określone w art. 47 Konstytucji RP. W ust. 2 art. 51 Konstytucji RP konkretyzuje prawo do prywatności w aspektach proceduralnych[449]. W odniesieniu do ochrony danych osobowych chodzi o podkreślenie środków organizacyjnych i technicznych, a także uwydatnienie autonomii jednostki w wykonywaniu przysługującego jej prawa do prywatności[450].

Ustrojodawca odrębnie uregulował prawo do ochrony danych osobowych od prawa do prywatności, ponieważ dostrzegał niebezpieczeństwo dla jednostki i tym samym pojawiła się z jego strony chęć zabezpieczenia tej wolności[451]. Dokonując analizy relacji występujących pomiędzy prawem do prywatności a prawem do ochrony danych osobowych, należy zwrócić szczególną uwagę na miejsce ich występowania w systematyce Konstytucji RP. Oba te prawa poprawnie zostały zaliczone do wolności i praw osobistych, a więc takich, dla których fundamentem nie jest wola państwa, ale przyrodzona godność człowieka. Zależność ochrony danych osobowych od godności człowieka nie powinna wiązać się tylko ze stwierdzeniem, że jest ona fundamentem wolności i praw zagwarantowanych w Konstytucji RP. Oba prawa, zarówno prawo do ochrony danych osobowych, jak i prawo do prywatności przyczyniają się do zagwarantowania poszanowania godności człowieka. Zatem godność jest wspólnym

[448] L. Szymańska, *Prawo do ochrony życia prywatnego na podstawie art. 47, 49-51 Konstytucji RP-wybrane zagadnienia,* [w:] *Polska wobec europejskich standardów praw człowieka,* red. T. Jasudowicz, Toruń 2001, s. 139.
[449] Wyrok TK z dnia 19 maja 1998 r., sygn. akt: U 5/97…
[450] M.-Th. Tinnefeld, *Ochrona danych osobowych-kamień węgielny budowy Europy,* [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa 1999, s. 35.
[451] K. Wygoda, *Ochrona danych osobowych i prawo do informacji…,* s. 400.

źródłem realizacji tych praw[452].

Gwarantując prawo do prywatności, nie można zezwalać organom władzy publicznej na dokumentowanie służącym własnym celom danych osobowych o indywidualnych właściwościach. Również do nagannego zachowania zalicza się zgłębianie zachowań osób prywatnych, czy przymuszanie ich do ujawniania swych cech oraz osobistego postępowania nie tylko władzy publicznej, ale komukolwiek. Wszystko to bierze swój początek z godności osoby ludzkiej, natury praw osobistych, prawa do prywatności i zasady demokratycznego państwa prawnego. W omawianym przypadku nie bez znaczenia jest konstytucyjny charakter prawa do prywatności. Dużą rolę odgrywa wertykalna relacja kształtująca się pomiędzy państwem a jednostką. Wiąże się to z tym, że dane osobowe jednostki podlegają zwiększonej ochronie przed nieodpowiednim działaniem organów władzy publicznej. Relacja horyzontalna zaś, występująca pomiędzy jednostkami, ma znaczenie drugorzędne. W ustawodawstwie zwykłym, ochrona prywatności, w tym danych osobowych przybiera postać zaniechania podejmowania różnorodnych czynności. Przejawiają się one m.in. w nieingerowaniu w obszar spraw intymnych, osobistych i rodzinnych, a także w pozostawieniu jednostki w spokoju i w nierozpowszechnianiu informacji odnoszących się do powyższych sfer[453].

Podstawową funkcją, jaką spełnia ochrona danych osobowych w demokratycznym państwie prawnym, jest zagwarantowanie prawa do prywatności. Z tego wynika, że odwołanie się do zasady demokratycznego państwa prawnego jest zasadnie umotywowane, pomimo odmiennego zdania wyrażonego w jednym z orzeczeń Trybunału Konstytucyjnego, które w swej istocie stanowi, że przyjęty przez Konstytucję RP szeroki katalog wolności i praw jednostki, obejmujący regulacje wyrażone w art. 47 i 51 ustawy zasadniczej nie wymaga uzupełnienia poprzez odwołanie się do art. 2 Konstytucji RP[454]. Zależność ochrony danych osobowych z zasadą demokratycznego państwa prawnego nie jest przypadkowa. Państwo prawa statuuje pewne standardy, wśród których znajduje się poszanowanie prywatności jednostki.

Zagwarantowanie prawa do prywatności ma kolosalne znaczenie w procederze wykorzystywania przepisów mających chronić dane osobowe. Ustrojodawca pozwolił na przetwarzanie danych osobowych, ograniczające prawo do prywatności, niemniej jednak tym

[452] Wyrok TK z dnia 30 października 2006 r., sygn. akt: P 10/06…
[453] M. Jagielski, *Konstytucjonalizacja ochrony prywatności…,* s. 275.
[454] Wyrok TK z dnia 19 maja 1998 r., sygn. akt: U 5/97…

samym je chroniąc. Ta konstytucyjna sprzeczność jest pozorna[455]. Konkretna osoba, korzystająca ze swojego prawa może decydować o tym, komu i które dane osobowe przekaże. Kwestią problematyczną mogą być przepisy ustawodawstwa zwykłego. To na ich podstawie jednostka może zostać zobowiązana do udostępnienia danych osobowych.

W nauce prawa można spotkać też zdania odmienne. Dokonując analizy systematyki przepisów art. 47 i 51 Konstytucji RP stwierdzono, że ochrona danych osobowych nie jest współzależna od prawa do prywatności, ponieważ są to dwa odrębne uregulowania. Ochrona prawa do prywatności wraz z ochroną danych osobowych nachodzą na siebie tylko w momencie, gdy pojawią się takie zachowania, które jednocześnie naruszają ochronę przewidzianą w obu unormowaniach. Zatem prawa te można zaliczyć do kategorii praw od siebie niezależnych[456]. Przy przetwarzaniu danych osobowych, które narusza prawo do prywatności występuje ochrona kumulowana z art. 23 k.c., gdzie dobra osobiste znajdują się także pod ochroną prawa cywilnego. Przepis ten nie stanowi enumeratywnie wyliczonego katalogu dóbr osobistych, umożliwiając włączenie dóbr odnoszących się do życia prywatnego, rodzinnego i sfery intymności.

Dynamicznie rozwijająca się technologia wpływa na pojmowanie prawa do prywatności, na postrzeganie prawa do ochrony danych osobowych, które nierozerwalnie wiążą się z postępem prawa do informacji. Można zatem utożsamiać prawo do ochrony danych osobowych z nowoczesną ochroną prywatności, biorąc pod uwagę globalizację informacji, a także szybkość przepływu wszelkiego rodzaju informacji[457]. Motywem przemawiającym za uznaniem prawa do ochrony danych osobowych za element prawa do prywatności jest przekonanie, że prawo do ochrony danych osobowych sprowadza się do anonimowości[458]. Co prawda, wiele wskazuje na to, że opisywane prawa się ze sobą łączą, a ochrona danych osobowych stanowi emanację prawa do prywatności. Jednakże procesy przeobrażeń w dziedzinie ochrony danych osobowych wychodzą poza ramy pojęcia prywatności. Prywatność w dalszym ciągu pozostaje jednym z celów ochrony danych. Technizacja przetwarzania danych osobowych uniemożliwia realizację również innych praw, zaliczanych do kategorii praw politycznych i socjalnych. Świadczy to o rozszerzaniu się ochrony danych osobowych, co tym samym stanowi, że jej granice nieco ulegają zatarciu.

Trudno w sposób jednoznaczny określić związek zachodzący pomiędzy prawem do

[455] P. Sobczyk, *Ochrona danych osobowych…,* s. 310.
[456] J. Barta, R. Markiewicz, *Prawo do prywatności w społeczeństwie informatycznym,* „Ethos" 1999, nr 45-46, s. 380.
[457] M. Safjan, *Prawo do prywatności…,* s. 10.
[458] A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 1999, s. 11.

prywatności a prawem do ochrony danych osobowych. Nie ma pomiędzy nimi relacji odnoszącej się do całości i części, ale też niełatwo je rozgraniczyć. Ustawa zasadnicza reguluje je oddzielnie, zachowując tym samym ich odrębność. Biorąc pod uwagę funkcje, jakie pełnią te dwa uprawnienia, można stwierdzić, że autonomia informacyjna wchodzi w zakres prawa do prywatności. Prawo do prywatności stanowi kompozycję wartości podlegających ochronie, do których należą dane osobowe[459]. W oparciu o tę koncepcję obecne jest twierdzenie, że ochrona danych osobowych jest niemalże wyspecjalizowaną postacią prawa do prywatności. Jednakże temu prawu nie można w pełnym zakresie nadawać takiego znaczenia. Początki powstawania zagadnienia związanego z ochroną danych osobowych sięgają ochrony prywatności przed ingerencją z zewnątrz w procesach związanych z gromadzeniem informacji przez podmioty publiczne i prywatne. Wobec tego, prawo do ochrony danych osobowych służy ochronie prawa do prywatności, jednak tylko w tym przypadku, kiedy wiąże się z informacjami odnoszącymi się do danej osoby oraz gwarancji stanu niezależności. Stan niezależności przejawia się w autonomii informacyjnej, gdzie podmiot samodzielnie podejmuje decyzje o zakresie i zasięgu udostępniania informacji o swoim życiu. Może wybrać, czy chce pozostać anonimowym, czy też nie. Pierwszoplanową funkcją prawa do ochrony danych osobowych jest zabezpieczenie prawa do prywatności.

Nikt tak naprawdę nie ma możliwości, aby ukryć wszystkie o sobie informacje. Prawo do samodecydowania jednostki o dotyczących jej danych osobowych jest prawem oczywistym, jednak należy mieć na względzie, że pewne informacje o konkretnym podmiocie są dostępne, ponieważ „nieodłącznym elementem naszej egzystencji są wiadomości, jakie o nas mają inni”[460]. Nie istnieją takie środki, które pozwolą na wymazanie tych informacji, bądź na zawężenie ich zakresu, stąd też aktualna jest teza, że możliwość dysponowania wszystkimi o sobie informacjami jest w znacznym stopniu ograniczona[461].

1.5. Podsumowanie

Prawo do prywatności zaliczane jest w prawie wewnętrznym, unijnym oraz międzynarodowym do fundamentalnych praw człowieka. Gwarantowane jest przez Konstytucję RP w art. 47, a pośrednio także w art. 51. W prawie Unii Europejskiej,

[459] M. Wilbrandt-Gotowicz, *Prywatność osoby fizycznej jako ograniczenie jawności informacji publicznych w świetle orzecznictwa sądów administracyjnych,* [w:] *Jawność i jej ograniczenia. Znaczenie orzecznictwa,* red. M. Jaśkowska, Warszawa 2014, s. 160-161.
[460] M. Mucha, *Obowiązki administracji publicznej…,* s. 54.
[461] N. Brieskorn, *Ochrona danych osobowych a zagrożenie prywatności,* [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa 1999, s. 206-207.

prywatność nie znajdowała początkowo ochrony w traktatach ustanawiających Wspólnoty. Dopiero z biegiem czasu powstał autonomiczny system ochrony praw podstawowych, w tym także prawa do prywatności. Znaczną rolę w tej kwestii odgrywał Trybunał Sprawiedliwości Unii Europejskiej, gdzie w swoim orzecznictwie podkreślał, iż prawa człowieka stanowią część zasad ogólnych dawnego prawa wspólnotowego, a więc zasad branych pod uwagę przy stosowaniu i wykładni prawa unijnego, wywodzonych przez TSUE z traktatów, wynikających z tradycji kulturowych i konstytucyjnych krajów członkowskich UE. Ochrona praw podstawowych stała się na tyle potrzebna, że pojawiła się w judykaturze w 1969 roku w odniesieniu do zasad ogólnych prawa w sprawie Stauder. Przełomowym momentem dla rozwoju ochrony praw podstawowych, w tym prawa do prywatności, było uzyskanie przez Kartę Praw Podstawowych takiej samej mocy prawnej, jak traktaty.

Stworzenie precyzyjnej definicji prawa do prywatności jest niemożliwe. Zmieniająca się sytuacja społeczna, gospodarcza, rozwój techniki, a zwłaszcza przestrzeni informatycznej, powodują, że nie można wyznaczyć jednolitych granic prywatności. Definicje opierają się na przykładowym wyliczeniu obszarów, które mogą wchodzić w zakres prywatności. Najogólniej, można ją rozumieć jako sferę wolną od ingerencji zarówno władzy, jak i drugiego człowieka. Akceptowanym podejściem jest ujęcie przedmiotowego prawa jako instrumentu hamowania nadmiernej ingerencji w obszar wolności jednostki.

W prawie polskim, prawo do prywatności uznaje się za „dobro osobiste w postaci życia prywatnego, obejmującego wszystko, co na uzasadnione odseparowanie się jednostki, służy jej do rozwoju fizycznego lub psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej”[462]. Zakresem tego prawa objęte jest życie rodzinne, mir domowy, tajemnica korespondencji, ochrona danych osobowych, a nawet tajemnica bankowa. Postuluje się także, aby prawa do prywatności nie ograniczać wyłącznie do bycia pozostawionym w spokoju. Prywatność przejawia się w akcie dyspozycji, gdzie jej zakres jest uzależniony od stopnia, w jakim określony akt dyspozycji wiąże się z innymi dobrami podlegającymi ochronie prawnej, zwłaszcza z interesami innych podmiotów.

Można zauważyć, że powstały dwa modele prawa do prywatności. Pierwszy model jest chroniony przez Konstytucję RP jako „prawo do prywatności”, „prawo do poszanowania prywatności”, „prawo do ochrony życia prywatnego”. Inne prawa i wolności stanowią konkretyzację i rozwinięcie prawa do prywatności. Powstałe kolizje powinno się rozstrzygać poprzez odwołanie do klauzuli generalnej. W drugim modelu, to prawo należy wyprowadzić

[462] A. Kopff, *Koncepcja prawa do intymności…,* s. 20.

z postanowień konstytucyjnych chroniących inne prawa i wolności. Zatem na jego treść składa się poniekąd suma tych praw.

Prawo do prywatności może być uznawane za konglomerat wartości chronionych, w którego obrębie wyróżnia się charakterystyczne postaci prywatności i prawnych gwarancji ich ochrony, do których należy ochrona danych osobowych[463]. Prawo do ochrony danych osobowych wywodzone jest z prawa do prywatności. Traktowane jest jako jego emanacja lub element[464]. Zarówno prawo do prywatności, jak i prawo do ochrony danych osobowych są prawami „trzeciej generacji", o ile w ogóle można mówić, że prawo do ochrony danych osobowych występuje odrębnie od prawa do prywatności[465]. Te dwa prawa mają cechy wspólne, bowiem odnoszą się do prywatności jako dobra zasługującego na ochronę prawną. Bliższa analiza prawa do ochrony danych osobowych wymaga oceny relacji, które zachodzą między tymi prawami[466]. Konstytucja RP posługuje się pojęciem wartości, stanowiąc na wstępie, że uniwersalnymi wartościami są dobro, sprawiedliwość, prawda i piękno[467]. Konstytucyjny termin wartości jest współistotny pojęciu godności człowieka, zaliczonej do zasad, których poszanowanie stanowić ma niewzruszoną podstawę RP. W tym znaczeniu zarówno prawo do prywatności, jak i prawo do ochrony danych osobowych są wartościami konstytucyjnymi jako współistotne godności człowieka, stanowiącej fundament demokratycznego państwa prawnego. Proklamowanym wartościom konstytucyjnym, wstęp do Konstytucji RP, nadaje normatywny charakter[468]. Prawo do prywatności, znajdujące swój wyraz w regulacji art. 47 Konstytucji RP i prawo do ochrony danych osobowych z art. 51 Konstytucji RP są normatywną podstawą ustroju, zdeterminowaną przez godność i wolność jednostki[469]. W judykaturze Trybunału Konstytucyjnego znajduje wyraz pogląd, w myśl którego ochrona życia prywatnego obejmuje także ochronę danych osobowych, określaną jako autonomię informacyjną, która oznacza „prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów"[470]. Koncepcja autonomii informacyjnej jest w orzecznictwie Trybunału Konstytucyjnego uogólnieniem prawa do prywatności. Konstytucja RP realizuje najbardziej zasadnicze

[463] M. Sakowska-Baryła, *Prawo do ochrony danych osobowych…,* s. 92.
[464] M. Jabłoński, K. Wygoda, *Dostęp do informacji…,* s. 207.
[465] P. Sarnecki, *Uwaga 2 do art. 47,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, M. Zubik, tom II, Warszawa 2016, s. 57.
[466] M. Sakowska-Baryła, *Prawo do ochrony danych…,* s. 23.
[467] B. Szmulik, J. Szymanek, *Introduction to the Constitution of the Republic of Poland,* Warszawa 2019, s. 182.
[468] Wyrok TK z dnia 12 września 2005 r., sygn. akt: SK 13/05…
[469] R. Piotrowski, *Prawo do prywatności…,* s. 18.
[470] Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01…

elementy składające się na treść prawa do ochrony życia prywatnego, tj. szacunek dla autonomii informacyjnej jednostki, a więc sam obowiązek udostępniania danych, zawężony do *sensu stricte* określonych ustawowo zdarzeń oraz ograniczenia arbitralności prawodawcy[471]. W doktrynie i orzecznictwie prawo do prywatności i ochrony danych osobowych, jako wartości konstytucyjne odnoszą się nie tylko do relacji między władzą publiczną a jednostką, ale także do relacji pomiędzy jednostkami.

Z powyższego więc wynika, że prawo do ochrony danych osobowych jest pochodną prawa, jakim jest prawo do prywatności[472], a za jeden z aspektów prawa do prywatności uważa się właśnie prawo do ochrony informacji (danych) osobistych, co jednak w Konstytucji RP zostało ujęte w odrębnym przepisie[473]. Związek, jaki istnieje pomiędzy tymi dwoma prawami można określić jako materialny. Ochrona prywatności w głównej mierze zależna jest od ochrony danych osobowych dotyczących jednostki. Konstytucyjna gwarancja prawa do prywatności ma istotne znaczenie w procesie stosowania przepisów mających na celu ochronę danych osobowych. Ustawodawca zezwolił na przetwarzanie danych osobowych, ograniczających prawo do prywatności, ale też jednocześnie je chroniąc, obejmując tym samym życie prywatne, rodzinne i osobiste.

Powyższe prawa nie mają jednak charakteru absolutnego. Te konstytucyjne wartości mogą zostać ograniczone dla realizacji innej normy konstytucyjnej, która oddaje pod ochronę dobro, jakie w danym przypadku ma pierwszeństwo przed prywatnością[474]. Przesłanki ograniczenia stanowią ogólny wyjątek i muszą się mieścić w zasadach demokratycznego państwa prawnego oraz nie powinny prowadzić do naruszenia istoty chronionego prawa[475].

Problematyka ochrony danych osobowych i ochrony prywatności jest złożona. Wpływa na to szybkość zmian technologicznych, rozwój Internetu, globalizacja komunikacji oraz wzrost ilości gromadzonych i przetwarzanych danych. Wraz z rozwojem technologii informacyjnych i cyfrowych pojawiły się nowe wyzwania w dziedzinie ochrony danych osobowych. W związku z gromadzeniem, przetwarzaniem i transferem danych na dużą skalę, potrzebna stała się ochrona poufności, integralności i dostępności informacji, a także konieczne było zapewnienie jednostkom kontroli nad swoimi danymi i zminimalizowanie ryzyka nadużyć. Zagwarantowanie przejrzystych, spójnych i skutecznych ram prawnych jest nie tylko powinnością, lecz stanowi wyraz dla poszanowania praw i wolności jednostek.

[471] Wyrok TK z dnia 12 listopada 2002 r., sygn. akt: SK 40/01…
[472] P. Sobczyk, *Ochrona danych osobowych…,* s. 306.
[473] L. Garlicki, M. Zubik, *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* „Wydawnictwo Sejmowe" 2016, nr 2, s. 98.
[474] Wyrok TK z dnia 13 lutego 2001 r., sygn. akt: K 19/99…
[475] M. Gdula, *Wprowadzenie do prawa do prywatności…,* s. 38.

Odpowiednie zrozumienie, przestrzeganie oraz egzekwowanie przepisów związanych z ochroną danych osobowych jest traktowane jako fundament dla budowania zaufania i zagwarantowania harmonijnego rozwoju społeczeństwa opartego na szacunku do prywatności i godności jednostek.

Odpowiedzią na powyższe zjawiska było wprowadzenie nowej regulacji prawnej, tj. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE w celu zagwarantowania należytego poziomu ochrony prywatności i bezpieczeństwa.

Rozdział 2. „Prawo do bycia zapomnianym" w pracach Komisji Europejskiej i Parlamentu Europejskiego

2.1. Uwagi wstępne

Charakterystyczną cechą współczesnych procesów poznawczych jest stały i nielimitowany dostęp do informacji. Informacja, z jednej strony stanowi dobro, dzięki któremu możliwy jest rozwój państwa, społeczeństwa i samej jednostki. Z drugiej strony, traktowana jest nie tylko jako zagrożenie dla poszanowania wolności i praw. Niewłaściwie upubliczniona, uważana jest za niedozwoloną ingerencję w sferę chronioną, zarówno w prawodawstwie międzynarodowym, jak i krajowym.

Jednym z powodów zachodzących zmian na płaszczyźnie funkcjonowania jednostki jest dążenie do coraz to większego wykorzystywania zdobyczy nowoczesnych technologii. Wpływają one nie tylko na pojmowanie istoty i treści znanych wcześniej wolności i praw, ale także tych definiowanych na bieżąco, w odpowiedzi na wciąż pojawiające się niebezpieczeństwa. Powstawanie nowych uprawnień jest ściśle powiązane z przekazem elektronicznym o zasięgu globalnym, z dostępem do informacji za pośrednictwem Internetu i z informacyjnymi platformami[476].

Dostęp do informacji łączy się ze swobodą tworzenia i osobistego zamieszczania każdej informacji. W wyniku tego powstają spory, w odniesieniu do ochrony oraz poszanowania wolności i praw jednostki. Z praktycznego punktu widzenia, każdy zainteresowany ma możliwość nie tylko pozyskiwania informacji – funkcja informacyjna, ale może się nią wymieniać z innymi podmiotami – funkcja komunikacyjna, lub też dalej ją przekazywać – funkcja kreacyjna. Pojęcie komunikacji zapewnia konkretnej osobie zarówno dotarcie do pożądanych danych, czy uzyskanie dodatkowych informacji poprzez dwustronną ich wymianę, ale też tworzenie lub modyfikowanie już istniejącego zasobu informacyjnego.

Powszechna swoboda definiowania różnego rodzaju informacji, dotyczących nie tylko określonego rodzaju zdarzeń, lecz też konkretnych osób, przybiera rozmaite postaci. W przestrzeni publicznej zamieszczane są dane, które nie tylko dotyczą faktów, czy wynikają z ustawowo zdefiniowanych obowiązków informacyjnych, ale również stanowią wynik subiektywnie definiowanej chęci upowszechnienia wiedzy na temat danej osoby, zdarzenia, czy też okoliczności. W związku z tym, dochodzi do upubliczniania informacji

[476] P. Wąglowski, *Internet a dobra osobiste człowieka,* [w:] *Internet-fenomen społeczeństwa informacyjnego,* red. T. Zasępa, R. Chmura, Częstochowa 2001, s. 317.

nieprawdziwych, niepełnych i nierzetelnych, co wpływa na poczucie braku odpowiedniego poszanowania szeregu wolności i praw gwarantowanych jednostce. Przekaz elektroniczny zmodyfikował klasyczne rozumienie mechanizmów informacyjnych, w tym to, co można rozumieć przez trwanie informacji[477]. Pod tym sformułowaniem kryje się sytuacja stałej dostępności danych, odnoszących się do zindywidualizowanej osoby fizycznej, bez ograniczeń czasowych. Zdarza się, że informacja po jej uzewnętrznieniu, używana jest w zupełnie innych celach, niż pierwotnie zakładano. Sytuacja ta budziła zastrzeżenia, przede wszystkim w kontekście poszanowania prawa do prywatności i powiązanej z nim ochrony danych osobowych. Przyczyniła się nie tylko do powstania dyskusji na temat wolności przekazu i dostępu do informacji, ale ostatecznie doprowadziła do normatywizacji treści „prawa do bycia zapomnianym"[478].

Ochrona danych osobowych i poszanowanie życia prywatnego zgodnie z art. 7 i 8 KPP zaliczają się do kategorii europejskich praw podstawowych. Na mocy art. 16 ust. 1 oraz 2 Traktatu o Funkcjonowaniu Unii Europejskiej, każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, 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.

Wdrażanie nowych reguł prawnych w zakresie ochrony danych osobowych nie było ani szybkie, ani proste. Całość procedury prawnej dotyczącej nowych przepisów poprzedzona była publicznymi konsultacjami przeprowadzonymi przez Komisję Europejską. Ich celem było sprawdzenie, na jakim poziomie jest zachowana ochrona danych osobowych i czy wymagane jest jej usprawnienie. Rezultatem postanowień podjętych podczas konsultacji był komunikat Komisji Europejskiej skierowany do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów[479]. Następnie, podejmowane były prace nad przygotowaniem pierwszego projektu Rozporządzenia. Wobec

[477] Pod tym pojęciem kryje się stała dostępność konkretnych danych, w tym dotyczących zindywidualizowanej osoby fizycznej, bez ograniczeń czasowych. W Internecie nic nie ginie i nic nie jest zapomniane. Zob. M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym,* Wrocław 2021, s. 15.

[478] J. Żak, *Koncepcja „prawa do bycia zapomnianym",* [w:] *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi,* red. M. Jabłoński, S. Jarosz-Żukowska, Wrocław 2014, s. 142-155.

[479] Komunikat zatytułowany był „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej" z dnia 4 listopada 2010 r., a więc ogłoszony rok później od czasu przeprowadzonych konsultacji w 2009 roku,
[dostęp: 29.06.2017] http://ec.europa.eu/Justice/news/consulting_public/0006/com_2010_609_pl.pdf.

tego, w styczniu 2012 r. Komisja Europejska zaprezentowała gotową propozycję modyfikacji prawnych. Wyciągniętą konkluzją z prac Komisji, które były prowadzone przez cały ten czas było ukazanie, jak ważne jest zastąpienie obowiązującej Dyrektywy 95/46/WE, aktem normatywnym rangi Rozporządzenia unijnego.

Komisja Europejska za priorytet nowej regulacji przyjęła zwiększenie praw osób fizycznych, które automatycznie są podmiotami danych osobowych. Oczekiwanym skutkiem Rozporządzenia było jednocześnie wzmocnienie rynku wewnętrznego i struktury obszaru Unii Europejskiej, zagwarantowanie wysokiego poziomu ochrony danych, egzekwowanie we właściwy sposób przepisów prawnych oraz wprowadzenie norm odnoszących się do ochrony danych osobowych w zasięgu globalnym[480]. Komisja Europejska przedstawiła rozwiązania, które okazały się kontrowersyjne. W marcu 2014 r. swoje uwagi zaprezentował Parlament Europejski, a w czerwcu 2015 r. Rada[481]. W dniu 15 czerwca 2015 r. ministrowie sprawiedliwości i spraw wewnętrznych podjęli próbę wspólnego wypracowania treści Rozporządzenia. Wobec czego, Rada rozpoczęła negocjacje z Parlamentem Europejskim. Największym kłopotem, który przeszkadzał w ujednoliceniu treści aktu prawnego było zagwarantowanie swobody prowadzenia działalności gospodarczej a połączone z tym prawo do prywatności i ochrona danych osobowych. Była to kwestia najbardziej problematyczna, dla której odpowiedzią był Program „Bezpieczna Przystań" *(ang. Safe Harbour)*, który miał zapewniać bezpieczeństwo przesyłanych danych poza teren Unii Europejskiej[482]. Swobodny przepływ danych miał nastąpić pomiędzy Stanami Zjednoczonymi a UE, w sytuacji, kiedy kraj będący docelowym odbiorcą danych nie zapewni adekwatnego poziomu ochrony danych osobowych w rozumieniu Dyrektywy 95/46/WE. Przesłanie danych poza terytorium Unii Europejskiej powiązane było z brakiem federalnych regulacji prawnych dotyczących ochrony danych osobowych. Ten program miał na celu wypracowanie wspólnego stanowiska umożliwiającego pogodzenie dwóch odmiennych porządków prawnych.

W grudniu 2015 roku został wypracowany kompromis, który pozwolił jednocześnie na uchwalenie wchodzących reform. Stąd też Rozporządzenie zostało uchwalone przez Parlament Europejski 14 kwietnia 2016 r., natomiast niespełna miesiąc później w dniu 4 maja 2016 r. oficjalnie opublikowano tekst nowego Rozporządzenia w Dzienniku Urzędowym Unii Europejskiej.

---

[480] M. Kluska, *Droga do ogólnego rozporządzenia o ochronie danych osobowych,* [w:] *Vademecum ABI cz. II-Przygotowanie do roli Inspektora Ochrony Danych,* red. T. Izydorczyk, M. Kluska, M. Kołodziej, Warszawa 2017, s. 1.

[481] D. Lubasz, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi,* Warszawa 2018, s. 9.

[482] K. Gałaj-Emiliańczyk, *Tworzenie systemu ochrony danych osobowych krok po kroku,* Warszawa 2016, s. 21.

Przedstawiając projektowany akt normatywny unowocześniający system ochrony danych osobowych, komisarz Viviane Reding podkreśliła fundamentalne cele przyświecające reformie[483]. Ogólne Rozporządzenie o Ochronie Danych Osobowych weszło w życie 24 maja 2016 r., ale zaczęło być stosowane od 25 maja 2018 r., po dwuletnim okresie przygotowawczym. Uzasadniano to koniecznością zobowiązania administratorów i podmiotów przetwarzających dane do wprowadzenia takich rozwiązań w swoich organizacjach, zarówno w sektorze publicznym, jak i prywatnym, które ułatwiłyby implementację nowych regulacji prawnych.

Rozporządzenie unijne zastąpiło unormowania Dyrektywy 95/46/WE, która jawiła się jako przestarzały akt normatywny. Podstawowym motywem zmiany modelu ochrony danych osobowych była chęć zagwarantowania większej skuteczności prawu do ochrony danych osobowych, a także potrzeba dostosowania unijnych regulacji prawnych do potrzeb wynikających z postępującego rozwoju nowych technologii oraz cyfryzacji. Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych potraktowana została jako środek nieprzystosowany do nowo pojawiających się zjawisk, do których zaliczano komercjalizację Internetu, transgraniczny przepływ danych, jak też nowe sposoby przetwarzania danych (np. przy użyciu chmury obliczeniowej). Dyrektywa w wystarczający sposób nie gwarantowała bezpieczeństwa danych osobowych obywateli Unii Europejskiej (Europejskiego Obszaru Gospodarczego) w wypadku transferu danych do tzw. państw trzecich, czyli krajów niebędących członkami Unii Europejskiej (EOG)[484].

Czynnikiem początkującym podjęcie prac nad wyodrębnieniem „prawa do bycia zapomnianym" przez Komisję Europejską na poziomie unijnym była refleksja nad instytucją zatarcia skazania. Z uprawnienia tego mogli skorzystać sprawcy osadzeni w jednostkach penitencjarnych nawet za najcięższe przestępstwa. Prace nad „prawem do bycia zapomnianym" inspirowane były konkluzją, zgodnie z którą nie występuje w Internecie, w przeciwieństwie do rzeczywistości, zatarcie skazania po upływie oznaczonego czasu. Zatem zatarcie skazania po upływie określonego czasu nie posiadało swojego odpowiednika w sieci. Informacja o popełnionych czynach trwale pozostawała dostępna w Internecie,

[483] Jednym z nich był wybór środka legislacyjnego, tj. rozporządzenia, czyli aktu prawa europejskiego stosowanego bezpośrednio w państwach członkowskich Unii Europejskiej, pozbawionego wymogu implementacji, co jest konieczne w przypadku chociażby dyrektywy.

[484] *Co zmienia nowe rozporządzenie o ochronie danych osobowych?,* [dostęp: 07.02.2017] https://biznesalert.pl/zmienia-nowe-rozporzadzenie-o-ochronie-danych-osobowych/.

oddziałując na życie codzienne bez czasowego ograniczenia[485].

Brak unormowań prawnych o „prawie do bycia zapomnianym" nie przesądzał o tym, że ono nie istniało. Trybunał Sprawiedliwości Unii Europejskiej w jednym ze swoich wyroków z dnia 13 maja 2014 r. w sprawie zawisłej pod sygn. akt: C-131/12[486], przyznał podmiotom danych osobowych „prawo do bycia zapomnianym". Trybunał swoim orzeczeniem wzmocnił prawne mechanizmy ochrony prywatności wynikające z art. 7 i 8 Karty Praw Podstawowych. Jednocześnie wzbudził obawy dotyczące ograniczenia wolności wypowiedzi i informacji. Wskazał również zakres terytorialny obowiązywania Dyrektywy 95/46/WE. Za administratora danych osobowych uznano operatora wyszukiwarki internetowej, odpowiedzialnego za przetwarzanie danych w rozumieniu art. 2 lit. d) Dyrektywy 95/46/WE. Po spełnieniu określonych warunków przez podmiot danych, operator jest zobligowany do usunięcia z wyświetlanej listy wyników wyszukiwania (mającej za punkt wyjścia imię i nazwisko danej osoby) linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje.

Warto wskazać, że wzmianki o „prawie do bycia zapomnianym" pojawiły się też w światowych doktrynach prawa znacznie wcześniej[487]. Na terenie Europy miało to miejsce w 2006 r., gdy zarówno organy ochrony danych osobowych, jak i organizacje stojące na straży wartości społeczeństwa obywatelskiego próbowały wyjaśniać co oznacza w krajach anglojęzycznych terminologia kryjąca się pod pojęciem „right to oblivion" albo „right to be forgotten"[488]. Zatem „prawo do bycia zapomnianym" nie jest instytucją całkowicie nową. Należy je traktować jako rozwinięcie i doprecyzowanie dotychczasowego porządku prawnego[489].

Konstrukcja prawna uregulowana w art. 17 RODO wywodzi się z art. 12 lit. b) Dyrektywy 95/46/WE, w którym przewidziano uprawnienie do żądania usunięcia swoich danych. Trybunał Sprawiedliwości Unii Europejskiej nie ustanowił nowego prawa, a jedynie

---

[485] I. Lipowicz, *Uwagi do strategii poprawy skuteczności unijnych przepisów dotyczących ochrony danych osobowych przedstawionej przez Komisję Europejską,* przygotowane przez Stowarzyszenie „Naukowe Centrum Prawno-Informatyczne", Warszawa 2011, s. 7.

[486] Wyrok TSUE z dnia 13 maja 2014 r., sygn. akt: C-131/12…

[487] Tak też, w Stanach Zjednoczonych nastąpiło to w II połowie XX wieku, tj. w 1989 r., gdy Sąd Najwyższy USA uznał, że dany podmiot może mieć interes w żądaniu „praktycznego zaciemnienia" pewnych informacji. Zob. E.P. Goodman, *Practical Obscurity and The Right to Be Forgotten*: *"Pretty Much" Privacy is Enough,* [dostęp: 04.02.2015] https://medium.com/@ellgood/practical-obscurity-and-the-right-to-be-forgotten-pretty-much-privacy-is-enough-c321bdaffa08#.rksxmkgp9.

[488] J. Liddicoat, *The Right to be Forgotten,* [dostęp:] https://www.privacy.org.nz/assets/Files/Speeches-presentations/Right-to-be-Forgotten-Joy-Liddicoat.pdf.

[489] K. Rostkowska, *RODO-zmiany w ochronie danych osobowych w 2018 roku. Najważniejsze informacje,* [dostęp: 28.12.2017] https://www.bankier.pl/wiadomosc/RODO-zmiany-w-ochronie-danych-osobowych-w-2018-roku-Najwazniejsze-informacje-7563322.html.

dokonał wykładni prawa do usunięcia i zablokowania danych. Niniejsze Rozporządzenie rozszerza jednak to uprawnienie, nadając mu miano „prawa do bycia zapomnianym".

W Rozdziale drugim przedstawiono genezę „prawa do bycia zapomnianym", w tym prace legislacyjne mające wpływ na jego kształtowanie się. Zwrócono uwagę na różne koncepcje tego prawa i funkcje, jakie pełni.

2.2. Geneza „prawa do bycia zapomnianym" w oparciu o wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain z dnia 13 maja 2014 r., sygn. akt: C-131/12

Unowocześniany dostęp do informacji, korelujący ze swobodą tworzenia oraz osobistego zamieszczania większości informacji, prowadzi do powstawania wielu sporów i wątpliwości interpretacyjnych, zwłaszcza w odniesieniu do ochrony i poszanowania wolności i praw jednostki. Z praktycznego punktu widzenia, zainteresowany ma możliwość nie tylko pozyskiwania informacji, ale ponadto przysługuje mu uprawnienie do bezpośredniego wymieniania się informacjami z innymi podmiotami oraz ich definiowania, a także dalszego przetwarzania. Definicja komunikacji zapewnia konkretnej osobie nie tylko dotarcie do pożądanych danych, czy możliwość uzyskania dodatkowych informacji przez dwustronną ich wymianę, ale tworzenie, czy zmianę już istniejącego określonego zasobu informacyjnego. Taka sytuacja budzi zastrzeżenia, chociażby w odniesieniu do należytego poszanowania praw gwarantowanych jednostce, tj. prywatności i związanej z nią ochrony danych osobowych. Finalnie doprowadziło to do powstania „prawa do bycia zapomnianym". Początkowo jawiło się ono jako prawo niepisane, a z czasem zostało wprost wyartykułowane w unijnym akcie normatywnym.

Brak unormowań prawnych o „prawie do bycia zapomnianym" nie oznaczał więc, że ono nie istniało. Trybunał Sprawiedliwości Unii Europejskiej w jednym ze swoich wyroków z dnia 13 maja 2014 r. w sprawie zawisłej pod sygn. akt: C-131/12[490], przyznał podmiotom danych osobowych „prawo do bycia zapomnianym"[491]. W głównej mierze prawo to odnosiło się do danych zamieszczanych w wyszukiwarkach internetowych. TSUE stanął na stanowisku, iż uprawnioną do poszanowania „prawa do bycia zapomnianym" jest każda osoba, której dane są przetwarzane, przy jednoczesnym sprawdzeniu tego, czy posiada ona

[490] Wyrok TSUE z dnia 13 maja 2014 r., sygn. akt: C-131/12…

[491] Był to pierwszy prekursorski wyrok, odwołujący się do „prawa do bycia zapomnianym", dlatego ma on tak istotne znaczenie, spośród innych orzeczeń, z punktu widzenia tego zagadnienia.

prawo, aby dotycząca jej informacja „nie była już w aktualnym stanie rzeczy powiązana z jej imieniem i nazwiskiem poprzez listę wyświetlającą wyniki wyszukiwania mającego za punkt wyjścia to imię i nazwisko”[492].

Trybunał Sprawiedliwości UE dokonał na tyle obszernej wykładni pojęcia „administrator danych”, tak aby objąć jego zakresem operatorów wyszukiwarek internetowych, co miało stanowić rezultat podkreślenia znaczenia dla aktywności Google w przetwarzaniu danych osobowych obywateli państw członkowskich Unii Europejskiej[493]. Bezpośrednim skutkiem wydanego orzeczenia było zobowiązanie podmiotów świadczących usługi wyszukiwania w sieci do usunięcia z wyświetlanej listy wyników wyszukiwania, po uprzednim wpisaniu imienia i nazwiska, linków do publikowanych przez osoby trzecie witryn internetowych zawierających informacje odnośnie tej osoby[494]. Dzień ten wyznacza początek używania w praktyce czysto teoretycznej dotąd koncepcji „prawa do bycia zapomnianym” [495]. Prawo to mogło zostać zrealizowane, gdy informacje uznano za nieprawdziwe, niewłaściwe, niestosowne albo nadmierne w stosunku do celów przetwarzania danych. Obowiązek ten nie mógł być wykonany wyłącznie dlatego, że konkretne informacje stały się niewygodne dla osoby, której dotyczą. O dużym zasięgu istniejącego problemu świadczył fakt, że od chwili ogłoszenia wyroku, spółka Google odebrała od użytkowników ponad pół miliona zgłoszeń, w których domagali się oni usunięcia informacji w ramach realizacji „prawa do bycia zapomnianym”.

Postępowanie sądowe zainicjował obywatel Hiszpanii, który domagał się od Google Spain SL i Google Inc. usunięcia zdezaktualizowanych informacji. W dniu 19 stycznia i 9 marca 1998 r. Dziennik „La Vanguardia” opublikował artykuł, który w późniejszym czasie został udostępniony także w Internecie. Swoją treścią obejmował licytacje nieruchomości w przedmiocie postępowania egzekucyjnego zaległych składek na ubezpieczenia społeczne. Pomimo faktu, że należność główna została uiszczona, to informacja o zadłużeniu pozostała w sieci ogólnodostępna. Po wpisaniu w wyszukiwarce Google nazwiska osoby, link przekierowywał do strony gazety. Redakcja Dziennika nie wyraziła zgody na usunięcie publikacji, bowiem w swoim pierwotnym założeniu została udostępniona w oparciu o przepis prawa, tj. zarządzenie Ministerstwa Pracy i Polityki Społecznej. W związku z tym, podmiot

[492] Wyrok TSUE z dnia 13 maja 2014 r., sygn. akt: C-131/12…
[493] M. Czerniawski, *Prawo do bycia zapomnianym w Internecie. Glosa do wyroku TS z dnia 13 maja 2014 r. C-131/12,* [dostęp: 02.03.2023] https://sip.lex.pl/komentarze-i-publikacje/glosy/prawo-do-bycia-zapomnianym-w-internecie-glosa-do-wyroku-ts-z-dnia-13-386107074.
[494] Punkt 88 wyroku.
[495] *„Prawo do bycia zapomnianym” w Internecie,* [dostęp: 15.03.2022] https://eur-lex.europa.eu/PL/legal-content/summary/right-to-be-forgotten-on-the-internet.html.

danych osobowych rok później zwrócił się do Google Spain z prośbą o zlikwidowanie linków kierujących do Dziennika po wpisaniu nazwiska w wyszukiwarce. Google Spain przekazał z kolei te żądanie do Google Inc. z/s w Kalifornii, będącego operatorem wyszukiwarki internetowej. Podmiot, którego dane zostały rozpowszechnione wniósł do hiszpańskiego organu ochrony danych osobowych sprzeciw wobec zaistniałej sytuacji. Organ, rozpatrując sprzeciw, nie uznał obowiązku gazety w przedmiocie usunięcia tych informacji, skoro ich publikacja nastąpiła zgodnie z obowiązującym wówczas porządkiem prawnym. Stwierdził jednak, że obowiązek ten powinien ciążyć na Google. Zarówno Google Spain, jak i Google Inc. złożyły od tej decyzji odwołanie. Sąd zwyczajny w Hiszpanii wydał postanowienie o zawieszeniu postępowania i skierował do Trybunału Sprawiedliwości pytania o charakterze prejudycjalnym, zmierzające do uzyskania odpowiedzi na pytania, czy przetwarzanie danych osobowych przez oddział lub spółkę zależną operatora wyszukiwarki internetowej w kraju członkowskim następuje w oparciu o prowadzoną działalność gospodarczą administratora danych, czy tenże operator jest utożsamiany z administratorem danych, a jego czynności interpretowane są jako przetwarzanie danych osobowych, oraz czy formułowane prawo sprzeciwu w stosunku do przetwarzania danych jest powodem domagania się od operatora wyszukiwarki internetowej, aby dane konkretnego podmiotu nie były dostępne w sieci[496].

Rzecznik Generalny Trybunału Sprawiedliwości Unii Europejskiej Niilo Jääskinen w sporządzonej przez siebie opinii w dniu 25 czerwca 2013 r. postulował, aby organ opowiedział się za tym, że przetwarzanie danych osobowych przez oddział, bądź spółkę zależną operatora wyszukiwarki w kraju członkowskim odbywa się w ramach działalności gospodarczej administratora danych, pod warunkiem, że działalność ta odnosi się do marketingu usług, z których korzystają mieszkańcy tego państwa. Rzecznik Generalny Trybunału postulował za przyjęciem, iż operator wyszukiwarki internetowej nie powinien być uważany za administratora danych osobowych, wyłączając jednak z tej kategorii dane przetwarzane w indeksie jego wyszukiwarki. Warunkiem uznania tego wyjątku był zakaz indeksowania i archiwizowania danych osobowych, pozostając w sprzeczności z wytycznymi wydawcy witryny internetowej. Wniosek końcowy opinii opierał się na braku odpowiedzialności operatora wyszukiwarki za tekst umieszczany na portalach internetowych, do jakich odsyła wyszukiwarka. Co istotne na gruncie niniejszej sprawy, to Nillo Jääskinen odrzucił postulat, że w oparciu o przepisy konstruujące prawo żądania usunięcia i zablokowania danych oraz zawierające sprzeciw w stosunku do przetwarzania danych,

[496] P. Fajgielski, *Funkcjonowanie portali internetowych-wybrane problemy prawne,* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* red. G. Szpor, W. Wiewiórowski, Warszawa 2012, s. 133.

podmiotom danych osobowych może przysługiwać „prawo do bycia zapomnianym" w wyszukiwarce internetowej w wypadku, gdy negowane informacje opublikowano na portalach internetowych zgodnie z prawem[497].

W dniu 13 maja 2014 r. Trybunał Sprawiedliwości Unii Europejskiej wydał w przedmiotowej sprawie przełomowe orzeczenie. Treść wyroku uzasadniała, że przepisy Dyrektywy 95/46/WE odnoszą się do internetowych wyszukiwarek, także wtedy, gdy serwery, których funkcją jest umożliwienie przetwarzania danych osobowych mają swoje miejsce w krajach trzecich, ale operator wyszukiwarki ma swój oddział albo spółkę zależną w państwie unijnym. Trybunał podniósł, że działalność wyszukiwarek internetowych wykorzystująca lokalizację informacji zamieszczanych w Internecie przez inne osoby, ich mechaniczne indeksowanie, periodyczne przechowywanie i udostępnianie użytkownikom można uznać za przetwarzanie danych osobowych w rozumieniu art. 2 lit. b) Dyrektywy, wówczas, gdy w informacjach tych zawierają się dane osobowe. Trybunał Sprawiedliwości UE utożsamił ponadto operatora wyszukiwarki internetowej z administratorem tych danych osobowych, na którym spoczywa obowiązek odpowiedzialności za ich przetwarzanie[498]. Uznanie wyszukiwarki internetowej Google za administratora danych osobowych spotkało się z dwoma przeciwstawnymi stanowiskami. Według Nilla Jääskinena za administratora danych należało potraktować tylko wydawcę źródłowych stron internetowych, posiadających odpowiednie uprawnienia do stosowania tzw. kodów wyłączenia znacznie ograniczających indeksowanie[499]. Z drugiej strony, wyrażano aprobatę dla przyjętego przez Trybunał Sprawiedliwości Unii Europejskiej rozwiązania. Chociażby brytyjska Izba Lordów podkreślała m.in. to, iż operator wyszukiwarki Google nie tylko pasywnie odbiera dane osobowe, lecz także przy pomocy specjalnych algorytmów ustala ich ważność, kolejność, jak też popularność wyszukiwania, co oddziałuje na prezentowane treści w przestrzeni internetowej, które mogą spowodować naruszenie prywatności użytkowników Internetu[500].

Trybunał podkreślił, że z uwagi na to, że działalność wyszukiwarki ma charakter subsydiarny w stosunku do tej prowadzonej poprzez wydawców stron internetowych oraz może w znacznym stopniu oddziaływać na prawa podstawowe, jak poszanowanie życia

[497] Opinia Rzecznika Generalnego Nila Jääskinena przedstawiona 25 czerwca 2013 r. w sprawie Google Spain SL i Google Inc. przeciwko AEPD i Mario Costeja Gonzàlez, sygn. akt: C-131/12.
[498] 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. 166.
[499] Opinia Rzecznika Generalnego Niila Jääskinena przedstawiona 25 czerwca 2013 roku…
[500] House of Lords, European Union Committee, *EU Data Protection law: a "right to be forgotten"?,* Evidence, 2nd Report of Session 2014-15, [dostęp: 12.07.2015]
https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf.

prywatnego czy ochronę danych osobowych, to operator tej wyszukiwarki powinien w granicach swojej odpowiedzialności i przysługujących mu uprawnień zagwarantować, że działalność wypełnia określone w Dyrektywie wymogi. Nie można było wykluczyć, że w pewnych sytuacjach odmiennej ocenie będzie podlegać te żądanie skierowane do operatora wyszukiwarki od tego skierowanego do wydawcy strony internetowej[501]. To jest o tyle możliwe, ponieważ upowszechnienie informacji w ramach listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko konkretnej osoby, może bardziej wkraczać w prawo do prywatności, aniżeli sama publikacja przez wydawcę strony internetowej[502].

Za przetwarzanie danych należało także uważać przekierowywanie przez wyszukiwarki internetowe do informacji o charakterze upublicznionym, które zostało dokonane przez podmioty trzecie (np. środki masowego przekazu). Odmowa stosowania Dyrektywy w takich sytuacjach powodowałaby jedynie pozorność zachowania ochrony danych osobowych. Orzeczenie utwierdzało w przekonaniu, iż przetwarzanie danych następuje w ramach działalności gospodarczej administratora danych na terytorium konkretnego państwa członkowskiego w momencie, kiedy operator wyszukiwarki internetowej posiadał w nim oddział albo spółkę zależną. Warunkiem miało być jednak prowadzenie marketingu zadedykowanego mieszkańcom tego państwa. Właściwość miejscowa ustalana była zatem nie z uwagi na siedzibę administratora danych osobowych, lecz na podstawie pochodzenia podmiotu danych. Z tego wynikało, że operator wyszukiwarki internetowej, który posiadał swoją siedzibę w państwie trzecim, podlegał normom regulującym ochronę danych osobowych w UE oraz decyzjom administracyjnym organu ochrony danych w kraju członkowskim, którego społeczność jest odbiorcami usług.

Trybunał Sprawiedliwości Unii Europejskiej po zapoznaniu się ze stanowiskiem Rzecznika Generalnego, nie podzielił jego argumentacji. Zapewnił podmiotom danych osobowych „prawo do bycia zapomnianym" w sieci. Traktowano to za przełomowy moment, gdyż prawo to miało być uregulowane przez pierwotną wersję projektu rozporządzenia jako osiągnięcie prowadzące do zwiększenia ochrony danych. Było to odpowiedzią na zagrożenia wynikające z procesu przetwarzania danych osobowych w Internecie, którego Dyrektywa 95/46/WE nie przewidywała, ponieważ korzystanie z Internetu nie było jeszcze na tyle powszechnym zjawiskiem. Niemniej jednak, Trybunał podniósł, że w zasadzie „prawo do bycia zapomnianym" można wywieść z Dyrektywy. Na zasadzie art. 12 lit. b) przedmiotowego aktu, podmiot danych posiada prawo do żądania usunięcia lub zablokowania

[501] Punkt 85 wyroku.
[502] Punkt 87 wyroku.

danych, których przetwarzanie nie pozostaje w zgodzie z jej przepisami, zaś na podstawie art. 14 lit. a) Dyrektywy podmiot mógł wnieść sprzeciw wobec przetwarzania jego danych. Taka niezgodność może wynikać nie tylko z tego, że dane te nie są prawdziwe, ale także mogą one być niewłaściwe, niestosowne, nieaktualne czy nadmierne wobec celów, dla jakich podlegają procesowi przetwarzania, jak też zarówno przechowywane przez dłuższy okres niż jest to wymagane, z wyjątkiem przechowywania na poczet celów historycznych, statycznych i naukowych[503]. Z tego wynika, że nie istnieje bezpośredni wymóg, aby dane, które miały podlegać usunięciu cechowały się w swej naturze nieprawdziwością[504].

W oparciu o wyrok TSUE w sprawie o sygn. akt: C-131/12, operator wyszukiwarki internetowej wypełnia te prawa osoby w chwili, kiedy szukanie informacji po wpisaniu imienia i nazwiska nie doprowadzi do pozyskania linków do upowszechnionych przez podmioty trzecie witryn internetowych obejmujących informacje w odniesieniu do wnioskodawcy. Zaś rezultatem sprzeciwu w stosunku do przetwarzania danych przez operatora wyszukiwarki internetowej jest usunięcie wskazanych informacji zawierających imię i nazwisko, nawet wówczas, gdy informacje te w dalszym ciągu publikowane są na źródłowej stronie internetowej. Co więcej, według Trybunału Sprawiedliwości Unii Europejskiej nie ma znaczenia czy informacje te zostały pierwotnie upowszechnione zgodnie z literą prawa. Ponadto, prawo żądania usunięcia danych przysługuje również w wypadku, kiedy publikacja tych danych na liście wyników wyszukiwania nie wyrządza szkody osobie zgłaszającej żądanie[505]. Dokonując wykładni uzasadnienia wyroku, należy zauważyć, że warunkiem usunięcia linków z nazwiskiem wnioskodawcy z wyników wyszukiwania jest zatem niezgodność opublikowania tych wiadomości z Dyrektywą w momencie złożenia żądania. Nie przesądza to jednak o niezgodności pierwotnej publikacji z Dyrektywą. Sprzeczność może powstać na skutek upływu czasu, kiedy dalsze przetwarzanie danych osobowych straciło na znaczeniu i przez to narusza dobra osobiste jednostki, jak na gruncie kazusu, którego przedmiotem było ogłoszenie egzekucji należności pieniężnych, które zostały uregulowane[506]. Tak przedstawione „prawo do bycia zapomnianym" jest instrumentem realnego egzekwowania prawa do prywatności. Informacje mogą pozostawać na źródłowej witrynie internetowej, ale ich zasięg dzięki przełomowemu orzeczeniu TSUE stał się w dużym stopniu ograniczony z uwagi na brak widoczności w wyszukiwarkach

[503] Punkt 92 wyroku.
[504] Dodatkowo, nawet sam TSUE potwierdził, że „początkowo zgodne z prawem przetwarzanie prawidłowych danych może z upływem czasu stać się niezgodne z Dyrektywą, jeśli dane te nie są już potrzebne do realizacji celów, ze względu na które były gromadzone i przetwarzane". Zob. punkt 93 wyroku.
[505] Punkt 99 wyroku.
[506] Punkt 93 wyroku.

internetowych. Oznacza to, że zapoznanie się z treścią informacji wymaga podjęcia większego wysiłku, które pomimo tego może okazać się bezskuteczne. Trybunał zaznaczył przy tym, że prawa wynikające z przepisów Dyrektywy wskazanych powyżej nie mają charakteru absolutnego. Zasadność uprawnienia polegającego na usunięciu danych informacji z listy wyników wyszukiwania podlega ocenie w kontekście naruszenia prawa do prywatności oraz umotywowanego interesu potencjalnych adresatów przekazu[507]. Wobec czego, wkroczenie w sferę prywatności poprzez pozostawienie w wyszukiwarce internetowej linków kierujących do stron powiązanych z nazwiskiem danego podmiotu może być uzasadnione w przypadku, gdy interes publiczny zostanie uznany za nadrzędny w porównaniu z zagwarantowaniem prawa do prywatności (podlega to indywidualnej i spersonalizowanej ocenie organu ochrony danych i sądu). Równowaga ta może zależeć od charakteru informacji poddanych analizie oraz tego, w jakim stopniu są one ważne dla prywatności osoby, z którą są powiązane. Nie bez znaczenia jest także interes publiczny w zestawieniu z tą informacją[508]. Podstawa odmowy zablokowania wyników wyszukiwania nie może opierać się na poglądzie, iż publikacja danych w wyszukiwarce nie spowoduje szkody dla skarżącego, ani też na interesie gospodarczym operatora wyszukiwarki internetowej.

Z punktu widzenia podmiotów, na jakich ciąży obowiązek realizacji zgłaszanych żądań w ramach przysługującego „prawa do bycia zapomnianym", kluczowym aspektem jest rozporządzanie określonymi kryteriami oceny zasadności żądania usunięcia danych. Trybunał Sprawiedliwości Unii Europejskiej choć mało precyzyjnie nawiązał do tego problemu, nie wskazując, w jaki sposób dokonywać wyważenia prawa do prywatności, prawa do informacji czy wolności wypowiedzi, to jednak poddając orzeczenie kompletnej wykładni, można wyinterpretować pewne wskazówki, które mogą nieco ułatwić podjęcie decyzji w przedmiocie słuszności żądania usunięcia informacji. Jedną ze szczególnych okoliczności, która powinna być brana pod uwagę, jest funkcja sprawowana przez daną osobę w społeczności. Odnosi się to do sytuacji, gdzie „ingerencja w prawa podstawowe tej osoby jest uzasadniona nadrzędnym interesem tego kręgu odbiorców, polegającym na posiadaniu dostępu do danej informacji"[509]. Następną przesłanką, na którą zwraca uwagę Trybunał Sprawiedliwości UE, jest czas, jaki upłynął od opublikowania konkretnej informacji.

Po wydaniu orzeczenia, przedsiębiorstwo informatyczne Google wskazało, że w ich ocenie dostateczne jest usuwanie spornych wyników wyszukiwania jedynie z jego

[507] Miało to wynikać z wolności słowa i mediów czy funkcji publicznej sprawowanej przez wnioskodawcę. Zob. punkt 83 wyroku.
[508] Punkt 81 wyroku.
[509] Punkt 97 wyroku.

wyszukiwarek europejskich[510]. Praktyka ta pozostaje w sprzeczności ze wskazówkami Grupy Roboczej Art. 29[511], która żądała usuwania informacji w skali światowej, skoro użytkownikom przysługuje globalny dostęp do dowolnej wyszukiwarki Google. Stanowisko Google było w zupełności nieprawidłowe. Stało bowiem w sprzeczności z ideą „prawa do bycia zapomnianym". W tej sytuacji zainterweniował francuski organ ochrony danych *Commission Nationale de I'informatique et des Libertés*, grożąc nałożeniem sankcji karnych. Google zaciekle broniło swojego zdania, przyjmując, że „prawo do bycia zapomnianym" jest wymogiem unijnym i nie odnosi się do państw trzecich[512]. Na marginesie warto wskazać, że pogląd podobny do zaprezentowanego przez Google wyraził także Facebook[513]. Wspomniany organ ochrony danych nie przyjął odwołania Google od decyzji nakładającej obowiązek stosowania „prawa do bycia zapomnianym" w wyszukiwarkach na jakichkolwiek domenach z pominięciem kryterium geograficznego, a więc również na domenach krajowych wykraczających poza terytorium Unii Europejskiej, np. google.com. Źródła tego obowiązku upatruje się w tym, że dostęp do informacji ma każdy użytkownik, bez względu na rozszerzenie geograficzne domeny. Google, pragnąc zrealizować przełomowy wyrok TSUE, udostępnił formularz służący do wskazania danych osobowych podmiotów oraz linków stron, których zablokowania żądają w wynikach wyszukiwania[514]. Z terytorium Polski wpłynęło około 13 tysięcy wniosków, dotyczących blisko 48 tysięcy adresów URL[515].

Orzeczenie TSUE dotyczące „prawa do bycia zapomnianym" budzi kontrowersje wśród specjalistów do spraw prywatności. Mimo przełomowego znaczenia nadanego wyrokowi C-131/12, nie znaleziono odpowiedzi na pytania w dziedzinie praktycznej realizacji „prawa do bycia zapomnianym". Są one formułowane zarówno przez użytkowników sieci jako podmioty uprawnione, jak też przez administratorów wyszukiwarek internetowych jako podmioty zobowiązane. Google czynnie wykrywa użytkowników swojej wyszukiwarki pochodzących z obszaru Unii Europejskiej. Blokuje widoczność stron

[510] J. Fioretti, *Google sticks to EU only application of "right to be forgotten",* [dostęp: 20.09.2016] http://www.reuters.com/article/2015/01/19/us-google-eu-privacy-idUSKBNOKS21E20150119.
[511] Oficjalna nazwa Grupy Roboczej Art. 29 brzmi Zespół Roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Niezależny podmiot o charakterze doradczym, powołany na mocy art. 29 Dyrektywy 95/46/WE. Z dniem wejścia w życie RODO, Zespół Roboczy został zastąpiony przez Europejską Radę Ochrony Danych.
[512] J. Naughton, *In the battle of free speech now it's France vs. Google,* [dostęp: 20.09.2016] http://www.theguardian.com/commentisfree/2015/aug/09/battle-free-speech-france-google-right-to-be-forgotten.
[513] S. Gibbs, *Facebook questions use of „right to be forgotten" ruling,* [dostęp: 20.09.2016] http://www.theguardian.com/technology/2015/jul/07/facebook-questions-use-of-right-to-be-forgotten-ruling.
[514] Wyrok TSUE co prawda odnosił się do Google, jednakże „prawo do bycia zapomnianym" w sieci znajduje swoje zastosowanie we wszystkich wyszukiwarkach internetowych. Zob. Google Transparency Report, stan na 13.06.2016, [dostęp: 20.09.2016] https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en.
[515] https://www.google.com/transparencyreport/removals/europe-privacy/?hl=pl; dane aktualne na dzień 31 lipca 2016 r.

internetowych zawierających informacje na temat osób, które mogłyby zostać ujawnione po wpisaniu w wyszukiwarkę należytego zapytania, zawierającego imię i nazwisko. Simon Migliano, szef zespołu badawczego Top10VPN – firmy zajmującej się ochroną prywatności i bezpieczeństwa w sieci, stwierdził, że „do obejścia tego rodzaju systemu wykrywania lokalizacji jest zdolny każdy korzystający z usługi wirtualnej sieci prywatnej (VPN) przy pomocy serwera zlokalizowanego poza UE. Tym samym można zyskać dostęp do tych wyników (zawierających wrażliwe dane – PAP) niezależnie od tego, czy zostały one objęte „prawem do bycia zapomnianym", czy też nie". W jego ocenie, „luka ta podkreśla znaczące ograniczenia geoblokowania zawartości Internetu w obecnych czasach". Z kolei, Ron Moscona – partner w międzynarodowej firmie prawniczej Dorsey&Whitney podniósł, że wyrok TSUE nie zapewnia jasności w kwestii interpretacji art. 3 RODO, który reguluje zakres terytorialny stosowania przepisów oraz warunki przetwarzania danych poza terytorium Unii Europejskiej[516].

Zasięg terytorialny „prawa do bycia zapomnianym" ograniczony wyłącznie do terytorium Unii Europejskiej może w przyszłości przyczynić się do tzw. bałkanizacji wyników wyszukiwania, czyli do sytuacji, gdzie inne informacje będą widoczne dla Amerykanów, inne dla Portugalczyków, a jeszcze inne dla Polaków[517]. W Europie i Stanach Zjednoczonych istnieje odmienne pojmowanie sfery prywatności. W opozycji do unijnego sądownictwa, działania amerykańskich organów sądowych nie podążają w kierunku wzmocnienia ochrony prywatności kosztem wolności słowa[518].

Zadania polegającego na wypełnieniu luk podjęły się podmioty zobligowane do przestrzegania „prawa do bycia zapomnianym" oraz organy stojące na straży ochrony danych osobowych obywateli państw unijnych[519]. Niemniej jednak, ciężar oceny zasadności żądań został przeniesiony na podmioty prywatne, dostawców usług wyszukiwania.

Powyższe nie zmienia jednak faktu, że Trybunał Sprawiedliwości Unii Europejskiej przychylił się do twierdzenia, iż „prawo do bycia zapomnianym" występujące w wyszukiwarkach internetowych wywodzi się z art. 7 i 8 Karty Praw Podstawowych[520],

---

[516] *„Prawo do bycia zapomnianym": kontrowersje po wyroku korzystnym dla Google,* [dostęp: 26.09.2019] https://cyberdefence24.pl/polityka-i-prawo/prawo-do-bycia-zapomnianym-kontrowersje-po-wyroku-korzystnym-dla-google.

[517] P. Rutkowska, *"Prawo do bycia zapomnianym" w cyfrowym świecie. Wybrane zagadnienia,* „Społeczeństwo i Polityka" 2019, nr 1 (58), s. 209.

[518] J. Rosen, *The right to be forgotten,* "Stanford Law Review" 2012, vol. 88, s. 88.

[519] T. Grzegory, *Pamięć absolutna czy kontrolowana amnezja-wybrane problemy prawne regulacji „prawa do bycia zapomnianym" w ogólnym rozporządzeniu o ochronie danych,* „Monitor Prawniczy" 2016, nr 20, s. 61.

[520] Na uwagę zasługują rozważania Trybunału Sprawiedliwości Unii Europejskiej, który w wydanym przez siebie wyroku podkreślił, że wyświetlanie zdjęć, po przeprowadzeniu wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby, przedstawiające ten podmiot w postaci miniatur (thumbnails), może stanowić

a ponadto z prawa do usunięcia danych z Dyrektywy 95/46/WE, wobec czego gruntowna reforma nie jest na tyle konieczna. Artykuł 17 Rozporządzenia wyznaczył mimo to granice „prawa do bycia zapomnianym", które zaczerpnął z przywołanego wyroku, stanowiącego przełom w kwestii usunięcia danych nie w miejscu źródłowym, ale w wyszukiwarce internetowej, co w praktyce spełnia cel tego prawa.

2.3. Geneza Ogólnego Rozporządzenia o Ochronie Danych Osobowych (2016/679)

2.3.1. Prace legislacyjne nad przepisami unijnego Rozporządzenia a uchylenie Dyrektywy 95/46/WE

Przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych zostały przyjęte w ramach zwykłej procedury ustawodawczej, w której Parlament Europejski i Rada Unii Europejskiej, składająca się z przedstawicieli krajów UE, mają takie samo prawo głosu. Podstawę prawną do rozpoczęcia prac nad projektem nowego Rozporządzenia stanowił art. 16 TFUE (dawniej art. 286 TWE[521]), na podstawie którego każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

W dniu 27 stycznia 2012 roku Komisja Europejska przedłożyła Radzie i Parlamentowi Europejskiemu wniosek ustawodawczy, którego uzasadnienie konkretyzowało proponowane nowe ramy prawne ochrony danych osobowych w UE. Dyrektywa 95/46/WE została przyjęta w 1995 roku i stanowiła podstawowy dokument ustanawiający unijne przepisy o ochronie danych osobowych. Uregulowania Dyrektywy miały służyć realizacji dwóch celów, a mianowicie obejmować ochronę danych osobowych oraz zagwarantować swobodny przepływ danych pomiędzy państwami członkowskimi. Szybki rozwój technologiczny przyniósł nowe wyzwania w zakresie ochrony danych osobowych. Wzrosła skala wymiany i zbierania danych. Technologia umożliwiła zarówno przedsiębiorstwom prywatnym, jak i organom publicznym wykorzystywanie danych osobowych do wykonywania powierzonych im zadań. Zmieniła zarówno gospodarkę, jak i życie społeczne. Budowanie zaufania do Internetu stało się kluczowym elementem rozwoju gospodarczego. Jego brak sprawiał, że

szczególnie poważną ingerencję w prawa do poszanowania życia prywatnego i do ochrony danych osobowych. Zdaniem TSUE, konieczne jest przeprowadzenie osobnej oceny wyszukiwarki działalności, polegającej na wyświetlaniu wyników wyszukiwania grafiki w postaci miniatur. „Wynikające z takiej działalności dodatkowe naruszenie praw podstawowych może być szczególnie intensywne z powodu łączenia w jedną całość wszystkich informacji dotyczących osoby, której dane znajdują się w Internecie". Zob. E. Skibińska, *„Prawo do bycia zapomnianym",* [dostęp: 12.01.2023] https://legalis.pl/prawo-do-bycia-zapomnianym/.

[521] Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z dnia 29 grudnia 2006 r. (Dz. Urz. UE C 2006 nr 321E, dalej: TWE).

konsumenci nie byli pewni, czy korzystać z usług internetowych. Zagrożenia te spowolniły rozwój innowacyjnego wykorzystania nowych technologii.

Wdrażanie procedury prawnej, dotyczącej przepisów w zakresie ochrony danych osobowych, poprzedzone było publicznymi konsultacjami przeprowadzanymi przez Komisję Europejską. Czas ich trwania wyniósł ponad dwa lata. Pierwsze konsultacje społeczne miały miejsce od dnia 9 lipca do dnia 31 grudnia 2009 roku i dotyczyły podstawowego prawa do ochrony danych osobowych. Komisja Europejska otrzymała 168 odpowiedzi[522]. Kolejne konsultacje zostały przeprowadzone od dnia 4 listopada 2010 roku do dnia 15 stycznia 2011 roku. Komisja Europejska otrzymała 305 odpowiedzi, z czego 54 od obywateli, 31 od organów publicznych, 220 od organizacji prywatnych, zwłaszcza od zrzeszeń biznesowych i organizacji pozarządowych[523]. Przeprowadzono również konsultacje specjalne. W miesiącach czerwiec – lipiec 2010 roku zorganizowano spotkania z organami państw członkowskich oraz z zainteresowanymi stronami z sektora prywatnego, a także organizacjami zajmującymi się prywatnością, ochroną danych osobowych oraz organizacjami konsumenckimi[524]. W listopadzie 2010 roku, wiceprzewodnicząca Komisji Europejskiej Viviane Reding, zorganizowała wspólną debatę na temat reformy ochrony danych.

W trakcie konsultacji, większość zainteresowanych stron wyraziła aprobatę dla stwierdzenia, że ogólne zasady mogą zachować swoją ważność, lecz z drugiej strony, istnieje potrzeba dostosowania obecnych ram prawnych, aby móc lepiej reagować na wyzwania stawiane przez szybki rozwój technologii, w szczególności Internetu i postępującą globalizację, przy jednoczesnym zachowaniu ich technologicznej neutralności. Słowa krytyki padły zwłaszcza ze strony podmiotów gospodarczych, które apelowały o ujednolicenie przepisów w zakresie ochrony danych osobowych, gdyż utrudnione jest dla nich przekazywanie danych z terenu Unii Europejskiej do innych części świata.

W Komunikacie do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z dnia 4 listopada 2010 roku w sprawie „Całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej”[525], który stanowił konsekwencję przeprowadzonych konsultacji publicznych, Komisja Europejska zajęła stanowisko, że UE potrzebuje spójnej polityki w obszarze prawa

[522] Z opiniami niezaklasyfikowanymi jako poufne można się zapoznać na stronie internetowej Komisji, [dostęp:] http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.
[523] Z opiniami niezaklasyfikowanymi jako poufne można się zapoznać na stronie internetowej Komisji, [dostęp:] http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.
[524] http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm.
[525] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej,* 4 listopada 2010 r., COM (2010) 609.

podstawowego do ochrony danych osobowych. Obowiązujące ramy prawne nie zapobiegły rozdrobnieniu sposobów realizacji ochrony danych osobowych w całej UE, ugruntowaniu niepewności prawnej oraz rozpowszechnieniu istniejącego w społeczeństwie poglądu, według którego z prowadzoną w Internecie działalnością wiążą się istotne ryzyka[526]. Stało się to bodźcem do stworzenia silniejszych, bardziej spójnych ram ochrony danych w Unii Europejskiej, które miały umożliwić rozwój gospodarki cyfrowej na rynku wewnętrznym, zapewnić osobom fizycznym kontrolę nad ich własnymi danymi oraz wzmocnić pewność prawną i praktyczną dla przedsiębiorców i organów publicznych.

Rezolucją z dnia 6 lipca 2011 roku Parlament Europejski zatwierdził sprawozdanie, w którym poparł podejście Komisji do reformy ram ochrony danych[527]. Rada UE w dniu 24 lutego 2011 roku wyraziła analogiczne stanowisko. Europejski Komitet Ekonomiczno-Społeczny także podzielił pogląd Komisji, by odpowiednio zbadać niedostosowane przepisy Dyrektywy 95/46/WE do zmieniającej się rzeczywistości, tak aby zagwarantować spójniejsze stosowanie unijnych przepisów we wszystkich krajach członkowskich[528].

W dniu 12 marca 2014 roku Parlament Europejski w pierwszym czytaniu przyjął opinię odnośnie do proponowanego Rozporządzenia. W dniu 15 czerwca 2015 roku, Rada wypracowała podejście ogólne, a tym samym dała mandat prezydencji do rozmów trójstronnych z Parlamentem Europejskim[529]. Od czerwca 2015 roku odbyło się dziesięć spotkań trójstronnych. W ich wyniku, prezydencja wraz z przedstawicielami Parlamentu Europejskiego, osiągnęli przy pomocy Komisji Europejskiej porozumienie co do całościowego tekstu kompromisowego. W dniu 16 grudnia 2015 roku Komitet Stałych Przedstawicieli zatwierdził tekst, który uzgodniono w rozmowach trójstronnych dzień wcześniej, tj. w dniu 15 grudnia. W dniu 17 grudnia 2015 roku parlamentarna Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych przegłosowała na nadzwyczajnym posiedzeniu tekst uzgodniony podczas rozmów trójstronnych. Przewodniczący Komitetu Stałych Przedstawicieli otrzymał pismo (Dok. 15323/15),

[526] Specjalna ankieta Eurobarometru (EB) nr 359 „Ochrona danych i tożsamość elektroniczna w UE (2011)", [dostęp: 29.08.2017] https://commission.europa.eu/index_pl.

[527] Rezolucja PE z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (2011/2025(INI)), [dostęp: 06.07.2011] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL.

[528] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), [dostęp:] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011.

[529] Prezydencja kieruje pracami Rady nad unijnym ustawodawstwem oraz dba o ciągłość działań Unii Europejskiej, porządek procedur legislacyjnych i współpracę państw członkowskich, [dostęp:] https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/; Dok. 9565/15, [dostęp: 11.06.2015] https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/pl/pdf.

w którym przewodniczący ww. Komisji parlamentarnej poinformował, że zaleci zarówno jej, jak i Parlamentowi Europejskiemu przyjąć bez poprawek na sesji plenarnej porozumienie wypracowane w rozmowach trójstronnych, z zastrzeżeniem jednak korekt prawno-językowych[530]. Na posiedzeniach w dniu 12 lutego 2016 roku, Rada wypracowała porozumienie polityczne w sprawie projektu rozporządzenia. W dniu 8 kwietnia 2016 r. przyjęła stanowisko w pierwszym czytaniu, w pełni zgodne z kompromisowym tekstem uzgodnionym podczas nieformalnych negocjacji z Parlamentem[531]. W dniu 14 kwietnia 2016 roku, Parlament Europejski podczas drugiego czytania zatwierdził stanowisko Rady przyjęte w pierwszym czytaniu oraz stwierdził, że akt prawny zostaje przyjęty zgodnie ze stanowiskiem Rady. Parlament Europejski zobowiązał swojego przewodniczącego oraz przewodniczącego Rady do podpisania aktu prawnego zgodnie z art. 297 ust. 1 TFUE. Taki sam obowiązek nałożył na sekretarza generalnego po sprawdzeniu, czy wszystkie procedury zostały prawidłowo zakończone oraz zobligował go do przygotowania publikacji w Dzienniku Urzędowym Unii Europejskiej wraz z sekretarzem generalnym Rady[532]. Tekst Rozporządzenia został oficjalnie opublikowany w dniu 4 maja 2016 roku.

2.3.2. Idea ujednolicenia zasad ochrony danych osobowych w Unii Europejskiej

Głównym celem, dla którego wprowadzono przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych było ujednolicenie, inaczej harmonizacja, prawa w zakresie ochrony i przepływu danych osobowych w państwach członkowskich UE[533].

Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala wymiany oraz gromadzenia danych osobowych wzrosła. Zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogły wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej zaczęły udostępniać publicznie i globalnie informacje osobowe. Przemiany te wymagały stabilnych, spójniejszych ram ochrony danych w Unii Europejskiej oraz zdecydowanego egzekwowania ich przepisów, gdyż istotna pozostawała budowa zaufania, która pozwalała na rozwój gospodarki cyfrowej na

[530] Dok. 5455/16, [dostęp: 28.01.2016] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN.
[531] Uzasadnienie Rady: Stanowisko Rady (UE) nr 6/2016 w pierwszym czytaniu w sprawie przyjęcia rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz. Urz. UE 2016 C 159/02).
[532] Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 14 kwietnia 2016 r. w sprawie stanowiska Rady przyjętego w pierwszym czytaniu w celu przyjęcia RODO (Dz. Urz. UE 2018 C 58/252).
[533] https://alterweb.pl/-rodo-jak-dziala [dostęp: 07.04.2022].

rynku wewnętrznym. Sugerowano, aby osoby fizyczne, podmioty gospodarcze i organy publiczne zyskały większe poczucie pewności prawa i jego praktycznych zastosowań.

Integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia ruchu transgranicznego. Wzrosła wymiana danych pomiędzy podmiotami publicznymi i prywatnymi, w tym między osobami fizycznymi, stowarzyszeniami i przedsiębiorstwami. Organy krajowe państw członkowskich były obligowane do tego, aby w celu wykonywania swoich obowiązków lub realizacji zadań w imieniu organu innego państwa podejmowały ze sobą współpracę i wymieniały się danymi osobowymi.

Cele i zasady Dyrektywy 95/46/WE nie spełniły do końca swoich pierwotnych założeń. Nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona danych osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami podejmowanymi w Internecie. Różnice w poziomie ochrony praw i wolności, które uwidaczniały się w państwach członkowskich w związku z przetwarzaniem danych osobowych, utrudniały swobodny przepływ danych osobowych w Unii Europejskiej. Stanowiły przeszkodę w prowadzeniu działalności gospodarczej, zakłócały konkurencję oraz utrudniały organom wykonywanie obowiązków nałożonych na nie prawem UE. Rozbieżności w poziomie ochrony wynikały z różnic we wdrażaniu i stosowaniu Dyrektywy.

Aby ochrona danych osobowych w Unii Europejskiej była efektywna, podjęto decyzję, żeby wzmocnić i doprecyzować prawa podmiotów danych oraz obowiązki podmiotów przetwarzających dane osobowe i kierujących przetwarzaniem, ale też wprowadzić równorzędne uprawnienia do monitorowania i egzekwowania przepisów oraz takie same sankcje wobec tych, którzy naruszają te normy w państwach członkowskich. Stąd też, żeby zapewnić spójny poziom ochrony osób fizycznych w Unii Europejskiej i zapobiegać rozbieżnościom hamującym swobodny przepływ danych na rynku wewnętrznym, należało przyjąć rozporządzenie, które miało zagwarantować podmiotom gospodarczym, w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom, pewność prawa i przejrzystość, natomiast osobom fizycznym we wszystkich krajach członkowskich ten sam poziom prawnie egzekwowalnych praw oraz obowiązków i zadań administratorów i podmiotów przetwarzających. Przepisy Rozporządzenia miały spójnie monitorować przetwarzanie danych osobowych, jak również zapewniać równoważne sankcje w państwach członkowskich oraz skuteczną współpracę organów nadzorczych.

Rozporządzenie miało wspierać wykorzystanie potencjału jednolitego rynku cyfrowego poprzez:

- jeden kontynent – jedno prawo: jednolite ogólnoeuropejskie prawo o ochronie danych, które miało zastąpić obowiązujący niespójny katalog przepisów z 28 państw członkowskich;
- punkt kompleksowej obsługi: prowadzenie działalności gospodarczej w całej Unii Europejskiej miało stać się tańsze i łatwiejsze dzięki możliwości zwracania się do jednego organu nadzorczego, a nie do 28 organów;
- równe szanse: po reformie, na spółki mające siedzibę poza Unią Europejską narzucono obowiązek przestrzegania tych samych przepisów, co na spółki mające siedziby na terenie UE. Przed reformą spółki europejskie przestrzegały bardziej restrykcyjnych standardów;
- neutralność technologiczna: nowoczesne regulacje Rozporządzenia utrzymują korzystne warunki, które sprzyjają innowacjom.

Ogólne Rozporządzenie o Ochronie Danych Osobowych jest stosowane w takim samym stopniu w każdym z państw członkowskich Unii Europejskiej. Krajowe akty normatywne, których treść jest niezgodna z Rozporządzeniem unijnym mogły być pozbawione atutu ważności. Z tego też powodu ustawodawstwa państw członkowskich dostosowywano do nowej rzeczywistości prawnej[534]. RODO zastąpiło dotychczas obowiązującą na terytorium Unii Europejskiej Dyrektywę 95/46/WE, jak również w polskim porządku prawnym ustawę o ochronie danych osobowych[535], wprowadzając odmienny model ochrony w oparciu o ryzyko, tj. *risk-based approach*[536]. Fundamentalną różnicą Rozporządzenia w porównaniu z wcześniej obowiązującą Dyrektywą 95/46/WE jest rodzaj samego aktu prawnego. Zgodnie z art. 288 TFUE, Rozporządzeniu nadano ogólny zasięg obowiązywania. Wiąże ono w całości i jest bezpośrednio stosowane, tzw. *direct effect.* Oznacza to przy tym redukcję różnic w poziomie ochrony danych osobowych w poszczególnych państwach członkowskich Unii Europejskiej, zagwarantowanie jednolitości stosowania prawa, a także wykształcenie mechanizmu spójności[537]. Wskutek tego, doszło do ujednolicenia stosowania prawa na całym terytorium Unii Europejskiej

[534] K. Gałaj-Emiliańczyk, *Tworzenie systemu ochrony…,* s. 19.
[535] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 nr 133, poz. 883 ze zm., dalej: u.o.d.o.).
[536] Reformę europejskiej ochrony danych osobowych od dawna brano pod uwagę. Dostrzegano konieczność unowocześnienia rozwiązań prawnych, wyrażano wolę wzmocnienia danych osobowych wykorzystywanych w gospodarce, zwłaszcza w aspekcie transgranicznym pomocnym ujednoliceniu rynku cyfrowego w Unii Europejskiej. Zob. D. Lubasz, *RODO. Zmiany w zakresie ochrony danych…,* s. 7.
[537] P. Makowski, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017, s. 976.

i zlikwidowania różnorodności ustawodawstw państw członkowskich w obszarze ochrony danych osobowych. Dyrektywa 95/46/WE jawiła się jako akt harmonizacji minimalnej, zobowiązując tylko do wdrożenia stosownych środków wskazujących na dolny pułap ochrony, natomiast w pozostałym zakresie pozostawiała krajom członkowskim swobodę, mając na względzie bardziej restrykcyjne uregulowania[538]. Dyrektywa 95/46/WE różniła się w tym zakresie, że zobowiązywała państwa członkowskie do osiągnięcia wskazanych w niej celów, niemniej jednak wskazywała na najniżej wymagany poziom dostosowania i dawała możliwość unormowania konkretnej dziedziny w stopniu przekraczającym symboliczne wymagania, co prowadziło do powstawania pewnych dyferencjacji pomiędzy przepisami prawnymi w danych państwach. Oprócz tego, wspomniana Dyrektywa nie egzekwowała od państwa członkowskiego narzuconej formy i środków prawnych wdrażania jej postanowień[539].

Bezpośrednie, a co za tym idzie, jednolite i równorzędne stosowanie przepisów Rozporządzenia przez kraje członkowskie wyłącza powstawanie rozbieżności między obszarami ochrony danych w Unii Europejskiej. Unijny system ochrony danych osobowych, oparty na przepisach Rozporządzenia, jest co do zasady wspólnym dla wszystkich krajów członkowskich Unii Europejskiej zbiorem reguł przetwarzania danych osobowych, zobowiązań administratorów danych oraz praw przysługujących podmiotom danych. Z praktycznego punktu widzenia odnosi się to do wyrażenia zgody na marketing elektroniczny, na gromadzenie wrażliwych danych, a w przypadku braku innej podstawy prawnej, na przesyłanie danych do państw trzecich. Do zbioru tych reguł zalicza się także zasadę celowości, zasadę jakości danych, zasadę adekwatności, czy zasadę ograniczenia czasowego. Ponadto uwzględnia się analizę ryzyka związanego z przetwarzaniem danych i obowiązek zabezpieczenia ich przed nieuprawnionym dostępem lub modyfikacją dokonywaną przez osoby trzecie, jak również status administratora bezpieczeństwa informacji. Zagwarantowanie jednostce udzielenia informacji o stanie przetwarzania danych, dostępie do danych, uprawnieniu do ich poprawiania i wniesienia sprzeciwu w stosunku do ich przetwarzania, jest przejawem procesu przetwarzania zgodnego z przepisami prawa. W model ochrony danych osobowych w skali UE wpisują się ponadto zasady międzynarodowych transferów danych, a zwłaszcza formy zapewnienia danym odpowiedniej ochrony następującej tuż po transferze poza terytorium Unii Europejskiej[540].

[538] https://geobid.pl/aktualnosci/rodo-co-zmienia-nowe-prawo-o-ochronie-danych-osobowych.
[539] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz…,* s. 4.
[540] *Tamże.*

Warto nadmienić, że poprzez zróżnicowane ujęcie zakresu terytorialnego, Rozporządzenie odnosi się również do podmiotów niemających jednostek organizacyjnych w UE. Jedynym jednak warunkiem jest przetwarzanie danych związanych z oferowaniem towarów lub usług osobom przebywającym w Unii Europejskiej, a także z monitorowaniem zachowania osób, których dane dotyczą[541].

Jednak, pomimo zunifikowania zasad ochrony danych w Unii Europejskiej, szczegółowe przepisy krajowe nadal różnią się w wybranych sferach. Wynika to z kompetencji państw członkowskich związanych przepisami traktatów, bądź też z unijnych aktów prawa wtórnego o randze równej rozporządzeniu. W zakresie, w jakim Rozporządzenie dopuszcza doprecyzowanie lub zaostrzenie jego regulacji przez prawo państw członkowskich, mogą one (o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie), włączyć elementy Rozporządzenia do prawa krajowego.

Obok ogólnego, horyzontalnego prawa o ochronie danych, państwa członkowskie dysponują uregulowaniami sektorowymi w dziedzinach wymagających przepisów bardziej szczegółowych. Rozporządzenie umożliwia też doprecyzowanie przepisów dotyczących przetwarzania danych newralgicznych. Zatem może istnieć takie prawo kraju członkowskiego, które określałoby okoliczności konkretnych sytuacji związanych z przetwarzaniem danych osobowych, w tym dookreślało przesłanki, które decydowałyby o zgodności tego procesu z porządkiem prawnym. Przykładem takiej dziedziny, w której różnice są dopuszczalne, jest przetwarzanie danych osobowych w ramach prowadzonych postępowań karnych z uwagi na występującą współpracę pomiędzy organami ścigania i wymiarem sprawiedliwości oraz potrzebę wprowadzenia ochrony danych osobowych i swobodnego ich przepływu pomiędzy państwami członkowskimi UE[542].

Dwuletnie *vacatio legis*[543] dało czas na przeprowadzenie analiz wpływu Rozporządzenia na poszczególne instytucje, wyodrębnienie wynikających z niego obowiązków, a także wdrożenie rozwiązań gwarantujących zgodność z unijnym aktem prawnym. Był to tylko pozornie niekrótki okres. Dało się to zauważyć w tych branżach, gdzie skala przetwarzania danych była kolosalna, a struktura organizacyjna wymagająca. Także i prawodawcy byli zmuszeni dostosować wiele lokalnych ustaw do przepisów nowego Rozporządzenia. Poziom ochrony danych osobowych i prawa do prywatności osób

[541] M. Czerniawski, *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych,* „Europejski Przegląd Sądowy" 2015, nr 5, s. 150.
[542] W.R. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej,* „Monitor Prawniczy" 2012, nr 7-dodatek specjalny „Ochrona danych osobowych 2012", s. 3.
[543] Rozporządzenie zostało uchwalone w 2016 roku, natomiast przepisy RODO weszły w życie w 2018 roku.

fizycznych zapewniany przez RODO powinien być interpretowany w kontekście Karty Praw Podstawowych. Konkretyzacja ram tych dwóch praw uregulowanych w aktach normatywnych o zasięgu europejskim następuje natomiast w judykaturze Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej.

2.4. Uregulowanie „prawa do bycia zapomnianym" w przepisach Rozporządzenia (2016/679)

2.4.1. „Prawo do bycia zapomnianym" jako jedno z założeń Ogólnego Rozporządzenia o Ochronie Danych Osobowych

Do fundamentalnych założeń RODO, poza „prawem do bycia zapomnianym" pozwalającym na usunięcie danych osobowych z baz danych tworzonych przez wszelkie podmioty dysponujące danymi osobowymi, zaliczała się swoboda w wyborze środków służących ochronie danych osobowych dostosowanych do specyfiki podejmowanych działań, prowadzenie rejestru czynności w zakresie przetwarzania danych osobowych, tworzenie rejestru naruszeń, informowanie organu nadzorczego oraz Prezesa Urzędu Ochrony Danych Osobowych o tych incydentach, wskazanie podstaw przetwarzania danych osobowych, wprowadzenie nowych wymogów dotyczących treści klauzul odnoszących się do wyrażania zgody na przetwarzanie danych osobowych, rozszerzenie obowiązków informacyjnych, ochrona danych osobowych na etapie tworzenia oferowanej usługi i planowania przetwarzania danych oraz szeroka ochrona prywatności i profilowanie danych osobowych[544].

„Prawo do bycia zapomnianym" było przez Komisję Europejską uważane za jedno z zasadniczych praw zwiększających ochronę podmiotom danych. Było przy tym traktowane jako odpowiedź na wyzwania wynikające z przetwarzania danych osobowych w Internecie. „Prawo do bycia zapomnianym" ma szczególne znaczenie w sytuacji, gdy podmiot danych udostępnił swoje dane lub udzielił zgody na ich przetwarzanie jako dziecko. Powodem podjęcia rozważań nad „prawem do bycia zapomnianym" stał się też wniosek, że skorzystanie przez sprawców poważnych przestępstw z dobrodziejstwa instytucji w postaci zatarcia skazania nie posiada swojego odpowiednika w Internecie[545].

W 1995 roku, kiedy to uchwalano Dyrektywę 95/46/WE, „prawo do bycia zapomnianym" nie było na tyle ważne, bowiem z Internetu korzystało mniej niż 1% ludności

[544] https://www.pckp.pl/rodo-podstawowe-zalozenia,4,6248.
[545] I. Lipowicz, *Uwagi do strategii poprawy skuteczności unijnych przepisów…,* s. 12.

kontynentu europejskiego[546]. Zagadnienia związane z „prawem do bycia zapomnianym" były pośrednio regulowane przez Dyrektywę 95/46/WE implementowaną do polskiego porządku prawnego ustawą o ochronie danych osobowych z 1997 roku. Zgodnie z art. 32 ust. 1 pkt 6 u.o.d.o., każdej osobie przysługiwało prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zgromadzone, jak też prawo do żądania zaprzestania przetwarzania danych. Mając na uwadze deklaracje Komisji Europejskiej, warto wskazać, że „prawo do bycia zapomnianym" miało wykraczać poza usuwanie bądź niszczenie danych określone w Dyrektywie 95/46/WE. Organ wykonawczy Unii Europejskiej uznał uprzednie prawo do żądania usuwania danych za niekompletne w stosunku do skali przetwarzania danych w sieci. Stąd też zrodziła się potrzeba jego uzupełnienia poprzez uregulowanie „prawa do bycia zapomnianym", dającego możliwość zlikwidowania danych osobowych z obiegu w Internecie[547].

Pojawiały się trudności związane z kontrolowaniem danych osobowych przez osoby fizyczne. Biorąc pod uwagę brak harmonizacji krajowych przepisów dotyczących ochrony danych osobowych, w niektórych państwach członkowskich ciężej było egzekwować swoje prawa niż w innych, zwłaszcza w odniesieniu do usług internetowych. Osoby fizyczne traciły kontrolę nad własnymi danymi, ponieważ codziennie wymianie podlegała bardzo duża ilość danych. Co więcej, osoby te nie zawsze miały świadomość, że ich dane były zbierane. Wielu Europejczyków uważało, że ujawnianie danych osobowych jest w coraz większym stopniu częścią życia[548], niemniej aż 72% użytkowników Internetu w Europie sądziło, że w wirtualnym świecie musi podawać zbyt wiele danych osobowych, częstokroć nie wiedząc, jak egzekwować swoje prawa on-line.

Komisja Europejska w Dokumencie Roboczym Służb Komisji – Streszczeniu Oceny Skutków z dnia 25 stycznia 2012 roku[549] podyktowała dwa warianty mające podwyższyć skuteczność podstawowego prawa do ochrony danych i umożliwić osobom fizycznym kontrolę dotyczących ich informacji. W przypadku, gdyby okazało się to niemożliwe, warianty miały wspomóc świadomość osób fizycznych, jak skutecznie egzekwować „prawo

[546] Opinia Komisji Przemysłu, Badań Naukowych i Energii dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych z dnia 26 lutego 2013 r. w sprawie wniosku dotyczącego Ogólnego Rozporządzenia o Ochronie Danych Osobowych (COM(2012)0011).
[547] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych…,* s. 157.
[548] Specjalna ankieta Eurobarometru (EB) nr 359…
[549] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52012SC0073.

do bycia zapomnianym". Przede wszystkim, miało ono zostać uregulowane wprost w przepisach Rozporządzenia nr 2016/679.

Pierwszy wariant zatytułowany jako „Działanie miękkie" opierał się na komunikatach Komisji zawierających wykładnię prawa, na narzędziach wsparcia technicznego oraz na finansowaniu, a także na zachęcaniu do standaryzacji i samoregulacji, tak aby wzmocnić wdrażanie obowiązujących przepisów w praktyce, a ponadto podnieść świadomość osób fizycznych. W ramach sporządzonej oceny skutków stwierdzono, że komunikaty Komisji Europejskiej zawierające interpretację przepisów Dyrektywy 95/46/WE nie byłyby wiążące, zatem miałyby jedynie ograniczony wpływ na zmniejszenie niepewności prawnej. Większa samoregulacja na szczeblu Unii Europejskiej pomogłaby w zapewnieniu większej jasności prawa w poszczególnych sektorach, ale nie byłaby wystarczająca, by zapewnić efektywne i spójne stosowanie przepisów w przypadku braku transparentnych ram prawnych UE leżących u jej podstaw. Kampanie informacyjne pomogłyby osobom fizycznym w lepszym poznaniu ich praw oraz zrozumieniu sposobów ich egzekwowania w praktyce. Biorąc pod uwagę egzekwowanie, komunikaty Komisji nie przezwyciężyłyby niechęci krajów członkowskich do zmiany przepisów w taki sposób, aby dać większą niezależność i zharmonizowane uprawnienia.

W ramach drugiego wariantu nazwanego „Nowoczesne ramy prawne" Komisja Europejska przedstawiała wnioski ustawodawcze, prowadzące do jeszcze większej harmonizacji przepisów materialnych poprzez wyjaśnianie przepisów szczególnych. Wnioski miały ułatwiać przepływ danych w ramach Unii Europejskiej oraz z UE do państw trzecich, jak też wzmocnić prawa osób fizycznych, w tym „prawo do bycia zapomnianym". Wierzono, że spotka się to z pozytywnym przyjęciem ze strony społeczności ochrony danych.

Postulowano jednak, aby połączyć wariant drugi z kilkoma „Działaniami miękkimi" z wariantu pierwszego. Preferowany wariant miał przyczynić się do osiągnięcia celów polityki bez konieczności ponoszenia nadmiernych kosztów.

Parlament Europejski w dniu 16 lutego 2012 roku oraz Rada w dniu 1 marca 2012 roku zasięgnęły opinii Europejskiego Komitetu Ekonomiczno-Społecznego zgodnie z art. 304 TFUE w sprawie wniosku dotyczącego Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. W swojej opinii, EKES pochwalił zasadniczo cele wniosku, które dotyczyły ochrony praw podstawowych, zwłaszcza w odniesieniu do propozycji uregulowania „prawa do bycia zapomnianym", wyrażając przy tym nadzieję, że zapewni ono obywatelom lepsze zarządzanie ryzykiem związanym z ochroną danych

osobowych w Internecie oraz możliwość ich usunięcia w sytuacji, gdy nie ma żadnych uzasadnionych podstaw do ich przechowywania[550]. W dniu 7 marca 2012 roku swoje zdanie przedstawił Europejski Inspektor Ochrony Danych, który wyraził aprobatę dla stworzenia norm prawnych dla „prawa do bycia zapomnianym". Postulował, aby dalej rozwijać przepis art. 17 RODO, by zapewnić jego skuteczność w rzeczywistości[551].

W dniu 8 kwietnia 2016 roku, Rada w wyrażonym przez siebie stanowisku[552] nadała mocną pozycję osobom, których dane dotyczą. Postulowała, że aby doszło do wzmocnienia prawa do ochrony danych osobowych, musi zostać uregulowane „prawo do bycia zapomnianym", dające swój wyraz w prawie do usunięcia danych osobowych. Podejście Rady uprawnia osoby fizyczne do żądania, by dane osobowe zostały usunięte, o ile ich przetwarzanie jest niezgodne z Rozporządzeniem lub z prawem Unii Europejskiej lub też z prawem państwa członkowskiego, któremu podlega administrator. Według tego organu, wzmianka o „prawie do bycia zapomnianym" wynika z potrzeby dostosowania usunięcia danych do realiów cyfrowych. Jeśli osoba, której dane dotyczą, zażądała usunięcia danych osobowych, ale administrator już upublicznił te dane, musi on (biorąc pod uwagę dostępną technologię i koszt realizacji), podjąć rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane, że podmiot składa żądanie usunięcia do nich łączy, ale też do ich kopii i replikacji. Nie ma to zastosowania, jeżeli przetwarzanie danych osobowych jest niezbędne do celów, których wyczerpująca lista znajduje się w Rozporządzeniu.

W Komunikacie do Parlamentu Europejskiego[553], Komisja Europejska w dniu 11 kwietnia 2016 r. powtórzyła, że Dyrektywa 95/46/WE, będąca wówczas głównym instrumentem prawnym w zakresie ochrony danych osobowych w Europie, była przełomowym dokumentem w historii. Nadal aktualne zostały cele Dyrektywy polegające na zapewnieniu funkcjonowania jednolitego rynku oraz skutecznej ochrony praw podstawowych i wolności osób fizycznych. Została ona jednak przyjęta, gdy Internet jeszcze raczkował.

[550] Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wniosku dotyczącego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, COM(2012)11 final-2012/011 (COD), (Dz. Urz. UE C 229 z 31.07.2012, s. 90-97).

[551] Opinia Europejskiego Inspektora Ochrony Danych z dnia 07.03.2012 r. w sprawie pakietu reform w zakresie ochrony danych (Dz. Urz. UE C 192/7 z 30.06.2012).

[552] Uzasadnienie Rady: Stanowisko Rady (UE) nr 6/2016 w pierwszym czytaniu w sprawie przyjęcia rozporządzenia Parlamentu Europejskiego i Rady…

[553] Komunikat Komisji do Parlamentu Europejskiego na podstawie art. 294 ust. 6 TFUE dotyczący stanowiska Rady dotyczącego przyjęcia Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylającego Dyrektywę 95/46/WE, Bruksela 11.04.2016, COM(2016)214 final, [dostęp:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52016PC0214.

W nowym, wymagającym środowisku cyfrowym, istniejące przepisy nie zapewniają wymaganego stopnia harmonizacji ani niezbędnej skuteczności gwarantującej prawo do ochrony danych osobowych. Zmiany miały umożliwić społeczeństwu większą kontrolę i ułatwić mu dostęp do danych. Zostały one wypracowane z myślą o zapewnieniu ochrony danych osobowych, niezależnie od tego, gdzie się one znajdują. Nowe przepisy miały rozwiać obawy w drodze zapisania „prawa do bycia zapomnianym", tj. zgłoszenia żądania usunięcia, jeśli dana osoba fizyczna nie życzyła sobie dłużej, aby jej dane były przetwarzane oraz pod warunkiem, że nie istnieją uzasadnione przesłanki ich zatrzymania.

Ostatecznie, to Rozporządzenie wprowadziło do unijnego porządku prawnego „prawo do bycia zapomnianym". Chociaż, jak wskazano wcześniej, było ono częścią dorobku prawnego już od orzeczenia TSUE w sprawie *Google Spain,* to dopiero w RODO zostało zdefiniowane w całości jako oddzielna norma prawna.

2.4.2. Prawo do usunięcia danych a „prawo do bycia zapomnianym"

Na gruncie nowych przepisów o ochronie danych osobowych dużo kontrowersji wzbudza art. 17 Ogólnego Rozporządzenia o Ochronie Danych Osobowych, zapewniający osobie, której dane są przetwarzane możliwość zgłoszenia żądania w postaci usunięcia jej danych. Poprzez koncentrowanie przez administratorów nadmiernej uwagi na prawie do usunięcia danych, nie zauważają oni innych nałożonych przez RODO zobowiązań, odnoszących się przykładowo do zastosowania odpowiednich procedur, które zabezpieczą przed potencjalnym zagrożeniem[554].

Można spotkać się z sytuacją, że nazewnictwo „prawa do usunięcia danych" i „prawa do bycia zapomnianym" stosuje się zamiennie, choć zachodzą pewne różnice pomiędzy tymi dwoma uprawnieniami[555]. W mojej ocenie nie są to identyczne prawa, pomiędzy którymi można postawić znak równości. Znaczącym elementem „prawa do bycia zapomnianym" jest możliwość zgłoszenia żądania usunięcia danych, w szczególności w Internecie, przez osobę, której te dane dotyczą lub przez osoby trzecie. Prawo to odnosi się także do procesu przetwarzania danych. „Prawo do bycia zapomnianym" jest pojęciem szerszym od prawa do usunięcia danych. Prawo do usunięcia danych wchodzi w zakres „prawa do bycia zapomnianym". Wniosek ten wynika z tego, że na „prawo do bycia zapomnianym" składają

[554] J. Kamiński, *Prawo do usunięcia danych a polityka retencji danych osobowych,* [dostęp:] https://www.roedl.pl/pl/warto-wiedziec/warto-wiedziec/rodo/prawo-do-usuniecia-danych-a-polityka-retencji-danych-osobowych.
[555] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Transfer danych* osobowych…, s. 155.

się dwie przesłanki, tj. żądanie od administratora niezwłocznego usunięcia danych osobowych (sprowadzające się wyłącznie do prawa do usunięcia danych osobowych) oraz żądanie poinformowania innych administratorów o zgłoszonym żądaniu[556].

Na następujących po sobie etapach procesu legislacyjnego, w przepisie art. 17 RODO sformułowano prawo do usunięcia danych i uznawano je za jedno z podstawowych praw – podobnie, jak w momencie wejścia w życie Dyrektywy 95/46/WE. Jednakże w projekcie Komisji Europejskiej z dnia 25 stycznia 2012 roku to „prawo do bycia zapomnianym" było uważane za jedno ze sztandarowych postulatów. Mimo tego, artykuł 17 unijnego Rozporządzenia wskazywał „prawo do bycia zapomnianym" jako pierwsze oraz prawo do usunięcia danych jako drugie. Zawarcie w art. 17 RODO w pierwotnej wersji zarówno „prawa do bycia zapomnianym", jak i prawa do usunięcia danych osobowych prowadzi do wniosku, że nie były to takie same prawa na etapie prac legislacyjnych. W wersji RODO z pierwszego czytania z dnia 12 marca 2014 roku pominięto „prawo do bycia zapomnianym" i poprzestano na prawie do usunięcia danych. W Rezolucji ustawodawczej Parlamentu Europejskiego nie ma wzmianki na temat tego, dlaczego oponowano przeciwko pozostawieniu „prawa do bycia zapomnianym". W wersji RODO przyjętej przez Radę Unii Europejskiej z dnia 15 czerwca 2015 roku znów wymieniono oba te prawa. W ostateczności, w art. 17 uchwalonego RODO nr 2016/679 z dnia 27 kwietnia 2016 roku prawa te figurują łącznie, ale tym razem nie jako niezależne, lecz tożsame[557]. W finalnej wersji, „prawo do bycia zapomnianym" umieszczono w nawiasie przy prawie do usunięcia danych. To właśnie oznacza, że „prawo do bycia zapomnianym" jest równoznaczne z prawem do usunięcia danych, choć w art. 4 pkt 2 Rozporządzenia nie wskazuje się czynności zapewniających wykonanie „prawa do bycia zapomnianym" jako form przetwarzania, a wymienia się tylko czynności, takie jak usuwanie i niszczenie. Należy wyjaśnić, że usuwanie danych to zarówno niszczenie nośników, jak i taka zmiana danych, która nie pozwala na identyfikację osoby, której dane dotyczą. Zabieg ten wywołuje skutek, który trzeba również przypisać „prawu do bycia zapomnianym". Realizacja tych uprawnień jest nieodwracalna. W przeciwnym wypadku należałoby uważać, że doszło jedynie do zaprzestania przetwarzania danych w określonym celu. Za sprzeczność uznaje się zatem określony niegdyś w art. 17 ust. 1 Rozporządzenia obowiązek „usunięcia danych osobowych oraz zaprzestania dalszego

[556] Spotkałam się z odmienną interpretacją tej problematyki-niektórzy uważają, że nie jest błędem utożsamianie „prawa do bycia zapomnianym" z prawem do usunięcia danych osobowych. Są to terminy równoznaczne, które można stosować zamiennie. Jeszcze inni twierdzą, że „prawo do bycia zapomnianym" dotyczy też usunięcia danych osobowych w sieci, czego nie można powiedzieć o prawie do usunięcia danych osobowych, które obowiązuje w innych obszarach życia, z wyjątkiem Internetu.

[557] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie…,* s. 157.

rozpowszechniania tych danych", a także zawarte w ust. 8 zastrzeżenie, jakoby „w przypadku usunięcia danych, administrator nie przetwarza w inny sposób tych danych osobowych", albowiem wraz z momentem ich realnego usunięcia, dalsze przetwarzanie danych, w tym rozpowszechnianie, jest przecież niemożliwe.

Elementem „prawa do bycia zapomnianym" z art. 17 RODO w pierwotnej wersji, który odróżniał je od usunięcia danych w dotychczasowej formie, był przejaw danych osobowych udostępnionych przez podmiot danych, podczas gdy był on dzieckiem, a więc w wieku poniżej 18 lat. Miało to korespondować z art. 17 RODO, gdzie przypisywano „prawu do bycia zapomnianym" funkcję zatarcia w Internecie danych, mających długotrwały negatywny wpływ na życie osoby, której dane dotyczą, a która w momencie ich ujawniania nie dysponowała doświadczeniem umożliwiającym racjonalne przewidywanie skutków tego posunięcia. Możliwość skorzystania z „prawa do bycia zapomnianym" nie była jedynie dopasowana do osób poniżej 18 roku życia. Co prawda, była to kategoria podmiotów, której prawo to przysługiwało w szczególności, ale nie można powiedzieć, że wyłącznie. Teza ta wynikała z brzmienia art. 17 RODO w jego pierwotnej wersji. Celem uniknięcia nieścisłości, sprowadzających się do tego, jakoby osoby starsze, a więc także i te powyżej 18 lat miały ograniczony dostęp do „prawa do bycia zapomnianym", aktualna wersja art. 17 Rozporządzenia dotyczy już tylko prawa do usunięcia danych, a zarazem pomija wzmiankę o podmiotach danych powyżej 18 roku życia. Roszczenie przysługuje osobie, której dane dotyczą, również w stosunku do stron trzecich przetwarzających jej dane i obejmuje żądanie usunięcia linków do informacji, kopii, bądź replikacji tych danych osobowych. Przyznanie jednostce uprawnienia w postaci wystąpienia z tym żądaniem wobec określonej puli osób, zwiększa zasięg i efektywność postulatu w Rozporządzeniu unijnym, w porównaniu z Dyrektywą 95/46/WE.

W art. 17 ust. 2 RODO uregulowany jest obowiązek podejmowania przez administratora wszelkich koniecznych działań zmierzających do usunięcia upublicznionych przez niego danych, jak też przekazania informacji innym administratorom, którym dane zostały upublicznione o zgłoszonym żądaniu usunięcia danych. Po raz kolejny świadczy to o zwiększeniu praw osób, których dane dotyczą, wobec uchylonej Dyrektywy 95/46/WE. Akt ten w art. 12 lit. c) nakazywał administratorowi zawiadomić osoby trzecie, którym dane zostały upublicznione o ich sprostowaniu, usunięciu albo zablokowaniu, pod warunkiem, że nie okaże się to niemożliwe lub nie będzie wymagało nadmiernego wysiłku. Przepis RODO jest w tym zakresie dość nieprecyzyjny, ponieważ nie określa, jak powinni zachować się wtórni administratorzy w stosunku do takiego ich poinformowania. Poza tym, podmiot

danych nie zawsze wyraża wolę, by jego dane osobowe zostały zlikwidowane przez innych administratorów, a oprócz tego, obowiązek informacyjny zachodzi jedynie wtedy, gdy dane zostały upublicznione, a nie udostępnione. Nie wolno zatem w każdym przypadku traktować „prawa do bycia zapomnianym" jako nierozłączną część prawa do usunięcia danych.

Wymóg ten był znacznie mniej rygorystyczny w zestawieniu z art. 17 ust. 2 Rozporządzenia sprowadzającego się do podjęcia stosownych działań mających na celu usunięcie danych osobowych także przez podmioty trzecie. W pierwszym czytaniu dotyczącym art. 17 ust. 2 RODO postulowano podjąć „wszelkie racjonalne kroki w celu doprowadzenia do usunięcia tych danych", a więc nie tylko do poinformowania, że podmiot danych wniósł takie żądanie. Dyrektywa 95/46/WE ograniczała się do zawiadomienia osób trzecich o usunięciu danych, z kolei art. 17 w ust. 2 Rozporządzenia przewiduje wszelkie racjonalne działania. Nie ma legalnej definicji, co należy rozumieć pod tym pojęciem, stąd też pomiędzy podmiotami danych, jak i administratorami mogą rodzić się konflikty na tle tego, który przepis nakłada na administratorów danych obowiązek stosowania środków prawnych skierowanych do osób trzecich, jeśli tylko lekceważą one informację o usunięciu danych. Wyjątkiem od tej powinności jest upublicznienie danych, które nastąpiło na zasadzie art. 6 ust. 1 Rozporządzenia, w którym sformułowano warunki dopuszczalności przetwarzania danych[558]. W praktyce oznacza to, że usunięcie danych jest ograniczone tylko do przypadków, gdzie upowszechnienie danych miało charakter nielegalny. To doprecyzowanie wiąże się z rezygnacją z „prawa do bycia zapomnianym" w jego pierwszej, bardziej dyscyplinującej, wersji. Prawo to miało przysługiwać nie tylko wtedy, gdy dane zostały upublicznione bez jakiejkolwiek podstawy prawnej, lecz także wówczas, gdy publikacja była zgodna z prawem, ale przykładowo dane osobowe stały się zbędne po upływie określonego czasu. Było to zatem przeciwstawne do zamierzeń instytucji „prawa do bycia zapomnianym", skoro miałoby istnieć tylko jako narzędzie służące do poprawy błędów administratorów danych, na skutek których zostały one upowszechnione.

W dotychczasowym stanie, pozostałością po wcześniej postulowanym „prawie do bycia zapomnianym" jest obowiązek administratora, sprowadzający się do usunięcia upublicznionych przez niego danych osobowych, bez jakiejkolwiek przesłanki prawnej, a tym bardziej określonej w art. 6 ust. 1 Rozporządzenia. „Prawo do bycia zapomnianym" stało się zatem narzędziem umożliwiającym podjęcie stosownych środków służących do naprawy błędu popełnionego przez administratora danych osobowych. Nie ma natomiast zastosowania

[558] Zatem opierało się na podstawie prawnej, takiej jak zgoda podmiotu danych, wykonanie umowy zawartej z podmiotem danych, czy niezbędność do realizacji przez administratora danych obowiązku prawnego.

np. w sytuacji, kiedy dane zostały opublikowane w uprawniony sposób. Co ważne, nie oznacza to jednak, iż podmioty trzecie mają prawo do przetwarzania upublicznionych danych osobowych bez stosownej podstawy prawnej.

Nałożenie na administratora danych osobowych obowiązku w postaci podejmowania wszelkich umotywowanych działań stanowi punkt wyjścia do egzekwowania przy tym od niego należytej staranności. Dokonując jednak głębszej interpretacji tego przepisu, administrator nie ma obowiązku absolutnego osiągnięcia skutku w postaci kompletnego usunięcia upublicznionych danych osobowych. Pomimo tego, że „prawo do bycia zapomnianym" było znaczące dla skuteczności prawa do prywatności, na podobny obowiązek wskazywała Dyrektywa 95/46/WE w art. 12 lit. c), która wymagała poinformowania podmiotów trzecich znajdujących się w posiadaniu ujawnionych danych o ich zablokowaniu, z wyjątkiem sytuacji, kiedy okazałoby się to niemożliwe, bądź wymagało nadmiernego wysiłku.

Unijne Rozporządzenie jasno precyzuje przesłanki pozytywne, na gruncie których można żądać usunięcia danych. Prawo do usunięcia danych osobowych z art. 17 ust. 1 Rozporządzenia, pomijając ograniczenia wynikające z uprzedniego upublicznienia danych bez podstawy prawnej z art. 17 ust. 2 RODO, przysługuje podmiotowi danych w przypadkach wskazanych w ust. 1 lit. a – f, a więc:

a) gdy dane stały się nieprzydatne dla celów, do których zostały zebrane, albo dla których były przetwarzane – nawiązuje to do zasady ograniczenia czasowego, tj. jednej z naczelnych zasad dotyczących przetwarzania danych osobowych z art. 5 ust. 1 lit. e) Rozporządzenia o Ochronie Danych Osobowych, nawiązującej do zakazu przechowywania danych dłużej niż jest to wymagane do celów, dla jakich są wykorzystywane. Realizacja tej zasady potrzebuje określenia przez administratora maksymalnych ram czasowych dla retencji, a więc zatrzymania danych. Tak też, w sytuacji, kiedy wykonanie umowy nie jest jedynym celem przetwarzania danych, niemożliwe staje się zgłoszenie żądania likwidacji danych z uwagi na ustanie celu ich przetwarzania, w szczególności, kiedy przesłanką przetwarzania danych jest wypełnienie obowiązku przez administratora danych osobowych albo wykonanie zadania w interesie publicznym. Uwzględnienie sprzeciwu zgłoszonego przez podmiot danych byłoby wyrazem dla dezaprobaty obowiązkom ciążącym na administratorze danych. Takie rozumowanie jest także kwintesencją wyroku TSUE z dnia 13 maja 2014 r. (sygn. akt: C-131/12), w którym przyznano w Internecie „prawo do bycia zapomnianym", w sytuacji, kiedy publikacja danych była pierwotnie zgodna

z prawem, lecz w związku z upływem czasu przetwarzanie w dalszym ciągu danych osobowych przestało służyć jakiemukolwiek celowi;

b) gdy podmiot danych osobowych cofa zgodę wyrażoną uprzednio w celu przetwarzania jego danych bądź minął okres przechowywania danych, dla którego osoba, której dane dotyczą wyraziła zgodę, a przy tym nie ma innej podstawy prawnej przetwarzania danych. W przeciwieństwie do Dyrektywy 95/46/WE, Rozporządzenie o Ochronie Danych Osobowych w art. 7 ust. 3 bezpośrednio nadaje podmiotowi danych uprawnienie w zakresie odwołania udzielonej na ich przetwarzanie zgody[559]. Rozporządzenie unijne w art. 17 ust. 1 lit. b) dopuszcza możliwość udzielenia tzw. zgody czasowej. Usunięcie danych jest obowiązkowe, gdy zgoda podmiotu danych jest wyłączną przesłanką dopuszczalności poddania ich procesowi przetwarzania. W przypadku natomiast, kiedy istnieją inne powody wynikające z treści przepisu 6 ust. 1 lit. a – f Rozporządzenia, braku zgody nie należy utożsamiać z brakiem przesłanek prawnych dalszego przetwarzania danych osobowych, a zatem nie prowadzi to do konieczności usunięcia danych. Warte podkreślenia jest to, że często podmiot danych błędnie twierdzi, że w sytuacji odwołania przez niego zgody, dane zostaną kompleksowo usunięte, zapominając przy tym, iż zarówno jego, jak i administratora może dodatkowo łączyć umowa, do realizacji której w dalszym ciągu są wymagane konkretne dane. Usunięcia danych może żądać ponadto rodzic czy opiekun prawny dziecka, które korzysta z usług internetowych na podstawie wcześniej udzielonej zgody;

c) gdy osoba, której dane osobowe dotyczą wniosła sprzeciw w związku z ich przetwarzaniem, zgodnie z przesłankami określonymi w art. 19 Rozporządzenia. Podstawą zgłoszenia sprzeciwu mogą być powody odnoszące się do szczególnej sytuacji podmiotu danych, w tym m.in. w przypadku, gdy celem przetwarzania jest wykonanie prawnie uzasadnionych interesów administratora lub strony trzeciej, w tym profilowanie (art. 21 Ogólnego Rozporządzenia o Ochronie Danych Osobowych). Wówczas uwzględnienie sprzeciwu prowadzące do usunięcia danych jest uzależnione od zbadania, czy sytuacja, w której znajduje się wnioskodawca jest na tle innych wysoce odmienna, a także czy nie występują prawnie uzasadnione przesłanki przetwarzania nadrzędne w zestawieniu z prawem do wniesienia sprzeciwu oraz wobec interesów wnioskodawcy. Przedmiotem sprzeciwu może okazać się

[559] M. Krzysztofek, *Zmiana przepisów o zgodzie na przetwarzanie danych osobowych,* „Przegląd Prawa Handlowego" 2011, nr 4, s. 57.

przetwarzanie danych na potrzeby marketingu bezpośredniego, jak również profilowanie w zakresie związanym z tym marketingiem. Wtedy prawo do sprzeciwu jest bezwarunkowe. Obowiązek usunięcia danych powstaje, gdy nie ma innych podstaw przetwarzania;

d) gdy sąd albo administracyjny organ regulacyjny z siedzibą w Unii Europejskiej zadecydował o kategorycznym usunięciu danych, bądź też dane osobowe muszą zostać usunięte celem wywiązania się z obowiązku prawnego określonego w prawie Unii Europejskiej lub w prawie kraju członkowskiego, któremu podlega administrator. Administrator może przechowywać dane osoby, która domaga się ich usunięcia, jeśli jest to niezbędne do wywiązania się z prawnego obowiązku, jaki na nim spoczywa, bądź w sytuacji ustalenia, dochodzenia albo obrony roszczeń. Stąd też, w przypadku wpłynięcia wniosku o usunięcie danych osobowych, administrator powinien zbadać, czy takie żądanie jest uzasadnione, tj. czy zachodzą pozytywne przesłanki usunięcia danych oraz czy roszczenie nie podlega żadnym ograniczeniom. Jeżeli zatem przesłanki te zostaną spełnione, to administrator jest zobowiązany do usunięcia danych;

e) gdy poddanie danych osobowych procesowi przetwarzania jest z innych powodów nielegalne od tych określonych w art. 17 ust. 1 RODO. Jak słusznie można zauważyć, przesłanka ta wiąże się z zasadą legalności, formułującej w art. 5 ust. 1 lit. a) Rozporządzenia wymóg, aby dane osobowe były przetwarzane zgodnie z prawem. Obowiązek legalnego przetwarzania danych polega na zgodności z przepisami rangi ustawy, rozporządzenia, prawa materialnego, proceduralnego oraz judykatury. Najściślej rzecz ujmując, nielegalne przetwarzanie danych odbywa się bez podstawy prawnej lub w celu niezgodnym z prawem. Zadanie administratora polega na zagwarantowaniu legalnego przetwarzania danych, a więc na podstawie art. 4 pkt 2 RODO, który znajduje swój odpowiednik w art. 2 lit. b) Dyrektywy 95/46/WE. Obejmuje etap, począwszy od zebrania do usunięcia danych, w oparciu o co najmniej jedną z przesłanek dopuszczalności przetwarzania danych uregulowanych w art. 6 RODO (art. 7 Dyrektywy). Sprowadza się to do zakazu pozyskiwania i przetwarzania danych w sposób niezgodny z prawem, np. gdy podstawą przetwarzania danych ma być zgoda podmiotu danych, to musi być ona jednoznaczna i wyrażona swobodnie. Proces przetwarzania danych cechuje się legalnością, pod warunkiem, że dokonuje się na podstawie aktu rangi ustawowej oraz jest niezbędny w demokratycznym społeczeństwie do osiągnięcia uzasadnionego celu. Przepis art.

17 ust. 1 lit. d) RODO nie konkretyzuje rodzajów niezgodności z prawem, które uzasadniają proces usunięcia danych. Przykładowo, obowiązki informacyjne administratorów danych należą do podstawowych zadań, z których muszą się wywiązać. Jednakże, nie oznacza to, że mogące wystąpić nieprawidłowości w ich wypełnieniu determinują usunięcie danych. Usunięcie danych może być jedynie skutkiem niewykonania bądź nieprawidłowego wykonania obowiązku informacyjnego, gdy przetwarzanie danych jest uzależnione od zgody lub braku sprzeciwu osoby, której dotyczą, bowiem warunkiem ważności oświadczenia o zgodzie jest świadomość wszystkich aspektów planowanego przedsięwzięcia[560];

f) gdy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego świadczonych bezpośrednio dziecku na podstawie zgody na przetwarzanie danych. Usługi społeczeństwa informacyjnego to nic innego, jak wszystkie usługi świadczone za wynagrodzeniem, na odległość, drogą elektroniczną oraz na indywidualne żądanie odbiorcy usług[561]. Nie jest zakazane przetwarzanie danych dzieci w wieku powyżej 16 lat na podstawie udzielonej przez nich zgody w celu świadczenia im bezpośrednio usług społeczeństwa informacyjnego, a poniżej tego wieku jedynie w przypadku, kiedy zgodę wyraziła osoba sprawująca władzę rodzicielską nad dzieckiem lub opiekę prawną. Powiązanie instytucji „prawa do bycia zapomnianym" z granicą wieku ma znaczenie w tym kontekście, że celem tego uprawnienia jest ochrona osób, które wyraziły zgodę na przetwarzanie danych jeszcze jako dzieci, a zatem bez wystarczającej świadomości swojego postępowania[562].

Nakaz usunięcia danych osobowych z uwagi na żądanie podmiotu z powodu niezgodności z prawem, a ściślej rzecz ujmując z Rozporządzeniem, co nie zostało wymienione w art. 17 ust. 1 lit. d) RODO, budzi wątpliwości ze względu na fakt, że obowiązki informacyjne wyrażone w art. 13a i art. 14 ust. 1 – 3 Rozporządzenia mieszczą się w kategorii podstawowych obowiązków administratorów danych, a zatem zbieranie danych i jego zgodność z prawem zależna jest od sumiennej realizacji obowiązków administracyjnych przez administratora. Niemniej jednak, wydaje się, iż nieprawidłowe spełnienie obowiązku administracyjnego przysługującego wobec podmiotu danych nie należy

[560] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Transfer…,* s. 159-161.
[561] Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, [dostęp:] https://eur-lex.europa.eu/eli/dir/2015/1535/oj.
[562] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Transfer…,* s. 160-161.

bezwzględnie traktować jako niezgodność z prawem procesu przetwarzania danych osobowych. Obowiązkowi informacyjnemu towarzyszą inne, liczne zasady legalności przetwarzania. Warunkiem legalności poddawania danych procesowi przetwarzania jest wykazanie przez administratora danych jednej z podstaw z art. 6 RODO, a także spełnienie dodatkowych zobowiązań określonych w przepisach o ochronie danych osobowych. Niewykonanie zaś obowiązku informacyjnego jest znaczącym naruszeniem, ale nie w każdym przypadku świadczy o nielegalności procesu przetwarzania. Zakaz przetwarzania danych może być rezultatem niewykonania bądź nienależytego wykonania obowiązku informacyjnego jedynie w sytuacji, gdy dla dopuszczalności przetwarzania danych wymagana jest zgoda albo brak sprzeciwu osoby, której dane dotyczą, gdyż warunkiem prawidłowości oświadczenia o zgodzie jest świadomość beneficjenta w zakresie wszystkich kwestii planowanego przetwarzania[563].

Do kluczowych zasad przetwarzania danych należy również obowiązek zapewnienia ścisłości oraz w uzasadnionych przypadkach aktualności danych z art. 5 ust. 1 lit. d) Rozporządzenia. Z tego wynika, że przetwarzanie danych nieścisłych oraz nieaktualnych nie jest zgodne z przepisami Rozporządzenia unijnego, a zatem może to zostać uznane za przesłankę uzasadniającą zgłoszenie żądania usunięcia danych na podstawie art. 17 ust. 1 lit. d) Rozporządzenia. Te dwa terminy zostały bezpośrednio wskazane w art. 16 Rozporządzenia, na mocy którego osoba, której dane dotyczą posiada uprawnienie do żądania poprawienia albo uzupełnienia przez administratora danych nieprecyzyjnych lub niekompletnych. Przepisu tego nie można jednak łączyć z prawem żądania usunięcia danych, w przeciwieństwie do art. 12 lit. b) Dyrektywy 95/46/WE. Z kolei zaś art. 5 ust. 1 lit. d) Rozporządzenia nakazuje podjęcie działań dla zagwarantowania niezwłocznego usunięcia lub poprawienia danych osobowych, które są nieścisłe, biorąc pod uwagę cele ich przetwarzania. Regulacja art. 17 ust. 4 lit. a) Rozporządzenia dopuszcza możliwość odstąpienia od usunięcia danych przez administratora, a w zamian za to poddanie ich procesowi przetwarzania bez zwykłego dostępu i przymusu dokonywania operacji na danych, jeżeli powodem żądania podmiotu jest nieścisłość danych, ale tylko podczas czasu niezbędnego do sprawdzenia przez administratora danych ich prawidłowości. Zbieżność tych regulacji powoduje wątpliwość w kwestii, czy niepoprawność lub niekompletność danych motywuje jedynie żądanie ich poprawy w oparciu o treść art. 16 Rozporządzenia, czy także żądanie ich usunięcia na podstawie art. 5 ust. 1 lit.

[563] Stanowisko odmienne zajęli J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…,* s. 480, którzy uznali realizację obowiązku informacyjnego za warunek legalności zbierania danych. Z tym stwierdzeniem polemizują P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2016, s. 248.

d) oraz art. 17 ust. 1 lit. d) Rozporządzenia.

Unijne Rozporządzenie przyznaje osobie, której dane dotyczą uprawnienie do żądania od administratora usunięcia danych osobowych w wypadkach wskazanych w art. 17 ust. 1 lit. a – d RODO, bez względu na to, że przesłanki te wykluczają przetwarzanie danych niezależnie od sprzeciwu podmiotu danych w sytuacji jego złożenia. Tak też, cofnięcie lub ustanie zgody na przetwarzanie danych w przypadkach, kiedy była ona wyłączną podstawą procesu przetwarzania, należy utożsamiać z brakiem podstawy prawnej przetwarzania, a zatem jego niedopuszczalność. Kolejnym przykładem jest uregulowanie w art. 17 ust. 1 lit. c) Rozporządzenia instytucji sprzeciwu na warunkach określonych w art. 19 RODO, będącej przesłanką usunięcia danych na podstawie zgłoszenia żądania przez podmiot danych, mimo że art. 19 ust. 3 Rozporządzenia wprost wskazuje, iż w sytuacji sprzeciwu, na administratorze danych ciąży obowiązek zaprzestania przetwarzania danych osobowych dla celu, którego dotyczył ujawniony sprzeciw. Prawo podmiotu danych do żądania od administratora ich usunięcia w przypadkach wskazanych w unijnym Rozporządzeniu jest instrumentem ułatwiającym egzekwowanie przez podmiot danych tego obowiązku, gdy administrator danych go nie wykonał, pomimo że był do tego zobowiązany na podstawie przepisów prawa.

2.4.3. „Prawo do bycia zapomnianym" w regulacjach prawnych RODO

Na gruncie prawa polskiego brak jest regulacji wprost odnoszącej się do „prawa do bycia zapomnianym". Znajduje się ona w prawie Unii Europejskiej, w głównej mierze w art. 17 Rozporządzenia o Ochronie Danych Osobowych. Jednakże RODO odwołuje się także do „prawa do bycia zapomnianym" w innych unormowaniach. Już w motywie 65 preambuły zauważono, że każdej osobie fizycznej powinno przysługiwać uprawnienie do sprostowania danych osobowych jej dotyczących oraz „prawo do bycia zapomnianym".

Celem zapewnienia podmiotom danych pełnej ochrony, unijny prawodawca wyróżnił katalog przypadków, gdzie możliwa jest sytuacja zatrzymania danych, mianowicie:

1) przy korzystaniu z prawa wolności wypowiedzi i informacji, co jest najbardziej kontrowersyjną kwestią urzeczywistniania „prawa do bycia zapomnianym";
2) w celu realizacji interesu publicznego w dziedzinie zdrowia publicznego;
3) w celu prowadzenia dokumentacji, statystyk i badań naukowych;
4) odnosząca się do wypełniania przez administratora obowiązku zatrzymania danych, wynikającego z prawa unijnego bądź krajowego;

5) w celu ograniczenia przetwarzania danych, które jest możliwe zamiast ich usuwania, gdy:
    - podmiot kwestionuje ścisłość danych;
    - przechowywanie danych jest konieczne dla celów dowodowych;
    - podmiot kieruje wniosek o ograniczenie wykorzystywania danych, których przetwarzanie nie jest zgodne z prawem, ale jednocześnie nie mogą one zostać usunięte z uwagi na sprzeciw podmiotu danych;
    - dane poddawane są procesowi przetwarzania w związku z ich przekazywaniem do innego automatycznego systemu przetwarzania[564].

Pomimo tego, że stosowanie powyższych wyjątków nie jest do końca zrozumiałe, są one potrzebne dla zachowania równowagi pomiędzy „prawem do bycia zapomnianym" a innymi prawami podstawowymi. Zainteresowanie literatury wzbudza prawo wolności wypowiedzi stojące w pewnym stopniu w sprzeczności z metodami realizacji „prawa do bycia zapomnianym". Zależność między wolnością słowa a prawem do ochrony danych wymaga wykładni sposobu urzeczywistniania „prawa do bycia zapomnianym" w kontekście informacji przekazanych do udostępnienia. Zestawienie ze sobą tych dwóch praw określa się mianem *media exception.* To zastosowanie przy łącznej interpretacji art. 17 i art. 80 Rozporządzenia może wzbudzać pewne wątpliwości. Zgodnie z treścią art. 80, każde z krajów członkowskich stosuje środki zmierzające do zagwarantowania współistnienia obu tych praw. Obecne brzmienie tego przepisu daje państwom członkowskim swobodę analizy regulacji Rozporządzenia, dlatego, że prawodawca unijny nie konkretyzuje wprost zakresu ograniczeń i odstępstw. W tym kontekście trzeba poddać pod rozwagę zakres funkcjonowania działalności gospodarczej. Coraz bardziej jest ona popularna, obok aktywności blogerów oraz użytkowników forów internetowych. Za tego typu działalność coraz częściej zaczęto uważać taką, której przedmiotem jest publiczne rozpowszechnianie informacji i opinii bez względu na wykorzystywany rodzaj nośnika do ich przekazania. Instytucję „prawa do bycia zapomnianym" można pogodzić z wolnością słowa przy jednoczesnym wypracowaniu pewnych procedur na poziomie krajów członkowskich. Z praktycznego punktu widzenia, to właśnie organy krajowe, na których leży obowiązek sprawowania kontroli nad sposobem przetwarzania danych, będą współtworzyć zakres „prawa do bycia zapomnianym" i wypełniać treścią przepisy Rozporządzenia.

[564] E. Shoor, *Narrowing the right to be forgotten: why the European Union needs to amend the proposed data protection regulation,* "Brooklyn Journal of International Law" 2014, nr 38, s. 505.

Przepisy Rozporządzenia unijnego jasno normują, że wymagane jest wzmocnienie „prawa do bycia zapomnianym", zwłaszcza w sieci. W motywie 66 preambuły podnosi się, że jeżeli administrator upublicznił dane osobowe niezgodnie z przesłankami, to ma obowiązek je usunąć. Powinien jednak przy tym wziąć pod rozwagę dostępną technologię i koszt realizacji[565]. Stąd też, RODO posługuje się sformułowaniem, że administrator „winien podjąć rozsądne działania", przez które rozumie się takie środki techniczne, dzięki jakim administratorzy przetwarzający dane osobowe są informowani o tym, iż osoba, której dane dotyczą żąda, by usunęli wszelkie łącza do tych danych, kopie danych osobowych, bądź ich replikacje. Takie rozwiązanie powoduje szereg wątpliwości w praktyce, zwłaszcza podczas interpretacji zasięgu odpowiedzialności za publikację danych oraz w odniesieniu do art. 13 unijnego Rozporządzenia, sankcjonującego ogólny obowiązek administratora zobowiązujący do informowania każdego odbiorcy, któremu zostały udostępnione dane o ich poprawieniu i usunięciu w oparciu o przepis art. 16 oraz 17 RODO[566]. Z treści art. 17 Rozporządzenia wynika, iż obowiązek administratora danych sprowadza się tylko do podjęcia pewnych działań, nie zaś do efektywnego poinformowania osób trzecich o wystąpieniu danej sytuacji.

Odwołanie się unormowań Rozporządzenia unijnego do „prawa do bycia zapomnianym" jest też pośrednio widoczne w art. 16, który nadaje zainteresowanym osobom prawo do sprostowania ich danych, które są nieprawidłowe. W odniesieniu do celów przetwarzania, osoba, jakiej dane dotyczą ma również prawo żądania uzupełnienia niekompletnych danych osobowych[567]. Artykuł 17 RODO ma znaczenie, bowiem nadaje uprawnienie do usunięcia danych, bezpośrednio używając określenia „prawo do bycia zapomnianym". Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, natomiast na administratorze ciąży ustawowy obowiązek usunięcia danych osobowych bez zbędnej zwłoki, jeżeli zachodzi jedna z następujących okoliczności:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;

[565] https://rodoradar.pl/motywy-61-75/.
[566] M.L. Ambrose, J. Ausloos, *The right to be forgotten across the pond,* "Journal of Information Policy" 2013, nr 3, s. 13.
[567] Odbywa się to poprzez przedstawienie dodatkowego oświadczenia.

3) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;
4) dane osobowe były przetwarzane niezgodnie z prawem;
5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator;
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1[568].

W dokumencie tym, szczególną uwagę zwraca się na to, że „prawo do bycia zapomnianym" ma doniosłe znaczenie w sytuacji, kiedy osoba, której dane dotyczą wyraziła zgodę jako dziecko, czyli wtedy, kiedy nie była w pełni świadoma konsekwencji swojego działania związanego z procesem przetwarzania danych, a w późniejszym czasie wyraża wolę usunięcia takich danych osobowych, zwłaszcza z Internetu. Osoba, której dane dotyczą powinna mieć możliwość wykonania tego prawa, mimo że już nie pozostaje w wieku dziecięcym. Przepisy RODO w kwestii „prawa do bycia zapomnianym" uznają, że obowiązek usunięcia danych o prywatności człowieka nie posiada charakteru absolutnego. Analizując uprawnienie „prawa do bycia zapomnianym" na zasadzie regulacji unijnego Rozporządzenia, trzeba dostrzec, iż regulacje prawne wprowadzają własną definicję terminu danych osobowych. Dane o prywatności człowieka, a zatem jego dane osobowe, w oparciu o treść art. 4 pkt 1 Rozporządzenia określają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. To szerokie pojęcie odnosi się do danych opublikowanych bezpośrednio przez podmiot danych, jak też przez osoby trzecie. Trudności praktyczne może sprawiać określenie stopnia powiązania informacji z podmiotem danych[569]. Możliwa do zidentyfikowania osoba fizyczna to osoba, której tożsamość można bezpośrednio albo pośrednio ustalić, zwłaszcza na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji czy identyfikatora internetowego. Można to zrobić również poprzez dostrzeżenie czynników charakterystycznych dla konkretnego podmiotu w sferze fizycznej, fizjologicznej, genetycznej, psychicznej, ekonomicznej, kulturowej lub społecznej. Przez odbiorcę tych danych, a więc osobę, do której mogą one dotrzeć, uważa się zgodnie z art.

[568] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679…
[569] J. Rosen, *The Right to be Forgotten…,* s. 92.

4 pkt 9 Rozporządzenia osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu udostępnia się dane osobowe, bez względu na to, czy jest osobą trzecią. Osoba trzecia w rozumieniu przepisów RODO, a konkretnie w kontekście przepisu art. 4 pkt 10, to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot niż osoba, której dane dotyczą, jak również administrator, podmiot dokonujący przetwarzania czy osoby uprawnione do przetwarzania danych osobowych z upoważnienia administratora lub podmiotu przetwarzającego.

W Ogólnym Rozporządzeniu o Ochronie Danych Osobowych szczególny nacisk położono na ochronę człowieka. Ochrona danych osobowych ma charakter jedynie następczy. W pierwszej kolejności chroniona jest jednostka i jej sfera prywatności. Rozwiązania prawne przyjęte na szczeblu Unii Europejskiej są szansą na polepszenie sytuacji słabszego podmiotu w styczności z podmiotami, które mają zasięg globalny. Są przejawem demokratyzacji prawa, ponieważ dają skuteczniejszy dostęp pokrzywdzonym do środków zapewniających ochronę ich praw w wyniku naruszenia poprzez zastosowanie nowych technologii jako otwartej platformy. Narzucane przez Unię Europejską pewne sposoby działania służą do zredukowania wyrządzenia szkody, zarówno w sferze moralnej, jak i materialnej.

„Prawo do bycia zapomnianym" zawiera w sobie nieścisłości, niemniej jednak jego uwzględnienie w systemie ochrony danych należy ocenić pozytywnie, szczególnie w kontekście celów proponowanych rozwiązań na poziomie unijnym, przejawiających się w zwiększaniu kontroli jednostek w zakresie wykorzystania informacji ich dotyczących oraz w zapewnieniu przejrzystych mechanizmów ochrony, w tym w propagowaniu ochrony danych osobowych w Internecie. Co ważne, „prawu do bycia zapomnianym" zarzuca się aktualnie konflikt z innymi podstawowymi prawami i wolnościami, czy niedoprecyzowanie procedur i sposobu usuwania danych objętych kontrolą, jak też niedookreślenie regulacji w sytuacji informowania podmiotów trzecich o skorzystaniu przez jednostkę z „prawa do bycia zapomnianym". Kolejny problem przejawia się w niedostosowaniu praktycznych możliwości administratorów danych z uwagi na techniczne ograniczenia i brak możliwości kontrolowania każdego użytkownika sieci korzystającego z dotąd udostępnionych informacji. Wobec tego, zrozumiałe jest, że obok praktycznych i teoretycznych kwestii, istotne jest projektowanie udoskonaleń technologicznych[570].

W związku z tym, że „prawo do bycia zapomnianym" stanowi pewne novum, to wskazuje się na konieczność przyzwyczajenia społeczeństwa, składającego się

[570] M.L. Ambrose, J. Ausloos, *The right to be forgotten across the pond…,* s. 22-23.

z poszczególnych jednostek, do korzystania z niego. Przede wszystkim ludność w nowoczesnym świecie, aby promować „prawo do bycia zapomnianym" powinna być z nim zaznajomiona i oswojona. Tak też, niektóre podmioty w sposób negatywny są nastawione wobec procesu urzeczywistniania tego prawa. Może to zostać odebrane jako rodzaj „pośredniej cenzury"[571]. Zamierzeniem prawodawców było przygotowanie na poziomie unijnym takiej reformy, która spowoduje wzrost efektywności prawa podstawowego do ochrony danych, przy jednoczesnym zapewnieniu osobom fizycznym kontroli nad swoimi danymi. Stworzenie „prawa do bycia zapomnianym" usprawniło wymiar ochrony danych związany z rynkiem wewnętrznym poprzez wzmocnienie spójności. Intencje te spowodowały, że „prawo do bycia zapomnianym" uwzględnione zostało w Rozporządzeniu, a ich całościowe wykonanie korelowało z zamiarem stworzenia kompleksowego systemu ochrony danych we wszystkich sferach funkcjonowania podmiotów. Niemniej jednak, uruchomienie należytych procedur kontrolnych oraz próba faktycznego wdrażania „prawa do bycia zapomnianym" mogły okazać się fiaskiem i powodować wrażenie niskiej efektywności nowego Rozporządzenia. Realizowanie jednak tych rozwiązań przyczyniło się do powstania nowej cybergeneracji praw człowieka, pośród której jednym z fundamentalnych praw jest właśnie „prawo do bycia zapomnianym".

2.5. „Prawo do bycia zapomnianym" w judykaturze

„Prawo do bycia zapomnianym" było także przedmiotem zainteresowania TSUE w późniejszych latach. W wyroku z dnia 24 września 2019 r. w sprawie C-507/17[572] Trybunał zauważył, że „operator wyszukiwarki odpowiada nie za to, iż dane osobowe objęte tymi przepisami znajdują się na stronie internetowej opublikowanej przez osobę trzecią, ale za odsyłanie do tej strony, a w szczególności za wyświetlenie linku do niej na udostępnianej internautom liście wyników wyszukiwania, którego punktem wyjścia jest imię i nazwisko danej osoby fizycznej"[573], wobec czego „operator musi na podstawie wszystkich istotnych elementów danego przypadku i uwzględniając powagę ingerencji w prawa podstawowe do poszanowania życia prywatnego oraz ochrony danych osobowych przysługujących osobie, której dane dotyczą, sprawdzić, czy umieszczenie linku do danej strony internetowej na

[571] P. Fleischer, *Foggy thinking about the right to oblivion,* [dostęp: 22.07.2014] http://peterflesicher.blogspot.com/2011/03/foggy-thinking-about-the-right-to-oblivion.html.
[572] Wyrok TSUE z dnia 24 września 2019 r. w sprawie *Google LLC przeciwko Commission Nationale de I'informatique et des Libertés (CNIL),* sygn. akt: C-507/17, [dostęp:] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CC0507.
[573] *Tamże.*

wyświetlanej liście wyników wyszukiwania, mającego za punkt wyjścia imię i nazwisko tej osoby, jest ściśle niezbędne do ochrony prawa do wolności informacji przysługującego internautom potencjalnie zainteresowanym uzyskaniem, dzięki takiemu wyszukiwaniu, dostępu do tej strony internetowej”[574].

Odnośnie do wyszukiwarek internetowych uznanych za administratorów, TSUE w wyroku w sprawie Google LLC/CNIL zmodyfikował stanowisko co do zakresu terytorialnego żądania usunięcia danych. O ile w wyroku Google Spain przyjął on, że usunięcie z listy wyników wyszukiwania dotyczy również pozaeuropejskich wyszukiwarek internetowych, to w wyroku Google LLC/CNIL ograniczył ten zasięg do wyszukiwarek krajów członkowskich Unii Europejskiej. Zastosowany w ramach przedmiotowego orzeczenia mechanizm geoblokady doprowadził do odejścia od uniwersalnej opcji „prawa do bycia zapomnianym”.

W sprawie wniesionej przez Google przeciwko francuskiemu organowi do spraw ochrony danych osobowych, Trybunał Sprawiedliwości Unii Europejskiej został zobligowany do ustosunkowania się do pytania dotyczącego geograficznego zakresu obowiązywania „prawa do bycia zapomnianym”[575]. W 2016 roku, organ francuski nałożył na Google karę grzywny w wysokości 100 tys. Euro za odmowę globalnej realizacji „prawa do bycia zapomnianym”. Nakazał wykonanie tego prawa w odniesieniu do wszystkich domen Google, w tym do google.com. W odpowiedzi stwierdzono, że organ ds. ochrony danych ma prawo do wydania takich nakazów jedynie w nawiązaniu do francuskiej domeny google.fr. Trybunał Sprawiedliwości UE orzekł, że „prawo do bycia zapomnianym” nie dotyczy linków wyświetlanych w każdej wersji wyszukiwarki internetowej na świecie, ale obowiązuje w przypadku wyszukiwarek internetowych w domenach o nazwach powiązanych z krajami członkowskimi Unii Europejskiej, tzn. nie tylko google.fr, ale także np. google.it, czy google.nl. Na operatorów wyszukiwarek internetowych został nałożony, w razie takiej potrzeby, obowiązek stosowania środków, które faktycznie uniemożliwiają internautom, przeprowadzającym z terytorium państwa członkowskiego wyszukiwanie w oparciu o imię i nazwisko, uzyskanie dostępu do usuniętych linków, bądź przynajmniej poważnie zniechęcają ich do uzyskania takiego dostępu.

Z przedstawionych wyżej wyroków TSUE wynika, że „prawo do bycia zapomnianym” stało się przedmiotem dogłębnych analiz w aspekcie żądań kierowanych do operatora

[574] *Tamże.*
[575] Decyzja CNIL z 10.03.2016 r., nr 2016-054, [dostęp:] https://www.cnil.fr/fr/decision-n-2016-054-du-10-mars-2016.

wyszukiwarki internetowej przez osobę, której dane dotyczą. Wprowadzenie przez Trybunał Sprawiedliwości Unii Europejskiej mechanizmu „geoblokady" można łatwo obejść, a więc skuteczność „prawa do bycia zapomnianym" zdaje się być ograniczona[576]. Skoro skutkiem „prawa do bycia zapomnianym" nie jest całkowite usunięcie linku z wyszukiwarki i dostęp do informacji na temat konkretnej osoby jest nadal możliwy, z tym, że przy użyciu innych haseł wyszukiwania aniżeli imię i nazwisko, to realizacja „prawa do bycia zapomnianym" powinna mieć charakter uniwersalny.

Na gruncie polskich przepisów prawa, skorzystanie z „prawa do bycia zapomnianym" miało miejsce w toku postępowania sądowego, gdzie ujawniły się główne problemy związane z dochodzeniem usunięcia treści zamieszczanych w Internecie przy zastosowaniu art. 24 k.c.[577]. W pierwszej kolejności, Sąd Najwyższy pochylił się nad problematyką precyzyjnego określenia żądania oraz redagowania sentencji orzeczenia w sposób stanowczy, tak aby żadna ze stron nie miała możliwości jego modyfikacji i własnej interpretacji[578]. Nie stanowi tego wymagania zobowiązanie strony do podjęcia czynności zmierzających do usunięcia danych z portali internetowych, w tym skierowanie żądania do właścicieli lub administratorów portalu. W judykaturze nie wskazano konkretnego zakresu czynności, które powodowałyby usunięcie skutków naruszenia dobra osobistego w sieci. Ciężar sformułowania żądania spoczywa na osobie, która chce skorzystać z „prawa do bycia zapomnianym". Z powodu braku ujednoliconych procedur prawnych, ujęcie oświadczenia o chęci skorzystania z „prawa do bycia zapomnianym" jest znacznie utrudnione. Dostępność treści powodującej naruszenie dóbr osobistych strony skarżącej nie jest jedynie następstwem działań naruszającego, ale także niekontrolowanego postępowania podmiotów trzecich, które uzyskały dostęp do treści w związku z jej pierwotnym udostępnieniem. Sąd Najwyższy w sprawie wytoczonej przeciwko Skarbowi Państwa – Komendantowi Policji w przedmiocie ochrony dóbr osobistych stanął na stanowisku, że nie wolno traktować zachowań anonimowych osób użytkujących usługi internetowe za rezultat naruszenia w rozumieniu art. 24 k.c. Ten tok rozumowania prowadzi do konkluzji, że żądanie podjęcia działań mających na celu usunięcie treści zamieszczonych na portalach internetowych, nie zawiera się w granicach środków

[576] Możliwe to jest poprzez użycie narzędzia *Virtual Private Network* (dostęp do globalnego Internetu jest zachowany, ukrywając lokalizację użytkownika, co oznacza, iż zastosowana wobec krajów członkowskich UE technika geoblokowania wyszukiwania jest fikcją).
[577] Wyrok SN z dnia 14 stycznia 2015 r., sygn. akt: II CSK 747/13, OSNC 2016, nr 1, poz. 9.
[578] Uchwała SN z dnia 20 września 1988 r., sygn. akt: III CZP 37/88, OSNCP 1989, nr 3, poz. 40.

zmierzających do usunięcia skutków naruszenia w rozumieniu art. 24 k.c.[579]. Umożliwiono jednak podjęcie takich środków, które zobowiążą naruszającego do zawiadomienia danych podmiotów, w których interesie leży zarządzanie portalami internetowymi, że znajdują się tam informacje prawomocnie uznane za naruszające dobra osobiste. Analogiczne rozwiązanie zostało przyjęte w unijnym Rozporządzeniu, przy czym z niego nie wynika, że to osoba domagająca się usunięcia treści ma wskazać portale, które należy powiadomić o tym, że znajduje się na nich dana informacja. Z treści art. 17 ust. 2 RODO wynika, iż obowiązek identyfikacji administratorów przetwarzających treść nałożono na administratora, do którego najpierw skierowano żądanie usunięcia. Wykładnia tego przepisu nie może być uznana za racjonalne działanie ustawodawcy, ponieważ jest wiele sposobów powielania treści. Mogą być one rozpowszechniane poprzez kopiowanie za pomocą narzędzi elektronicznych czy ręczne przepisywanie treści. Stąd też kontrola nad zwielokratnianiem informacji jest znacznie utrudniona, prawie niemożliwa. Obowiązek administratora w przedmiocie poinformowania podmiotów, którym udzielił zgody na skopiowanie danych nie jest szczególnie propagowany. Sensowniejszym do przyjęcia rozwiązaniem jest zobowiązanie administratora do poszukiwania kopiujących. Zakres tego obowiązku powinien być wyznaczony, uwzględniając technologiczne możliwości, koszty i postulat proporcjonalności. W zależności od rodzaju danych osobowych poziom ich ochrony i aktywności administratora może być większy lub mniejszy. W polskim porządku prawnym zwykło się przyjąć, że jeżeli jakaś treść, która naruszyła dobro osoby, została udostępniona nieoznaczonemu kręgowi osób, to czynności mające na celu doprowadzenie do zaprzestania naruszeń, również powinny dotrzeć do tego kręgu. Zgodnie z tym twierdzeniem, jeśli dane osobowe podmiotu, który skorzystał z „prawa do bycia zapomnianym" zostały udostępnione na stronie internetowej, to informacja o tym także powinna zostać opublikowana na tej stronie[580]. Jednakże takie rozumienie jest błędne, ponieważ liczba osób mogących zapoznać się z materiałem zawierającym konkretne dane osobowe w porównaniu z liczbą osób, do których dotrze informacja o skorzystaniu z „prawa do bycia zapomnianym" jest niewspółmierna.

2.6. Ocena regulacji RODO – podsumowanie dwuletniego okresu obowiązywania

W dniu 24 czerwca 2020 roku Komisja Europejska skierowała do Parlamentu

[579] Ośmieszająca powódkę rozmowa telefoniczna z funkcjonariuszem policji, który przyjął zgłoszenie, została nagrana przez Komendę Powiatową Policji, a następnie wprowadzona do Internetu przez nieustaloną osobę. Zob. Wyrok SN z dnia 14 stycznia 2015 r., sygn. akt: II CSK 747/13…
[580] Wyrok SN z dnia 19 maja 2011 r., sygn. akt: I CSK 497/10, LEX nr 936483.

Europejskiego i Rady Komunikat podsumowujący dwa lata stosowania Ogólnego Rozporządzenia o Ochronie Danych Osobowych[581]. Dokument stanowił pierwsze sprawozdanie z oceny i przeglądu RODO, zwłaszcza w odniesieniu do stosowania i funkcjonowania regulacji dotyczących przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych oraz odnoszących się do współpracy i spójności zgodnie z art. 97 Rozporządzenia. W wyniku przeprowadzonych obserwacji wysnuto pogląd, że dwa lata po wejściu w życie, RODO z powodzeniem spełnia swoje zamierzenia, które polegają na wzmocnieniu ochrony prawa jednostki do ochrony danych osobowych i zagwarantowaniu swobodnego przepływu tych danych w Unii Europejskiej. Zauważono też jednak, że w niektórych obszarach można wprowadzić pewne ulepszenia. Prawdopodobne jest przy tym, że przy rozwiązaniu większości problemów, na które zwracają uwagę kraje członkowskie i zainteresowane strony, będzie możliwe nabycie nowego doświadczenia w stosowaniu przepisów Rozporządzenia w nadchodzących latach. W sprawozdaniu przedstawiono wyzwania, które ujawniły się do tej pory oraz sposoby ich zwalczania.

W Komunikacie uznano, że Rozporządzenie unijne powinno być potraktowane jako istotny element ukierunkowanego na człowieka podejścia do technologii i tym samym nadającego kierunek w jej wykorzystywaniu w transformacji ekologicznej i cyfrowej, które to charakteryzują kształtowanie polityki Unii Europejskiej. Zostało to podkreślone w lutym 2020 roku w Białej Księdze w sprawie sztucznej inteligencji[582] oraz w Komunikacie w sprawie europejskiej strategii w zakresie danych[583]. Wezwano do utworzenia wspólnej europejskiej przestrzeni danych, jednolitego rynku danych, jak również dziesięciu europejskich sektorowych przestrzeni danych istotnych z punktu widzenia transformacji ekologicznej i cyfrowej. Przestrzenie sektorowe swoim zakresem mają obejmować zdrowie, produkcję przemysłową, energię, mobilność, rolnictwo, dane finansowe, administrację publiczną oraz europejską chmurę dla otwartej nauki[584]. W ramach strategii ujawniono zamiar

[581] Komunikat Komisji do Parlamentu Europejskiego i Rady, *Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej-dwa lata stosowania ogólnego rozporządzenia o ochronie danych,* COM(2020)264 final,
[dostęp:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0264.

[582] White Paper on Artificial Intelligence: a European approach to excellence and trust, Brussels, COM(2020)65 final, [dostęp: 19.02.2020] https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en?etransnolive=1.

[583] Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, *A European strategy for data,* Brussels, COM(2020)66 final,
[dostęp: 19.02.2020] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[584] Europejska chmura dla otwartej nauki (EOSC) wspomaga stosowanie oraz zarządzanie danymi badawczymi w celu zapewnienia naukowcom dostępu do nauki opartej na danych, [dostęp: 25.10.2024] https://digital-strategy.ec.europa.eu/pl/policies/open-science-cloud.

zbadania przez Komisję Europejską w przyszłym prawodawstwie, w jaki sposób można umożliwić wykorzystanie danych przechowywanych w publicznych bazach danych do celów badań naukowych w sposób zgodny z Rozporządzeniem. Przestrzenie danych powinny być wspierane przez federację chmury obliczeniowej. Przepisy Rozporządzenia mają z kolei zagwarantować niezbędną elastyczność umożliwiającą uwzględnienie różnych podejść.

Za priorytet Komisji Europejskiej w zakresie „Europy na miarę ery cyfrowej" i „Europejskiego Zielonego Ładu"[585] można potraktować opracowanie nowych inicjatyw umożliwiających obywatelom odgrywanie aktywniejszej roli w transformacji cyfrowej oraz w wykorzystywaniu narzędzi cyfrowych w dążeniu do społeczeństwa neutralnego dla klimatu i do bardziej zrównoważonego rozwoju.

W gospodarce, która coraz bardziej opiera się na przetwarzaniu danych, Rozporządzenie jest ważnym narzędziem gwarantującym, iż osoby fizyczne sprawują większą kontrolę nad swoimi danymi, zaś dane te są przetwarzane legalnie, do celów zgodnych z prawem, w uczciwy i przejrzysty sposób. Jednocześnie RODO wspiera innowacje godne zaufania, w szczególności dzięki podejściu opartym na analizie ryzyka i mając na uwadze zasadę uwzględnienia ochrony prywatności już w fazie projektowania oraz zasadę domyślnej ochrony prywatności.

Konieczność zapewnienia zaufania i zapotrzebowania na ochronę danych osobowych nie jest ograniczona do terytorium Unii Europejskiej. Osoby fizyczne na całym świecie aprobują prywatność i bezpieczeństwo swoich danych. W wyniku przeprowadzonego badania globalnego wykazano, że czynniki te wpływają na decyzje dotyczące zachowania w Internecie. Jedno z badań dotyczyło prywatności konsumentów. Ankietę przeprowadzono wśród 2600 konsumentów na całym świecie. Duże grono ankietowanych podjęło już działania, mające na celu ochronę swojej prywatności, w ten sposób, że zmienili firmę lub dostawców ze względu na prowadzoną przez nich politykę w zakresie danych lub praktykę w zakresie ich wymiany. Widoczna jest tendencja przedsiębiorstw do dobrowolnego rozszerzania uprawnień i zabezpieczeń przewidzianych w Rozporządzeniu na klientów spoza Unii Europejskiej. Przedsiębiorcy traktują poszanowanie danych za element przewagi konkurencyjnej, oferując innowacyjne usługi za pomocą nowatorskich rozwiązań w zakresie prywatności lub bezpieczeństwa danych. Zwiększenie zdolności podmiotów sektora prywatnego i publicznego do gromadzenia i przetwarzania danych na dużą skalę nasuwa

[585] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów-Europejski Zielony Ład, Bruksela, COM(2019)640 final, [dostęp: 11.12.2019] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52019DC0640.

złożone pytania, które stawiają prywatność w centrum debaty publicznej w różnych częściach świata.

Zwierzchnictwo Unii Europejskiej w dziedzinie ochrony danych osobowych świadczy o tym, że może ona być uznana za organ regulujący gospodarkę cyfrową. Sekretarz generalny Organizacji Narodów Zjednoczonych António Guterres potwierdził, że Rozporządzenie daje „dobry przykład, który inspiruje do podejmowania podobnych działań w innych częściach świata", począwszy od Chile po Koreę Południową, od Brazylii po Japonię, od Kenii po Indie oraz od Kalifornii po Indonezję. Zaapelował ponadto do państw członkowskich Unii Europejskiej, aby dalej wspierały kształtowanie ery cyfrowej i odgrywały wiodącą rolę w zakresie innowacji technologicznych[586].

Komisja Europejska stwierdziła, że okres dwóch lat po wejściu w życie przepisów Rozporządzenia, jest zdecydowanie za krótki, aby dokonać pełnej oceny funkcjonowania mechanizmów współpracy i spójności. Organy ochrony danych zacieśniły jednak współpracę poprzez mechanizm kompleksowej obsługi i szerokie wykorzystanie wzajemnej pomocy. Mechanizm kompleksowej obsługi jako atut rynku wewnętrznego, jest wykorzystywany do rozstrzygania spraw transgranicznych[587] i polega na tym, że jeżeli jedno przedsiębiorstwo przetwarza dane poza granicami jednego państwa, to właściwym organem ochrony danych jest jedno z państw członkowskich, w którym znajduje się główna siedziba spółki.

Komisja Europejska monitoruje wdrażanie przepisów Rozporządzenia w krajowych regulacjach. Wszystkie państwa członkowskie, z wyjątkiem Słowenii, przyjęły nowe przepisy albo dostosowały własne krajowe regulacje prawne o ochronie danych. Wobec tego, nadal istnieje pewien stopień fragmentaryzacji, który wynika z zastosowania opcjonalnych klauzul precyzujących. Widoczne są różnice w odniesieniu do wieku wyrażania zgody przez dzieci w usługach społeczeństwa informacyjnego[588]. Ta fragmentacja stwarza wyzwania dla rozwiązań związanych z cyberbezpieczeństwem[589].

Szczególnym wyzwaniem w odniesieniu do przepisów krajowych jest uzgodnienie

---

[586] Przemówienie Sekretarza Generalnego ONZ w Senacie Włoch, [dostęp: 18.12.2019] https://press.un.org/en/2019/sgsm19916.doc.htm.

[587] Od dnia 25 maja 2018 roku do dnia 31 grudnia 2019 roku przedłożono 141 projektów decyzji, z czego 79 skutkowało wydaniem finalnych rozstrzygnięć.

[588] Według badania dotyczącego praw podstawowych, to ok. 70% ludności Unii Europejskiej w wieku powyżej 16 r.ż. słyszało o Rozporządzeniu unijnym. Zob. Your rights matter: Data protection and privacy-Fundamental Rights Survey, [dostęp: 18.06.2020] https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

[589] Projekt Komisji w sprawie narzędzi identyfikacji wieku-projekt pilotażowy w celu zademonstrowania interoperacyjnej infrastruktury technicznej w zakresie ochrony dzieci, w tym weryfikacji wieku i zgody rodziców. Oczekuje się, że pomoże to przy wdrażaniu mechanizmów ochrony dzieci w oparciu o istniejące przepisy UE dotyczące ochrony dzieci w Internecie.

prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji, jak też należyte wyważenie obu tych praw. W niektórych przepisach krajowych ustanowiono regułę pierwszeństwa wolności wypowiedzi, podczas gdy w innych państwach prawo do ochrony danych osobowych jest ważniejsze. Zatem Komisja Europejska będzie nadal czuwać nad poszanowaniem istoty praw podstawowych. Zgodnie z jej stanowiskiem, przepisy dotyczące ochrony danych, w żadnym wypadku nie powinny mieć wpływu na korzystanie z prawa do wolności wypowiedzi i informacji, np. poprzez wywieranie presji na dziennikarzach celem ujawnienia ich źródeł. Według Komisji wyważenie tych dwóch praw na mocy prawa krajowego, powinno znaleźć swoje odzwierciedlenie w orzecznictwie TSUE i ETPCz.

Rozporządzenie jest traktowane za elastyczne narzędzie gwarantujące, że rozwój nowych technologii będzie zgodny z prawami podstawowymi. Zauważono, że osoby fizyczne są coraz bardziej świadome swoich praw, m.in. prawa do żądania usunięcia ich danych osobowych. Ramy prawne związane z ochroną danych i prywatnością okazały się ważne z punktu widzenia wybuchu pandemii Covid-19, zwłaszcza w kontekście projektowania aplikacji do śledzenia kontaktów i innych rozwiązań technologicznych mających za cel zapobieganie skutkom stanu epidemii. Przyszłe wyzwania wiążą się z koniecznością wyjaśnienia sposobu stosowania sprawdzonych zasad w sztucznej inteligencji, czy w rozpoznawaniu twarzy[590].

Zamierzeniem wprowadzenia przepisów RODO było stworzenie jednolitego podejścia i wspólnej europejskiej kultury ochrony danych, a także wspieranie skuteczniejszego postępowania w sprawach transgranicznych. Komisja Europejska doszła jednak do wniosku, że czynienie ostatecznych refleksji na temat wykorzystywania przepisów RODO jest jednak przedwczesne. Biorąc pod uwagę ciągłą ocenę regulacji krajowych, stosunkowo krótki okres praktycznego stosowania Rozporządzenia oraz fakt, że w wielu krajach członkowskich prawodawstwo sektorowe jest nadal poddawane przeglądowi, wyciąganie końcowych konkluzji może okazać się chybione. Podejmując wtórne działania, można odwoływać się do stosownej judykatury sądów krajowych[591] i TSUE, która pomoże w stworzeniu wspólnej wykładni przepisów o ochronie danych. W wymiarze międzynarodowym, Komisja w dalszym ciągu będzie czuwać nad bezpiecznym przepływem danych. Ma się to przejawiać w rozbudowie i modernizacji narzędzi stosowanych do przekazywania danych. Prace

[590] Tak na przykład Biała Księga Komisji w sprawie sztucznej inteligencji otworzyła w 2020 roku debatę publiczną na temat konkretnych okoliczności, które mogłyby uzasadniać użycie sztucznej inteligencji do celów zdalnej identyfikacji biometrycznej w miejscach publicznych. Zob. White Paper on Artificial Intelligence: a European approach to excellence and trust...
[591] Np. Austrii, Hiszpanii, Niemiec.

obejmują także negocjacje, które doprowadzą do stworzenia odpowiednich zabezpieczeń.

Ostateczne wnioski Komisji Europejskiej sprowadzały się do tego, że państwa członkowskie powinny dążyć do zakończenia procesu dostosowywania własnych przepisów sektorowych do Rozporządzenia oraz rozważyć ograniczenie stosowania klauzul precyzujących, które mogłyby doprowadzać do fragmentaryzacji. Z kolei Komisja Europejska musi jednocześnie prowadzić dwustronną wymianę z krajami członkowskimi na temat zgodności przepisów krajowych z RODO. Zadeklarowała, że będzie wspierać wymianę poglądów i praktyk pomiędzy państwami członkowskimi na tematy, które nadal wymagają doprecyzowania na szczeblach krajowych (tj. chociażby wolność wypowiedzi), celem zredukowania fragmentacji jednolitego rynku. Wezwała do przyjmowania dalszych, łatwych do zrozumienia wytycznych, które dostarczą transparentnych odpowiedzi i pozwolą uniknąć niejednoznaczności[592], przy czym te wytyczne mogą być dalej rozjaśniane przez TSUE w kontekście różnych doświadczeń i zmian. Natomiast, zgodnie ze strategią danych, Komisja Europejska będzie badać praktyczne środki ułatwiające szerszy zakres korzystania z prawa do przenoszenia danych przez osoby fizyczne, które zagwarantują większą kontrolę nad tym, kto może uzyskać dostęp do maszynowo generowanych danych i je wykorzystywać.

Na podstawie tej oceny stosowania RODO od maja 2018 r. wymienione powyżej działania zostały uznane za konieczne do wspierania jego stosowania.

2.7. Podsumowanie

Zauważalna jest stale rosnąca skala naruszeń gromadzonych danych osobowych. W dniu 27 kwietnia 2016 r. Parlament Europejski przyjął RODO, kończąc tym samym prace trwające ponad cztery lata nad reformą prawa unijnego dotyczącego danych osobowych. Rozporządzenie weszło w życie w dniu 25 maja 2018 roku, a więc po dwuletnim okresie *vacatio legis.* Był to okres przygotowawczy, w którym państwa członkowskie Unii Europejskiej dostosowywały przetwarzane dane do nowych wymogów. Dotąd obowiązujące przepisy ochrony danych osobowych, tj. Dyrektywa 95/46/WE, jak też implementująca ją ustawa o ochronie danych osobowych z 1997 roku, zostały zastąpione Rozporządzeniem. O ile przed 25 maja 2018 r., to ustawa o ochronie danych osobowych z 1997 roku była głównym aktem normatywnym w zakresie ochrony danych osobowych, to aktualnie takim aktem jest unijne Rozporządzenie. Z kolei nowa ustawa o ochronie danych osobowych z 2018

[592] Np. w odniesieniu do przetwarzania danych dzieci i osób, których dane dotyczą, w tym do korzystania z prawa do usunięcia danych.

roku, która to uchyliła wcześniej obowiązującą, jedynie uzupełnia i dookreśla postanowienia RODO[593].

Ogólne Rozporządzenie o Ochronie Danych Osobowych ma zasięg ogólny, a więc wiąże w całości i jest bezpośrednio stosowane we wszystkich krajach członkowskich, bez potrzeby krajowej implementacji[594]. Regulacje prawne zawarte w Rozporządzeniu Ogólnym są stosowane bezpośrednio i mają pierwszeństwo w przypadku kolizji z przepisami ustaw (art. 91 ust. 3 Konstytucji RP). To oznacza, iż krajowy organ stosujący prawo, jak i wszyscy zobligowani do ochrony danych osobowych, mają obowiązek traktowania postanowień unijnego Rozporządzenia jako części krajowego porządku prawnego, a w razie kolizji z ustawą – obowiązek jego zastosowania z jednoczesnym pominięciem przepisów aktu prawa krajowego[595]. W odróżnieniu od sytuacji, która miała miejsce do dnia 25 maja 2018 roku, istnieje możliwość bezpośredniego odwoływania się do aktu prawa unijnego w zakresie zdefiniowanej w nim istoty ochrony danych osobowych, związanej bezpośrednio z ochroną fundamentalnych praw i wolności osób fizycznych, w tym prawa do prywatności, prowadzącej do poszanowania „prawa do bycia zapomnianym".

Jednolite stosowanie Rozporządzenia jest zapewnione poprzez publikowanie w Dzienniku Urzędowym Unii Europejskiej, co oznacza, że kraje członkowskie nie mają prawa do ogłoszenia go w swoich wewnętrznych promulgatorach[596]. Unijne Rozporządzenie daje jednak możliwość państwom członkowskim przyjmowania przepisów szczegółowych w konkretnych obszarach, które mają za zadanie doprecyzowywać zasady ochrony, mające swój początek w Rozporządzeniu[597].

Unijne Rozporządzenie nr 2016/679 zostało uchwalone ze względu na konieczność

---

[593] Szukając unormowań odnośnie do ochrony danych osobowych w pierwszej kolejności trzeba sięgnąć do tekstu unijnego Rozporządzenia, a dopiero później do polskiej ustawy o ochronie danych osobowych. RODO w znacznej mierze nie wprowadziło jakichś nadzwyczajnych regulacji w stosunku do ustawy z 1997 roku, dlatego raczej powinno się je określać mianem ewolucji, a nie rewolucji. Inaczej ma się kwestia z „prawem do bycia zapomnianym", gdzie art. 17 RODO wyraźnie się do niego odniósł. Zob. Ustawa o ochronie danych osobowych z 1997 r., [dostęp:] https://odo24.pl/rodo-uodo/ustawa-o-ochronie-danych-osobowych-z-1997-r/,.

[594] D. Dörre-Kolasa, *Wpływ rozporządzenia ogólnego na zakres ochrony danych osobowych przetwarzanych w związku z zatrudnieniem,* [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2017, s. 35.

[595] Uchwała SN z dnia 2 czerwca 2010 r., sygn. akt: III CZP 37/10, [dostęp:] https://www.saos.org.pl/judgments/92394.

[596] K. Walczak, *Prawo pracy i ubezpieczeń społecznych,* red. K.W. Baran, Warszawa 2017, s. 160-161.

[597] Z tego wynika, że państwa UE mogą zawrzeć wyłącznie regulacje, które w sposób bardziej wnikliwy będą zapewniały szerszą realizację praw i wolności ludzi. Rozwiązania przyjęte na gruncie krajowym pozostające *contra legem* w stosunku do RODO, będą przez stosowne instytucje unijne uważane za nieważne. Przepisy te muszą obejmować należyte środki gwarantujące osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, zwłaszcza pod względem przejrzystości przetwarzania i przekazywania danych osobowych.

wprowadzenia zmian wynikających z dynamicznie rozwijającej się technologii[598]. Wyodrębniło szereg nowości w obszarze ochrony danych osobowych oraz nałożyło liczne obowiązki na podmioty, które poddają dane osobowe procesowi przetwarzania.

Podstawowymi celami RODO są harmonizacja podstawowych praw osób fizycznych, gwarancja swobodnego przepływu danych osobowych w ramach UE oraz zwiększenie ochrony danych osobowych poprzez wzmocnienie praw podmiotów danych, ujednolicenie przepisów dotyczących ochrony danych osobowych na terenie Unii Europejskiej, usprawnienie wymiany informacji i procedur wewnątrz UE, uatrakcyjnienie rynku Unii Europejskiej wobec państw trzecich i wyznaczenie standardów bezpieczeństwa odpowiadających wciąż postępującej technologii[599].

Założeniem wskazanym w motywie 3 Rozporządzenia jest wzmocnienie i zharmonizowanie ochrony podstawowych wolności i praw osób fizycznych w związku z czynnościami przetwarzania oraz zapewnienia swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi. Ochrona ta nie zawęża się jedynie do stworzenia gwarancji służących zdefiniowaniu prawidłowości procesu przetwarzania i przepływu danych osobowych. Powinna być szerzej rozumiana, czyli jako ochrona danych i ich przetwarzania z uwzględnieniem całościowego poszanowania wolności i praw związanych z autonomią informacyjną jednostki. Warto nadmienić, że przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub ich zestawach w sposób zautomatyzowany lub niezautomatyzowany i obejmuje usuwanie lub niszczenie danych (art. 4 pkt 2 Rozporządzenia). Udostępnienie danych przez administratora zgodnie z przepisami prawa krajowego jest w związku z tym przetwarzaniem w rozumieniu regulacji RODO. Powinnością każdego administratora, inaczej zobowiązanego, jest respektowanie obowiązków, jakie związane są z procesem przetwarzania danych osobowych, ale też tych wszystkich przepisów prawa, które definiowane są przez ustawodawcę unijnego oraz krajowego. Dotyczy to nie tylko organów i podmiotów publicznych, lecz również każdego przedsiębiorcy, który musi zadeklarować, że każda z prowadzonych przez niego działalności, podlegająca reżimowi ochrony danych osobowych, spełniać będzie standardy wynikające z obowiązujących regulacji w tym obszarze. Jedną z takich podstawowych regulacji jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

[598] M. Jędrzejak, *RODO-rozporządzenie o ochronie danych: to trzeba wiedzieć,* [dostęp: 01.02.2018] https://business.trustedshops.pl/blog/rodo-co-trzeba-wiedziec/.
[599] A. Marek, *RODO w praktyce, lekcja 1,* [dostęp:] https://www.podatki.biz/media/File/RODO/RODO_w_praktyce_1.pdf.

i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE.

Podstawy prawne przetwarzania na podstawie przepisów RODO są zgodne z tymi, które wynikały z uregulowań Dyrektywy 95/46/WE. W motywie 2 Dyrektywy podkreślono, że systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi. Powinny zatem szanować podstawowe prawa i wolności osób fizycznych, a w szczególności prawo do prywatności. Znalazło to swoje odzwierciedlenie w motywie 4 Rozporządzenia, w którym wskazano, że przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości.

W Rozporządzeniu unijnym pokazano, że ochrona osób fizycznych związana z przetwarzaniem danych osobowych jest jednym z praw fundamentalnych. Każda osoba ma prawo do ochrony danych osobowych jej dotyczących[600]. Początkowe założenia wskazywały, iż jednym z projektowanych rozwiązań RODO zmierzającym do zwiększenia poziomu kontroli jednostki nad danymi jej dotyczącymi i wdrożenia instytucji, które zagwarantują ochronę danych osobowych, będzie „prawo do bycia zapomnianym".

„Prawo do bycia zapomnianym" jest dowodem na to, że wraz z rozwojem mechanizmów pozyskiwania, rozpowszechniania i wyszukiwania informacji niezbędne było wypracowanie takiego rozwiązania, które zapewniłoby jednostce owocne egzekwowanie prawa do wyeliminowania z obrotu publicznego danych informacji, stanowiących z różnych powodów nielegalną lub nieuzasadnioną ingerencję w sferę gwarantowanych jej praw. Prawo to ma na celu zapewnić osobie fizycznej, niezależnie od obywatelstwa, czy miejsca stałego zamieszkania, poszanowanie podstawowych praw i wolności, zwłaszcza prawa do prywatności. Informacja, która została raz umieszczona w Internecie może być dowolnie kopiowana i rozprzestrzeniana. Pojawiła się wątpliwość, czy w związku z tym osoba, której dane zostały zapisane w sieci, może domagać się, aby wyszukiwarka internetowa nie wyświetlała wyników wyszukiwania, które mogłyby przekierować do stron źródłowych, na których znajdują się te dane. Usunięcie danych ze strony źródłowej nie było wystarczające, biorąc pod uwagę cel, jaki przyświecał Dyrektywie[601].

Trybunał Sprawiedliwości UE przyznał podmiotom „prawo do bycia zapomnianym" w sieci. Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 13 maja 2014 roku

[600] Ochrona ta jest niezależna od posiadanego obywatelstwa czy miejsca zamieszkania, a także nie powinna naruszać podstawowych praw i wolności, zwłaszcza prawa do ochrony danych osobowych. Rozporządzenie ma na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości, jak również pomyślności ludzi. Zob. J. Żołyński, *RODO. Prawo do zapomnienia w sferze zatrudnienia,* Warszawa 2018, s. 164.

[601] B. Baran, K. Południak-Gierz, *Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki,* „Zeszyty Naukowe Towarzystwa Doktorantów UJ" 2017, nr 2, s. 146.

w sprawie zawisłej pod sygn. akt: C-131/12 stanął na stanowisku, że uprawnioną jest każda osoba, której dane są rzeczywiście przetwarzane z jednoczesnym zbadaniem, czy posiada ona prawo do tego, aby dotycząca ją informacja nie była powiązana z jej imieniem i nazwiskiem poprzez listę wyświetlającą wyniki wyszukiwania mającego za punkt wyjścia właśnie to imię i nazwisko. Więc tak ujęte „prawo do bycia zapomnianym" jest narzędziem egzekwowania prawa do prywatności. Należy natomiast mieć na uwadze fakt, że informacje pomimo tego, że mogą nadal być dostępne na źródłowej stronie internetowej, to nie są jednak uwidocznione w internetowych wyszukiwarkach, a ich znalezienie wymaga podjęcia nieco bardziej skomplikowanych i wymagających wysiłku działań.

W Dyrektywie 95/46/WE zabrakło skonkretyzowania czy żądanie o usunięcie danych może odnosić się do podmiotu ponoszącego odpowiedzialność za stronę źródłową, czy może także za narzędzie wyszukujące. W wyniku podjęcia decyzji o usunięciu danych, przestaje być wyświetlana owa informacja w wyszukiwarce, ale treść, do której odnosi się wyszukiwanie na docelowej stronie internetowej pozostaje niezmieniona. Wymóg usunięcia jest niezależny od statusu treści zamieszczonej na stronie źródłowej. Operator zaś wyszukiwarki nie ma uprawnień, które umożliwiać mu będą weryfikację, czy publikacja w sieci jest zgodna z przepisami prawa, a zatem legalna i uzasadniona dla celów Dyrektywy 95/46/WE.

Trybunał Sprawiedliwości Unii Europejskiej przyjął nadrzędność „prawa do bycia zapomnianym" i ochrony prywatności w stosunku do interesu, jaki posiadają użytkownicy wyszukiwarek internetowych w znalezieniu wiadomości w ramach wyszukiwania danych określonego podmiotu. TSUE w analizowanym wyroku, pomimo że nadał prymat prawu do prywatności, to zwrócił uwagę na potrzebę ochrony wypowiedzi przed usunięciem w wyjątkowych przypadkach – wobec osób, które odgrywają w życiu publicznym szczególną rolę, a więc jeżeli przeważa interes społeczny.

Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 13 maja 2014 r. potwierdził, że z przepisów Dyrektywy 95/46/WE wynikało prawo do żądania usunięcia danych w Internecie, jeszcze przed wejściem w życie przepisów Rozporządzenia o Ochronie Danych Osobowych. Stanowi to niejako wyraz swoistej rewolucji, albowiem zaprezentowane uprawnienie miało być wprowadzone dopiero w pierwotnej wersji projektu rozporządzenia jako przełomowa regulacja.

„Prawo do bycia zapomnianym" stanowiło jeden z podstawowych elementów reformy europejskich przepisów ochrony danych osobowych. W art. 32 ust. 1 pkt 6 ustawy o ochronie danych osobowych z 1997 roku określono, że osoba, której dane dotyczą posiada uprawnienie

do żądania usunięcia danych, jeżeli są one niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne dla realizacji celu, dla jakiego zostały pozyskane. Ogólne Rozporządzenie o Ochronie Danych Osobowych ogranicza się jedynie do usunięcia danych, gdy te nie są już niezbędne do celów, w których zostały zebrane. W praktyce dokonanie oceny czy dane osobowe są przetwarzane zgodnie z celami, dla których były pozyskiwane, podobnie jak sprawdzenie, czy dane nie są już niezbędne do realizacji celów przetwarzania, może nie być prostym zadaniem. Podmiotowi, którego dane dotyczą może wydawać się, że cele zostały już zrealizowane i dane są niepotrzebne, natomiast administrator danych osobowych może ocenić tę sytuację zgoła odmiennie[602].

Cała koncepcja „prawa do bycia zapomnianym" wyznacza pewien nowy standard instrumentu ochrony danych osobowych. Wzrosła skuteczność prawa podstawowego, a zarazem powszechnego do ochrony danych osobowych oraz spowodowała umożliwienie osobom fizycznym nadzoru nad swoimi danymi. Reforma poprawiła wymiar ochrony danych osobowych powiązany z rynkiem wewnętrznym poprzez „ograniczenie rozdrobnienia, wzmocnienie spójności i uproszczenie otoczenia regulacyjnego, a tym samym zlikwidowanie niepotrzebnych kosztów i ograniczenie ciężaru administracyjnego"[603]. Założenia te silnie determinują uwzględnienie „prawa do bycia zapomnianym", a ich pełne zrealizowanie jest odpowiedzią na potrzebę stworzenia kompleksowego i pełnowartościowego systemu ochrony danych osobowych we wszystkich sferach funkcjonowania[604].

---

[602] Jednym z przykładów jest funkcjonowanie Krajowego Systemu Informacyjnego Policji. W praktyce obserwuje się, że organy Policji przechowują i przetwarzają dane osobowe w KSIP, nawet w sytuacji, gdy nastąpiło zatarcie skazania z mocy prawa. Z chwilą zatarcia skazania, za niebyłe uważa się nie tylko skazanie, ale samo popełnienie czynu zabronionego. Wobec tego, dalsze przetwarzanie danych osobowych wypacza celowość tej instytucji. Zob. P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 1022.

[603] Wniosek z 25 stycznia 2012 r. dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (Ogólne Rozporządzenie o Ochronie Danych Osobowych), COM(2012)11 final, [dostęp:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52012PC0011.

[604] J. Żak, *Koncepcja „prawa do bycia zapomnianym"…,* s. 155.

Rozdział 3. „Prawo do bycia zapomnianym" emanacją ochrony danych osobowych

3.1. Uwagi wstępne

„Prawo do bycia zapomnianym" kształtowało się w warunkach rewolucyjnych zmian technologicznych, a rezultatem jego urealniania stały się pierwsze propozycje nowelizacji na gruncie szeroko pojmowanej sfery ochrony danych osobowych w sieci internetowej[605].

Sztuczna inteligencja, pomimo tego, że stanowi wielką szansę dla ludzkości, stwarza też istotne dla niej wyzwania. Można zaobserwować skłonność do zbierania, gromadzenia i przesyłania pozyskanych informacji w postaci elektronicznej[606]. Ewolucja środowiska internetowego, wzrost szybkości przepływu informacji, ilość danych podlegających procesowi przetwarzania powodują, iż likwidacja lub modyfikacja tej informacji, która znalazła się w Internecie jest znacznie utrudniona. Internet staje się miejscem uznawanym za bezpowrotnie pochłaniające wszelkie umieszczone w nim dane[607].

Z tego też powodu, w cywilizowanym porządku prawnym, nie ma ochrony, która nie zapewniałaby prywatności człowieka[608]. Poufność jest jednym z elementów godności, podstawowym prawem do rozporządzania osobistymi informacjami. Udostępnienie danych wymaga zgody dysponenta bądź wyraźnego wskazania poprzez regulacje prawne[609]. Z tego wywodzi się „prawo do bycia zapomnianym", które nie jest szeroko analizowane na gruncie prawa polskiego[610]. Zgodnie z prawem Unii Europejskiej, dane osobowe mogą być zbierane tylko przy zachowaniu ściśle określonych przesłanek. Normatywizacja regulacji odnoszących

---

[605] J. van Hoboken, *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember. Freedom of Expression Safeguards in a Converging Information Environment,* opinia przygotowana dla Komisji Europejskiej, [dostęp: 01.05.2013]
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC86747/lbna26410enn.pdf.

[606] Zjawisko to określa się terminem *big data.* Odnosi się ono do wielkich i różnorodnych zbiorów danych, gdzie proces analizy i przetwarzania jest dość skomplikowany, niemniej jednak prowadzi do zdobycia nowej wiedzy. Pośród tych informacji znaczną część stanowią dane osobowe, które w powiązaniu z obowiązującymi regulacjami prawnymi powinny być poddawane szczególnej ochronie.

[607] Wbrew pozorom, można się spotkać także ze stanowiskami odmiennymi od zaprezentowanego, zdania są podzielone. Niektórzy przedstawiciele nauki występują w roli obrońcy w zakresie rozpowszechniania danych. Zob. I. Szekely, *The Right to Forget, The Right to be forgotten,* [w:] *European Data Protection: In Good Health?,* red. S. Gutwirth, R. Leenes, P. De Hert, Y. Poullet, Dordrecht 2012, s. 347.

[608] M. Gutowski, P. Kardas, M. Pietrzak, *Inwigilacja w obywateli, czyli wchodzimy w rok 1984,* [dostęp: 04.01.2016] https://prawo.gazetaprawna.pl/artykuly/915811,inwigilacja-w-obywateli-czyli-wchodzimy-w-rok-1984.html.

[609] Zauważalne jest to aktualnie w związku ze zjawiskiem „danych w chmurach", tzw. *cloud computing.* Chmura obliczeniowa wykorzystuje gotowe aplikacje on-line, które zawierają ogromne ilości prywatnych informacji. Umożliwiają dostęp do pozyskanych danych z dowolnego komputera, bez potrzeby instalowania specjalnego oprogramowania.

[610] R. Fellner, *The Right to be Forgotten in the European Human Rights Regime,* Műnchen 2014, s. 31; M. Krzysztofek, *"Prawo do bycia zapomnianym" i inne aspekty prawa prywatności w epoce Internetu w prawie Unii Europejskiej,* „Europejski Przegląd Sądowy" 2012, nr 8, s. 29-34.

się do przetwarzania danych osobowych nie byłaby dostatecznie wystarczająca do realizacji celów, gdyby nie mechanizm zezwalający na usunięcie danych osobowych, które zostały umieszczone w Internecie wbrew woli osoby, a ich przetwarzanie było zakazane na podstawie norm szczególnych[611]. Potencjał administratorów informacji wzrósł wraz z rozwojem ilości udostępnień, a potrzeba stworzenia kompleksowych ram prawnych, które stanowiłyby barierę ochronną dla społeczności, z jednoczesnym brakiem ingerencji w fundamentalne prawa i wolności jednostki, stała się dla prawodawców nie lada wyzwaniem[612].

W literaturze przedmiotu podkreśla się, że „prawo do bycia zapomnianym" jest rozwinięciem istniejących rozwiązań w prawodawstwie państw europejskich, które nawiązują do prawa do zapomnienia czy prawa do usunięcia danych[613]. Pojęcia te niejednokrotnie stosowane są zamiennie, pomimo że nie są tożsamymi wyrazami. Historycznie zaliczają się do różnych konstrukcji prawnych, niemniej jednak każda z nich zakłada prawo każdej osoby do usunięcia informacji jej dotyczących po upływie określonego czasu. W odniesieniu do przedmiotowej problematyki wydaje się, że trafniejsza jest druga ze wspomnianych koncepcji. To twierdzenie znajduje swoje uzasadnienie w tym, że w piśmiennictwie coraz częściej można odnaleźć zamienne stosowanie nazewnictwa wobec „prawa do bycia zapomnianym", a mianowicie *„right to be forgotten"* lub *right to erasure*[614]*,* aczkolwiek genezy tego prawa można doszukiwać się w obu koncepcjach.

Prawo do zapomnienia jest znane ustawodawstwu francuskiemu, włoskiemu i hiszpańskiemu. Stosowane było w celu ochrony byłych osadzonych, po odbyciu zasądzonej kary. Prawo do zapomnienia sprowadzało się do usunięcia danych dotyczących skazanego, popełnionego przez niego czynu zabronionego, czy przebiegu procesu sądowego. Znajdowało uzasadnienie w idei poszanowania życia prywatnego jednostki, której celem jest zapobieganie naruszeniom godności człowieka.

Prawo do usunięcia danych różni się od prawa do zapomnienia przyznaniem zainteresowanemu podmiotowi roszczenia prawnego o usunięcie informacji, przetwarzanych

---

[611] B. Baran, K. Południak-Gierz, *Perspektywa regulacji…,* s. 140.

[612] Warto w tym miejscu nadmienić, że niebezpieczeństwo związane z wykorzystaniem nowych technologii zauważono już w latach 90. Komitet Ekspertów Ochrony Danych, stacjonujący przy Radzie Europy, zaprojektował znaczące dla rozwoju instytucji „prawa do bycia zapomnianym" opracowania, tj. *New Technologies: a challenge to privacy protection?* z 1989 r., a w roku następnym *Data protection and media,* [dostęp:22.07.2014]
http://www.coe.int/t/dghl/standardsetting/dataprotection/reports_and_studies_en.asp?toPrint=yes&;
Zob. G. Orwell, *Rok 1984,* Warszawa 2013, s. 48.

[613] L. Szot, *"Prawo do bycia zapomnianym w sieci",* [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne,* red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017, s. 188.

[614] S. Gupta, *The right to be forgotten,* [dostęp: 29.06.2014] https://www.lexology.com/library/detail.aspx?g=58540b9b-b571-48ed-9aab-4b70c34fb196.

przez osoby trzecie, których jest podmiotem. Celem takiego rozwiązania jest uzyskanie balansu pomiędzy podmiotami przetwarzanych danych a osobami je przetwarzającymi. Można spotkać się też ze stwierdzeniem, że prawo do zapomnienia ewoluowało i z biegiem czasu przekształciło się w prawo do usunięcia danych.

Prace nad „prawem do bycia zapomnianym" inspirowane były myślą, zgodnie z którą w sieci internetowej, w przeciwieństwie do świata rzeczywistego, nie występuje po upływie oznaczonego czasu instytucja zatarcia skazania. Zatarcie skazania zapobiega wykluczeniu społecznemu. Uważa się też, że upływ czasu powoduje, iż w pamięci człowieka zaciera się ślad o popełnionym przestępstwie[615]. Podkreśla się także, że pomimo proponowanego kształtu ujętego jako „prawo do bycia zapomnianym", instrument ten stanowi raczej wartość etyczną lub społeczną.

Artykuł 17 Rozporządzenia nr 2016/679 wprowadza „prawo do bycia zapomnianym", na które składają się:

- kryteria wyznaczenia przypadków, gdy osoba, której dane dotyczą może żądać usunięcia danych;
- obowiązki administratora danych;
- wyłączenia stosowania „prawa do bycia zapomnianym";
- oraz sposób egzekwowania tego prawa.

Zważywszy na złożoność problemów prawnych wynikających z regulacji „prawa do bycia zapomnianym", rozważania w Rozdziale trzecim będą skupiały się na udzieleniu odpowiedzi na następujące pytania:

- komu przysługuje „prawo do bycia zapomnianym"?
- kto jest adresatem obowiązku z art. 17 Rozporządzenia nr 2016/679?
- na czym polega obowiązek przewidziany w regulacji „prawa do bycia zapomnianym"?
- kiedy „prawo do bycia zapomnianym" nie znajdzie zastosowania?

Zgodnie z art. 17 ust. 1 RODO, osoba, której dane dotyczą, ma prawo żądać od administratora danych niezwłocznego usunięcia dotyczących jej informacji, przy jednoczesnym zaistnieniu odpowiednich ku temu przesłanek.

„Prawo do bycia zapomnianym" przysługuje każdemu, bez wyjątku. Natomiast na

[615] M. Błaszczyk, *Instytucja zatarcia skazania w polskim prawie karnym,* „Studia Iuridica" 2006, t. XLVI, s. 1.

podstawie samej treści przepisów, bezpośrednim adresatem są tylko administratorzy tych danych, a zatem podmioty decydujące o celach i środkach przetwarzania. Pomimo dość jasnego brzmienia tej regulacji, pojawia się szereg wątpliwości.

Obowiązek realizacji „prawa do bycia zapomnianym" nakłada się zarówno na administratorów, ale i na podmioty przetwarzające dane mające siedzibę na terytorium Unii Europejskiej, jak też na te nieposiadające jednostek organizacyjnych w UE, jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług osobom przebywającym w UE lub z monitorowaniem ich zachowania, o ile ma to miejsce na terenie Unii Europejskiej[616].

Administrator bez zbędnej zwłoki, a w każdym razie, jak wynika z treści art. 12 ust. 3 Rozporządzenia, w ciągu jednego miesiąca od otrzymania żądania, informuje podmiot danych o czynnościach podjętych w związku ze zgłoszonym wnioskiem. W przypadku złożoności żądania lub gdy ich liczba jest znaczna, termin ten może zostać przedłużony o kolejne dwa miesiące.

W celu wzmocnienia „prawa do bycia zapomnianym" w Internecie, europejski prawodawca w art. 17 ust. 2 RODO uznał, iż prawo do usunięcia danych osobowych powinno zostać rozszerzone w taki sposób, aby administrator danych osobowych był zobowiązany do podjęcia wszelkich niezbędnych kroków prowadzących do zaprzestania przetwarzania danych osobowych, w tym do poinformowania pozostałych przetwarzających oraz administratorów o wpłynięciu żądania, tak aby zdawali sobie sprawę z konieczności usunięcia wszelkich odnośników i łączy do istniejących danych osobowych. Zakres jego działań został ograniczony do słowa „rozsądne", co oznacza, że w sytuacji wykazania nadmiernych niedogodności, w tym ekonomicznych, istnieje możliwość uchylenia się od odpowiedzialności. Co prawda, może się to wydawać ograniczające dla praw jednostki, lecz trzeba mieć na uwadze, że osoba zainteresowana może wówczas wystąpić z odpowiednim wnioskiem bezpośrednio do podmiotów przetwarzających jej dane osobowe. W sytuacji publikowania danych osobowych przez osoby trzecie, administratora danych należy uznać za odpowiedzialnego za publikację tych informacji, jeśli wyraził on zgodę na publikację tychże danych przez osobę trzecią.

W kontekście powyższych wywodów, pojawiają się stanowiska różnicujące przepis art. 17 Rozporządzenia na prawo do żądania usunięcia danych z ust. 1 oraz „prawo do bycia zapomnianym" z ust. 2[617]. Rozróżnianie uprawnień w ten sposób zdaje się być niecelowe.

---

[616] Art. 3 ust. 2 Rozporządzenia nr 2016/679.

[617] A.A. Sławiński, *„Prawo do bycia zapomnianym" w świetle ogólnego rozporządzenia o ochronie danych osobowych i orzecznictwa TSUE,* [w:] *Prawo do prywatności-współczesne wyzwania,* Warszawa 2019, s. 91.

Raczej należy opowiedzieć się za rozumieniem regulacji w następujący sposób: na wniosek podmiotu danych, przy jednoczesnym braku sposobności powołania się na wyłączenia od obowiązku usunięcia danych, administrator jest zobowiązany zarówno do usunięcia informacji, jak i do podjęcia wszelkich działań mających na celu zaprzestanie przetwarzania tych danych przez pozostałe podmioty.

„Prawo do bycia zapomnianym" nie jest prawem absolutnym, co oznacza, że powinno ustępować w określonych przypadkach prawom podstawowym[618]. Prawodawca unijny wymienił taksatywny katalog przesłanek wyłączających to prawo. Najbardziej kontrowersyjnym i budzącym najpoważniejsze wątpliwości praktyczne jest wyłączenie z art. 17 ust. 3 lit. a) RODO odnoszące się do korzystania z prawa do wolności wypowiedzi i informacji. Przy rozpatrywaniu żądania usunięcia danych należy je wyważyć z prawem do prywatności poprzez dążenie do osiągnięcia równowagi pomiędzy interesami użytkowników Internetu a fundamentalnymi prawami człowieka[619]. Balans ten może zależeć od rodzaju danych osobowych, będących przedmiotem wniosku oraz od tego, czy są to dane wrażliwe, a także, czy istnieje interes publiczny w posiadaniu tych informacji. „Prawo do bycia zapomnianym" może też zostać ograniczone w prawie unijnym lub krajowym na podstawie art. 23 RODO.

W Rozdziale trzecim zostały zaprezentowane podstawowe elementy treści rozwiązań, pozwalające na zrozumienie charakteru i znaczenia „prawa do bycia zapomnianym". Konieczne jest nie tylko przedstawienie sfery prywatności jednostki i jej danych osobowych, ale i modelu definiującego przesłanki realizacji „prawa do bycia zapomnianym" oraz jego wyłączeń.

3.2. Zdefiniowanie „prawa do bycia zapomnianym"

3.2.1. Problem z definicją „prawa do bycia zapomnianym"

Przy próbach tworzenia definicji „prawa do bycia zapomnianym" ważna jest jego ocena ze względu na skuteczność rozwiązań w nim zawartych, a więc aksjologicznej spójności prawa. System praworządności powinien być oparty na takich normach prawnych, które umożliwią realizację prawnie akceptowanych rozwiązań w sposób nienaruszający

[618] Factsheet on the „Right to be Forgotten" ruling (C-131/12), [dostęp: 29.06.2014] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2014/06/factsheet_data_protection_en.pdf.
[619] D. Klimas, *Prawo do zapomnienia-postulaty de lege lata i de lege ferenda,* „Prawo Mediów Elektronicznych" 2014, nr 2, s. 8.

godności człowieka. Z drugiej strony, regulacje prawne odnoszące się do komentowanego prawa winny utrudniać nadinterpretację prawa. Istotną maksymą jest staranność i jakość prawa[620]. W tym miejscu warto zauważyć, że niektóre idee prawne są przeciwieństwem rzeczywistości społeczno-politycznej, zatem niejednokrotnie wymagają zmian. Usprawnieniu sprzyja teoria równowagi ogólnej, która wskazuje, jak radzić sobie z niepewnością prawa. Inaczej bowiem prawo może przestać obejmować wartości ochroną, dla jakich zostało ustanowione[621]. Regulacje prawne nie powinny być wyimaginowanym instrumentem, lecz odzwierciedleniem realnych potrzeb społecznych, aby nie doprowadzać do instrumentalizacji prawa. Na pierwszym miejscu stawia się człowieka i emanację człowieczeństwa w postaci godności, co wiąże się z komfortem życia w swojej strefie intymności. Państwo w imperatywny sposób winno wkraczać w te kwestie, które wymagają zaangażowania aparatu państwowego, tak aby kreować normy prawne sprzyjające ludziom[622].

Do dnia 25 maja 2018 r. terminologia „prawa do bycia zapomnianym" nie była bliska pozytywnemu prawu polskiemu. Uprzednio, instytucja ta wypracowana została na gruncie teoretycznym, nie mając charakteru normatywnego. W dużej mierze była to raczej koncepcja z szeroko pojętej sfery praw człowieka[623]. Z uwagi na to, próbę wyjaśnienia powyższego uprawnienia podjęto się na tle rozwiązań doktrynalnych i normatywnych obowiązujących w innych systemach prawnych, przy czym nie należało to do łatwych zadań. Trudność polega na tym, że termin „zapomnienie" jest pochodną pojęcia prywatności, a więc należy do kategorii bardzo dynamicznych. Pojawia się jedynie wątpliwość, czy wszystkie sfery prywatności podlegają tej samej ocenie oraz z jakimi narzędziami dotyczącymi ukazania prywatności związane jest „zapomnienie". Nawiązując do rozwiązań innych krajów, można zauważyć, że „prawo do bycia zapomnianym" jest rozwinięciem historycznie istniejącego w prawodawstwie państw Zachodu „prawa do usunięcia danych", czy „prawa do niepamięci". Warto wspomnieć, iż do „prawa do bycia zapomnianym" podobna, ale nie tożsama jest instytucja określana mianem „prawa do usunięcia" danych osobowych. Te dwa prawa różnią się od siebie przyznaniem zainteresowanemu podmiotowi określonego roszczenia

[620] Oznacza to bardziej koncentrowanie się na sytuacjach częstych i powtarzających się, *a contrario* nie oznacza skupienia uwagi na sytuacjach jednostkowych. Zasięg adresatów normy prawnej powinien być z reguły nieograniczony *erga omnes.*

[621] J. Żołyński, *RODO. Prawo do zapomnienia…,* s. 53.

[622] Podmioty będące uprawnionymi do tworzenia prawa w przedmiocie ochrony prywatności powinny kierować się dwiema naczelnymi zasadami, tj. prawa są stanowione nie ze względu na konkretne osoby, lecz dla wszystkich oraz wszelkie prawo powinno być stanowione ze względu na człowieka, a dobro jednostki powinno być ostatecznym celem prawa samym w sobie.

[623] Od dnia 25 maja 2018 r. „prawo do bycia zapomnianym" obowiązuje w polskim porządku prawnym, ale nie z powodu bezpośredniego przyjęcia polskich rozwiązań prawodawczych, tylko w wyniku narzucenia przepisów obowiązujących w Unii Europejskiej.

prawnego[624].

W procesie tworzenia, a później stosowania prawa, co odnosi się również do „prawa do bycia zapomnianym" istotnym elementem jest interpretacja prawa. Zauważalne są postulaty dokonywania odwróconej wykładni. Zamiast przyjętej dotąd wykładni językowej, częściej spotyka się wykładnię celowościową[625]. W związku z tym, przepisy prawne w zakresie „prawa do bycia zapomnianym" powinny być tak normowane, ażeby w wykładni tych regulacji było jak najmniej semiotyki[626], a wykładnia ujawniała cel przepisów i ich znaczenie. Niedosyt takich reguł w większości będzie stwarzać problem z ustaleniem sprawiedliwości w realnym wymiarze. Tak też, o ile w wymiarze formalnym wszystko pozostanie w zgodności, o tyle w wymiarze materialnym będzie to stało w sprzeczności z poczuciem sprawiedliwości indywidualnej i powszechnej[627]. Prawo musi przynosić rezultaty, bowiem tego oczekuje ogół społeczności. Wykładnia prawa z kolei powinna być pragmatyczna. Niemałe znaczenie mają okoliczności związane z danym stanem faktycznym, które w sferze prywatności kojarzone są z przejawem ochrony godności człowieka.

Interpretacji „prawa do bycia zapomnianym" dokonuje się poprzez pryzmat istniejących kultur prawnych, w których się rozwijała[628]. S.C. Bennett podaje długą historię roszczeń związanych z naruszeniem prywatności w następstwie wykorzystania niezaktualizowanych informacji[629]. Tak też, Sąd Najwyższy Stanów Zjednoczonych wskazywał na potrzebę ochrony wolności prasy w związku z wiadomościami posiadającymi przymiot autentyczności. Rozwiązanie takie nie wpływało jednak całkowicie na rozstrzygnięcia wydawane w sprawach, które nie odnosiły się do prasy i wolności słowa.

---

[624] Podmiot posiada interes w przedmiocie usunięcia danych osobowych przetwarzanych przez osoby trzecie. Znajduje to swoje oparcie w idei, w świetle której każdemu przysługuje prawo złożenia takiego żądania, choć pod pewnymi warunkami. Takie rozwiązanie ma na celu uzyskanie stanu równowagi między podmiotem przetwarzającym dane a podmiotem, którego dane ulegają temu procesowi. Według niektórych poglądów „prawo do bycia zapomnianym" w późniejszym czasie przekształciło się w „prawo do usunięcia".

[625] J. Żołyński, *Glosa do wyroku SN z dnia 4 września 2013 r., sygn. akt: II PK 358/12,* „Praca i Zabezpieczenie Społeczne" 2014, nr 3, s. 38-41.

[626] Pod pojęciem semiotyki kryją się badania znaczenia języka, analiza znaczeń wyrazów, relacja formy znaku do treści oznaczonej.

[627] Wyróżnia się szereg zasad, które będą pomocne w formułowaniu sprawiedliwości realnej, m.in. regulacje prawne powinny być zredagowane w ogólny sposób (brak luzu interpretacyjnego może doprowadzić do wypaczenia funkcji konkretnego aktu normatywnego), normy *ius cogens* powinny być stosowane jedynie w wyjątkowych sytuacjach, regulacje prawne winny być nacechowane spójnością logiczną i kompleksowością, interpretacja prawa (a nie faktu) powinna być dokonywana zgodnie z zasadą *in dubio pro reo*, normy prawne nie mogą stać w sprzeczności ze zdrowym rozsądkiem, ponieważ tylko to jest przejawem sprawiedliwości obiektywnej.

[628] Nie jest czymś nowym, że sfera prywatności inaczej była postrzegana w Stanach Zjednoczonych, a inaczej w krajach na kontynencie europejskim. Niektórzy autorzy stoją na stanowisku, że idea „prawa do bycia zapomnianym" nie mogłaby w USA w ogóle funkcjonować. Zob. E. Shoor, *Narrowing the right to be forgotten…,* s. 489-493.

[629] S.C. Bennet, *Right to be forgotten,* "Berkeley Journal of International Law" 2012, nr 30, s. 168.

Godnym podkreślenia jest fakt, iż sądy amerykańskie, w przeciwieństwie do sądów europejskich, nie przykładają uwagi do osiągnięcia równowagi w czynieniu fundamentalnych praw realnymi, traktując przy tym wolność słowa jako nadrzędną wartość w odniesieniu do prywatności. Odmienne postrzeganie tego zjawiska odgrywa niemałą rolę w kształtowaniu kierunku rozwoju koncepcji praw podmiotów danych, które tworzą się na bazie powstałej dotąd judykatury w kwestii ochrony prywatności i danych osobowych w sieci. Przytoczone sformułowanie określa, wobec tego prawo przysługujące jednostce, z którą dane są nierozerwalnie złączone, tj. wiek, imię, nazwisko. Trudność implementowania „prawa do bycia zapomnianym" w amerykańskim porządku prawnym wyraża się w szerokim zakresie wolności słowa, podlegającej jedynie minimalnym ograniczeniom[630]. Prawodawcy na całym świecie zdają sobie sprawę, że ujednolicenie i harmonizacja międzynarodowego prawa ochrony danych osobowych może prowadzić do utrzymania kondycji globalnej ekonomii, dającej swój wyraz w Internecie. Przez ustawodawców podejmowane są próby urealniania ideologii związanej z instytucją „prawa do bycia zapomnianym", napotykając przy tym trudności skoordynowania przetwarzania danych osobowych w skali światowej.

„Prawo do bycia zapomnianym" jest różnie interpretowane. M.L. Ambrose i J. Ausloos wskazują na dwie wersje tej koncepcji. Pierwsza z nich stanowi rozwinięcie francuskiego prawa do niepamięci. Było ono historycznie używane w powiązaniu ze skazanymi za przestępstwa, które popełnili. Po odbyciu kary pozbawienia wolności dążono wówczas do zapobieżenia przekazania przedmiotowej informacji osobom trzecim. To właśnie traktuje się często jako formę poprzedzającą „prawo do bycia zapomnianym" w ówczesnym rozumieniu. Drugą wersję utożsamiono z „prawem do wymazania" rozpowszechnionej przez dane podmioty informacji. Jednak takie dwuaspektowe postrzeganie „prawa do bycia zapomnianym" nie jest racjonalnym rozwiązaniem. W nauce prawa, zauważa się przejście z prawa do niepamięci[631] do prawa do żądania usunięcia danych i to ten rodzaj relacji występujący pomiędzy tymi prawami wydaje się mieć wpływ na sposób pojmowania zakresu „prawa do bycia zapomnianym"[632]. „Prawo do bycia zapomnianym" w doktrynie francuskiej było kojarzone z zasadą ograniczania ilości gromadzonych danych. Powiązane było w dużej mierze ze społeczeństwem cyfrowym i widoczne w praktyce orzeczniczej sądów. Tak też, we Francji, z inicjatywy sekretarza stanu ds. rozwoju i planowania gospodarki cyfrowej, powstał

[630] Termin „słowo" odnosi się także do otrzymywanych wyników z wyszukiwarek internetowych. Zob. A.H. Stuart, *Google search results: buried if not forgotten,* "North Carolina Journal of Law & Technology" 2014, z. 15, s. 466.
[631] Prawo do niepamięci w dużej mierze związane było z Francją, ale stanowiło także część hiszpańskiego i włoskiego porządku prawnego.
[632] M.L. Ambrose, J. Ausloos, *The right to be forgotten across the pond…,* s. 12.

Kodeks Dobrych Praktyk Prawa do Bycia Zapomnianym w Sieciach Społecznościowych i Wyszukiwarkach Internetowych, który jest wyrazem emanacji realizowania praw człowieka odnoszących się do ochrony danych osobowych, a jednocześnie wpływa na postępowanie podmiotów w Internecie[633]. Wraz z upływem czasu, kiedy korzystanie z Internetu stawało się coraz modniejsze, orzekanie w przedmiocie ochrony danych osobowych było popularne nie tylko na kontynencie europejskim. Jedno z ważniejszych rozstrzygnięć dla rozwoju instytucji „prawa do bycia zapomnianym" wydano w sprawie Virginii Da Cunha. Argentyńska zarazem tancerka, piosenkarka, aktorka i modelka publikowała fotografie ze swoim wizerunkiem na profilu społecznościowym Facebook i Twitter. W wytoczonym przeciwko Google i Yahoo powództwie podniosła, że jej dane, tj. imię, nazwisko oraz zdjęcia pojawiają się w wyszukiwarkach internetowych jako rezultat wyszukiwania stron internetowych nawiązujących do treści pornograficznych, a umieszczenie jej danych w tym kontekście odbyło się bez uprzedniego wyrażenia przez nią zgody, wobec czego poniosła liczne straty materialne oraz moralne. Wydając w tej sprawie wyrok, zwrócono uwagę na fakt, że istnieje konflikt pomiędzy wolnością słowa a prawem jednostki do kontrolowania wykorzystania jej danych. Sąd I instancji przychylił się do stanowiska zaprezentowanego przez Virginię Da Cunha, czego nie podzielił sąd II instancji. Jednakże zarówno Yahoo, jak i Google zablokowały wyniki wyszukiwań w spornym zakresie[634].

Abstrahując od rozróżnienia tych dwóch terminów, zauważalne jest, że „zapomnienie" jest pewnym zbiorem, co tym samym prowadzi do uzasadnionego wniosku, że „prawo do bycia zapomnianym" może być definiowane zarówno w szerszym, jak i węższym znaczeniu. *Sensu largo,* oznacza szczególne uprawnienie jednostki do objęcia ochroną nienaruszalności własnej osobowości przed zagrożeniem dotknięcia jej cierpieniem psychicznym lub fizycznym, tak w wymiarze wewnętrznym określanym przez pryzmat ochrony godności, jak i w wymiarze zewnętrznym przejawiającym się w interesie publicznym. Dokonywane jest ono za pośrednictwem sprawowania ciągłej kontroli w stosunku do osób trzecich w zakresie umieszczania przez nich swoich danych w związku z prywatnością, zaś w przypadku umieszczania tychże danych bez ich zgody lub w sytuacji jej cofnięcia, sformułowania żądania niezwłocznego i nieodpłatnego skasowania danych osobowych pozostałych na wszystkich nośnikach, w tym nie tylko cyfrowych. *Sensu stricte* z kolei*,* oznacza również szczególne uprawnienie jednostki do ochrony nienaruszalności własnej osobowości, ale przez

[633] Kodeks ten odegrał znaczącą rolę w urealnieniu „prawa do bycia zapomnianym", [dostęp: 22.07.2014] www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_du_Droit.pdf.
[634] E. Carter, *Argentina's right to be forgotten,* "Emory International Law Review" 2012, z. 27, s. 28.

pryzmat sprawowania nieustannego nadzoru nad umieszczanymi danymi odnośnie jej prywatności, wyłącznie na nośnikach o charakterze cyberinformatycznym. Natomiast w sytuacji ich umieszczania bez uprzedniego wyrażenia przez jednostkę zgody lub jej cofnięcia, przysługuje żądanie ich usunięcia, jak powyżej[635]. Zatem „prawo do zapomnienia" jest elementem szeroko pojętej ochrony prywatności człowieka oraz wyrazem zasady ograniczonego gromadzenia, a następnie poddawania procesowi przetwarzania danych o konkretnej osobie fizycznej. Tak też w ujęciu aksjologicznym i filozoficznym jest wyrazem godności oraz wolności człowieka, a w obszarze prawa pozytywnego jest zapewnionym przez aparat państwowy prawem jednostki do jej autonomii.

Stuart A.H. wskazuje na następującą definicję „prawa do bycia zapomnianym", przyjmując, iż jest to termin nawiązujący do prawa jednostki w zakresie kontroli i możliwości usunięcia jej osobistych wiadomości znajdujących się w zasięgu innych osób, zazwyczaj z uwagi na fakt, że informacja ta straciła na znaczeniu, bądź stała się nieaktualna, w związku z czym dalsze jej wykorzystywanie prowadzi do naruszenia prawa do prywatności[636]. Nieco bardziej ogólna, ale zwięzła definicja została opublikowana w 2010 r., na podstawie której „prawo do bycia zapomnianym" to „prawo osób fizycznych do spowodowania usunięcia ich danych oraz zaprzestania ich przetwarzania, jeżeli przestały być potrzebne do zgodnych z prawem celów"[637].

Szczegółowe ramy tego prawa wyznaczają regulacje przyjmowane na gruncie międzynarodowym, regionalnym i lokalnym, których implementację egzekwują względy praktyczne.

3.2.2. Funkcje „prawa do bycia zapomnianym"

Pojęcie funkcji jest terminem wieloznacznym. Różnie jest postrzegane i w zależności od zakresu badań i metodologii nadaje się jej inne znaczenie. W wyniku tego, sporne jest zinterpretowanie funkcji prawa w aspekcie ogólnosystemowym. Prawoznawstwo, jak dotąd, nie przyjęło żadnej powszechnej definicji funkcji prawa. Wątpliwości odnoszą się do samego pojęcia funkcji prawa oraz użyteczności analizy prawa przez pryzmat pełnionych funkcji oraz kategoryzacji funkcji systemu prawnego jako całości, jak i poszczególnych jego dziedzin. Celem zagwarantowania odpowiedniej ochrony prywatności nieodzowne jest oznaczenie

[635] J. Żak, *Koncepcja „prawa do bycia zapomnianym"*…, s. 155.
[636] A.H. Stuart, *Google search results: Burried if not forgotten…,* s. 464.
[637] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów…

funkcji prawa pozytywnego *ius positivum* odnośnie „prawa do bycia zapomnianym". Tak też, przez funkcję prawa powinno rozumieć się ideę, jakiej ma służyć określone rozwiązanie. Zbigniew Salwa za funkcję prawa uważa „założone w normach prawa podstawowe cele, jakie stawia sobie przyjęta regulacja prawna, ujęta w określone kierunki oddziaływania ustanowionych norm prawnych"[638]. Przepisy prawne powinny wskazywać na szybką drogę postępowania administracyjnego, w tym sądowego w sprawach o zapomnienie. W obu tych postępowaniach nie może dojść do zachwiania zasady dwuinstancyjności. Wchodząc w sferę prywatności człowieka, aparat państwowy musi działać zgodnie z zasadą legalizmu, a zatem w oparciu o obowiązujące normy prawne, zebrane w zbiór przepisów rangi ustawy. Funkcja prawa polega na wyznaczaniu kierunków oddziaływania na rzeczywistość społeczną oraz kształtowaniu metod ochrony określonych wartości. Instytucja prawa jest narzędziem koniecznym do należytego funkcjonowania społeczeństwa, wobec czego również i społeczeństwo musi zachować postawę legalizmu w stosunku do prawa. Godne uwagi jest to, że trzeba zważać na samo istnienie norm, niezależnie od ich treści[639]. W „prawie do bycia zapomnianym" jest to przestrzeganie przez operatorów sieci społecznościowych obowiązku usuwania informacji o każdym człowieku, które wchodzą w sferę jego prywatności, a zwłaszcza dóbr osobistych.

Pojęcie funkcji może być dwojako pojmowane[640]. W ujęciu szerszym oznacza wszelkie skutki oddziaływania norm prawnych, które mogą mieć atypowy charakter. W ujęciu wąskim z kolei sprowadza się do zaplanowanego z góry użytecznego kierunku oddziaływania na rzeczywistość społeczną norm prawnych[641].

„Prawo do bycia zapomnianym" charakteryzuje się co najmniej kilkoma funkcjami[642]. Analiza ich wszystkich jest niemożliwa. Do najważniejszych funkcji „prawa do bycia zapomnianym" zalicza się funkcję ochronną, prewencyjną, wychowawczą, zwyczaju oraz administracyjną[643].

Przy częstej dezaprobacie potrzeby istnienia funkcji ochronnej w prawie, funkcja ta ma charakter podstawowy, ponieważ reguły w zakresie „prawa do bycia zapomnianym" odnoszą się do ochrony podmiotów, gwarantując im standardy godności. Funkcja ochronna

---

[638] Z. Salwa, *Prawo pracy,* Olsztyn 1994, s. 26.
[639] S. Wronkowska, *Podstawowe pojęcia prawa i prawoznawstwa,* Poznań 2005, s. 129.
[640] K.W. Baran, *O funkcjach zbiorowego prawa pracy uwag kilka,* [w:] *Prawo pracy a wyzwania XXI-go wieku. Księga jubileuszowa Profesora Tadeusza Zielińskiego,* red. M. Matey-Tyrowicz, L. Nawacki, B. Wagner, Warszawa 2012, s. 399.
[641] *Tamże,* s. 399.
[642] J. Żołyński, *RODO. Prawo do zapomnienia…,* s. 202.
[643] Wszystkie funkcje mają jednakowe znaczenie dla „prawa do bycia zapomnianym". Ich kolejność jest przypadkowa.

ma charakter metafunkcji. W znaczeniu *sensu largo* w aspekcie wewnętrznym polega na ochronie praw i interesów jednostek, a w aspekcie zewnętrznym na oddziaływaniu zbioru norm tegoż prawa na społeczeństwo. Funkcja ta jest również rozpatrywana pod względem podmiotowym, gdzie obejmuje swą ochroną interesy indywidualnej osoby, a także ogółu zbiorowości. Służy zatem należytemu postępowi aparatu państwowego, które za swój cel obiera unikanie napięć społecznych. Oznacza ponadto jedno z założeń, jakim jest stanie na straży ochrony wartości moralnych. Nawiązując do „prawa do bycia zapomnianym", funkcja ochronna w systemie społecznej gospodarki rynkowej obejmuje interesy grupy osób wrażliwych. Przejawia się to w przestrzeganiu wartości społecznych, do których zalicza się godność, honor, autonomię, a przede wszystkim zakaz wkraczania w sferę wewnętrzną danego podmiotu. Funkcja ochronna przyznaje jednostce uprawnienie w postaci podjęcia szeregu czynności zapobiegających naruszeniu przez osoby trzecie sfery przyporządkowanej wyłącznie konkretnemu podmiotowi. „Prawo do bycia zapomnianym" musi być narzędziem zapewniającym ochronę osobom podlegającym wykluczeniu czy napiętnowaniu przez innych, a tym samym służy zabezpieczeniu fundamentalnego prawa jednostki, tj. godności, która stanowiąc prawo naturalne posiada nadrzędny charakter w stosunku do praw stanowionych przez państwo. Badana funkcja może być interpretowana także w połączeniu z dokonywaną regulacją, zatem jako prawo „twarde" lub „miękkie". Pierwsza z metod, ma wymiar administracyjno-represyjny i przejawia się w administracyjnym nadzorze oraz sankcji karnej w przypadku naruszenia nakazu, bądź zakazu. Przejawia się to w bezwzględnie obowiązującym kształcie regulacji i sądowej kontroli przestrzegania norm prawnych. Druga z metod, polega z kolei na uzyskaniu pozasądowej kontroli prywatności w cyberprzestrzeni poprzez zgłoszenie żądania usunięcia danych bezpośrednio od operatora witryny internetowej. Zobowiązanie państwa polega na tworzeniu przepisów prawa zgodnych z normami etycznymi, aprobowanymi przez społeczeństwo, zapewniających systemowy poziom ochrony prywatności. Warte podkreślenia jest to, że funkcja ta nie ma charakteru statycznego. W zakresie „prawa do bycia zapomnianym", ochrona skupia się na ograniczeniu, a nawet wyeliminowaniu zjawiska w postaci naruszenia prywatności konkretnej jednostki. Jeśli już do tego dojdzie, podejmowane są działania powstrzymujące przed kolejnymi naruszeniami lub zapobiegające powstaniu rzeczywistego zagrożenia. Do kategorii niedozwolonych aktów zalicza się przede wszystkim ingerencję w całe życie prywatne, naruszenie integralności psychofizycznej, naruszenie czci, honoru i dobrego imienia, czy

rozpowszechnienie faktów intymnych dotyczących danego podmiotu[644].

Kolejną z funkcji „prawa do bycia zapomnianym" jest funkcja prewencyjna. Od strony aksjologicznej swoją ochroną obejmuje dobra powszechne, a mianowicie ład, porządek, bezpieczeństwo, moralność bądź dobre obyczaje w społeczeństwie. Idea tej funkcji powinna być rozpatrywana w charakterze stabilizująco-dynamizującym. Wymiar stabilizujący koncentruje się na kreowaniu obrazu zrównoważonego i demokratycznego państwa prawnego. Wymiar dynamizujący z kolei klarownie określa uprawnienia podmiotu, którego dobro osobiste uległo naruszeniu albo zagrożeniu przez osobę trzecią. Funkcja prewencyjna powinna być przejawem ewolucji prawa, co oznacza, iż należy ją rozumieć w ten sposób, że główną rolę odgrywają normy prawne, mające na celu zabezpieczenie nie tylko interesu podmiotu wprost zainteresowanego aspektem prywatności, ale jednocześnie interesu powszechnego. Występuje zatem w ujęciu horyzontalnym i wertykalnym. Stąd też funkcję prewencyjną, inaczej porządkową, należy postrzegać od strony podmiotowej[645] i strony przedmiotowej[646]. Aktualnie, szybki postęp techniczny postawił nowe wyzwania w zakresie ochrony prywatności. Można na wielką skalę wykorzystywać poszczególne informacje, zawierające w sobie dane osobowe[647]. Z tego względu funkcja prewencyjna posiada postać gwarancyjną, pełni charakter funkcji bezpieczeństwa. Adresatów norm prawnych, którzy nie dokonują naruszenia reguł postępowania, nie spotkają negatywne skutki ze strony aparatu państwowego. W przeciwnym wypadku zostanie wymierzona sankcja karna, bezpośrednio wyrażona w danym akcie prawnym. Funkcja ta, jak można zauważyć, stanowi niejako wyraz granicy pomiędzy zakresem uprawnień państwa a sferą praw i wolności jednostki. W odniesieniu do „prawa do bycia zapomnianym" wyrazem funkcji prewencyjnej jest prowadzona polityka bezpieczeństwa, która polega na ograniczaniu wstąpienia przez podmioty trzecie w sferę prywatności, a ściślej ujmując, w sferę intymności każdej osoby. Funkcja ta ma na celu zapobieganie takim sytuacjom. Wychodzi się bowiem z założenia, że lepiej unikać ponoszenia konsekwencji braku zabezpieczenia.

„Prawo do bycia zapomnianym" pełni także funkcję wychowawczą. Polega na kształtowaniu prawidłowych zachowań jednostek i całych grup społecznych. Charakteryzuje się przejawem dbałości o dobro wspólne. Stosunki interpersonalne powinny być oparte na

[644] J. Żołyński, *RODO. Prawo do zapomnienia…,* s. 202-206.
[645] Przybiera postać horyzontalną, gdzie zabezpiecza interesy konkretnych podmiotów, istniejących na tej samej płaszczyźnie, wzajemnie na siebie oddziałujących.
[646] Przybiera postać wertykalną, gdzie zabezpiecza należytą sprawność państwa w zakresie prawidłowego kształtowania ładu i zasad współżycia społecznego.
[647] D. Dörre-Kolasa, *Wpływ rozporządzenia ogólnego na zakres ochrony danych osobowych przetwarzanych w związku z zatrudnieniem*…, s. 35.

poszanowaniu wolności i godności, czyli wartości rozumianych poprzez zakaz naruszania dóbr osobistych, ale nie tylko. Należy je także interpretować w oparciu o obiektywne kryteria dokonywania oceny danej jednostki. Zagadnienie funkcji wychowawczej w obszarze „prawa do bycia zapomnianym" dotyczy niemal wszystkich dziedzin prawa, wobec czego bierze udział w zapewnieniu powszechnego pokoju społecznego[648]. Z drugiej zaś strony, polega na zakazie nielegalnego ujawniania prywatności, a więc kształtuje wśród ludzi takie zachowania, które zmierzają do wzmacniania relacji między partnerami społecznymi[649]. Funkcja wychowawcza wyraża się w istnieniu zakazu wkraczania w sferę prywatności w postaci jej upubliczniania bez uprzednio wyrażonej zgody przez adresata[650]. Dokonując analizy „prawa do bycia zapomnianym" przez pryzmat tego, że nie jest ono prawem absolutnym, w odniesieniu do funkcji wychowawczej należy je rozpatrywać w kontekście społecznego oddziaływania prawa, a zatem zestawić to prawo z innymi prawami podmiotowymi człowieka, a przetwarzanie danych osobowych zorganizować w taki sposób, aby służyło społeczności ludzkiej.

Następną funkcją, którą pełni „prawo do bycia zapomnianym" jest funkcja zwyczaju. Nawiązuje ona ściśle do anglosaskiego systemu *common law,* stąd też istotne jest, aby zastanowić się, czy zwyczaj w ogóle jest funkcją w polskim porządku prawnym. Interpretując tę funkcję w kontekście metody prawno-teleologicznej, należy zauważyć, że funkcja prawa w swej istocie to obrany kierunek oddziaływania na rzeczywistość społeczną norm prawnych, a zatem zwyczaj tym bardziej uznać należy za funkcję prawa. W czynionych rozważaniach da się zauważyć zjawisko odwoływania przez problematykę zwyczaju do zagadnień aksjologicznych czy etycznych w oparciu o pozasystemowe źródła prawa, dlatego tak ważne jest przeciwdziałanie nieprawidłowym zwyczajom, aby w rezultacie ich stosowania nie przekształciły się w prawo zwyczajowe. Zwyczaj nie może pozostawać w sprzeczności *contra legem* z obowiązującym porządkiem prawnym. Nie jest dozwolone, aby stanowił podstawę do ujawnienia danych osobowych, a więc i prywatności[651].

---

[648] T. Liszcz, *Prawo pracy,* Warszawa 2011, s. 31.

[649] Relacje te musi charakteryzować wzajemne zaufanie, wiarygodność, zgoda, a od strony aksjologicznej szacunek do godności, dobrego imienia oraz pozostałych dóbr osobistych.

[650] Aby można było mówić o świadomym wyrażeniu zgody, osoba, której dane dotyczą musi posiadać wiedzę, przynajmniej w zakresie tożsamości administratora oraz zamierzonych celów przetwarzania danych osobowych. Oprócz tego, w celu zapewnienia dobrowolności, przedmiotowa zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w przypadku, gdy istnieje brak równowagi pomiędzy osobą, której dane dotyczą a administratorem danych osobowych, zwłaszcza wtedy, kiedy jest nim organ publiczny.

[651] Byłoby to wówczas złamaniem zasady zawartej w art. 51 ust. 1 Konstytucji RP, która przewiduje, że ujawnianie informacji odnośnie do swojej osoby ma charakter szczególny i wyjątkowy, ponieważ odbywa się wyłącznie na podstawie aktu prawnego rangi ustawowej. Niemożliwe jest zatem dokonywanie wykładni w sposób rozszerzający *sensu largo,* a więc i na zasadzie zwyczaju.

Zwyczaj stanowi przejaw doświadczenia społecznego. Nie jest obligatoryjne, żeby posiadał charakter powszechny. Równie dobrze może występować w konkretnym środowisku bądź być powiązany z określonymi sytuacjami. Może być ponadto wykorzystany jako źródło formowania relacji w społeczeństwie. Obraz przestrzegania niepisanych reguł (zwyczajów), ukazuje jakość społeczności w aspekcie słowności, tj. dotrzymywania słowa lub ustalonych, lecz niesformalizowanych zasad zachowania się[652]. Do zwyczaju więc zaliczać się będą niepisane reguły postępowania, stosowane przez odpowiednio długi okres, które nie będą prowadziły do naruszenia prawa. Wręcz przeciwnie, pozostając z prawem stanowionym w zgodzie, umożliwią znalezienie rozwiązania określonego stanu faktycznego[653]. Zagadnienie zwyczaju jest wyrazem dobrych obyczajów. Z „prawem do bycia zapomnianym" wiąże się w ten sposób, że może być brany pod uwagę przez operatorów stron internetowych, a podmiotom nadzorującym system internetowy umożliwiać szybkie wdrożenie należytych procedur, co z kolei może doprowadzić do uwzględnienia żądania podmiotu w postaci usunięcia danych osobowych. Zwyczaj powinien sprzyjać nowym kierunkom rozwoju w dobie nieustannie zmieniających się okoliczności[654].

Z „prawem do bycia zapomnianym" wiąże się także funkcja administracyjna, chociaż ma ona wydźwięk jedynie pomocniczy w zestawieniu z pozostałymi. Przez nią rozumie się tworzenie nowych regulacji, które będą dawać podmiotom podjęcie skutecznych kroków prawnych na drodze administracyjnej, urealniając przy tym zlikwidowanie zagrożenia bezprawnego wkraczania w sferę prywatności. Postępowanie sądowe jest zazwyczaj spóźnione, to znaczy inicjowane *post factum,* czyli po naruszeniu określonego dobra. Przyjęcie szczególnego trybu na ścieżce prawa administracyjnego jest przejawem formalizmu ograniczonego do minimum, co z kolei występuje na etapie postępowania sądowego. Aktualnie taką regulację stanowi Rozporządzenie o Ochronie Danych Osobowych, na mocy którego adresatowi przysługuje uprawnienie zwrócenia się do odpowiedniego organu, w tym wypadku operatora strony internetowej, z żądaniem usunięcia jego danych osobowych, podczas gdy nie wyraził zgody lub została ona cofnięta[655]. Funkcja administracyjna ma charakter zarówno prewencyjny, jak i wychowawczy. Ten pierwszy przejawia się w możliwości dochodzenia swoich praw na innej drodze niż sądowa. Uświadamia także

[652] T. Zieliński, *Prawo pracy. Zarys systemu, cz. 2,* Warszawa-Kraków 1986, s. 202.
[653] L. Petrażycki, *Wstęp do nauki polityki prawa,* Warszawa 1968, s. 29.
[654] J. Wierzbołowski, *Informacja i technologie informacyjne jako element przekształceń strukturalnych i systemowych w gospodarce światowej,* tom 46, Warszawa 1997, s. 47.
[655] M. Mędrala, *Ochrona pracowniczych danych osobowych w postępowaniu sądowym w sprawach z zakresu prawa pracy,* [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* red. D. Dörre-Kolasa, Warszawa 2017, s. 123.

operatorom witryn internetowych ujemne skutki ich działania w sytuacji wydania decyzji odmownej w przedmiocie żądania usunięcia danych. Obejmuje ochroną jednostki, których dane mogą ulec naruszeniu przed ryzykiem wyrządzenia szkody majątkowej czy niemajątkowej. Natomiast funkcja administracyjna w aspekcie wychowawczym powinna wpływać na zachowanie operatorów stron internetowych w ten sposób, aby zachowane było przestrzeganie obowiązującego porządku prawnego. Tym samym doprowadzi to do zwiększenia poziomu kultury prawnej obywateli oraz innych podmiotów funkcjonujących w państwie wobec zmieniającej się rzeczywistości i kształtu instytucji prawnych.

„Prawo do bycia zapomnianym" wpisuje się raczej w generalne pojęcie funkcji prawa, ponieważ wyraża określony cel społeczny. Ideą funkcji „prawa do bycia zapomnianym" jest przeciwstawianie się powstaniu stanu zagrożenia, przejawiającego się pod postacią postępowania nieetycznego, niemoralnego i niekorelującego z zasadami współżycia społecznego.

3.2.3. „Prawo do bycia zapomnianym" – prawo publiczne czy prywatne

W nauce prawa pojawia się pytanie o charakter aktualnych i przyszłych regulacji. Sprowadza się ono do wyjaśnienia, czy mają one swoje źródło w prawie prywatnym, czy też publicznym. Zacieśnia się to do skonkretyzowania uprawnień adresatów norm prawnych oraz władczej ingerencji podmiotów trzecich[656]. Problematyka badań aksjologicznych, w tym ochrony prywatności jednostki, nie jest zamknięta i zobowiązuje do dalszych badań. Stąd też należy się zastanowić, czy „prawo do bycia zapomnianym" jest wartością tylko osobistą (prywatną), czy też obiektywną (powszechną).

Analizę charakteru „prawa do bycia zapomnianym" należy łączyć z prawem do prywatności. Nie jest łatwym zadaniem przyporządkować „prawo do bycia zapomnianym" do kategorii praw prywatnych lub powszechnych oddzielając je od prawa, z którego się wywodzi. To, czy „prawu do bycia zapomnianym" należy nadać miano prawa osobistego, czy powszechnego, należy oceniać kompleksowo, w szerszym zakresie, tj. brać pod uwagę całokształt okoliczności jego powstawania.

Argumentem, świadczącym o tym, że „prawo do bycia zapomnianym" należy traktować jako prawo osobiste, jest ten, który nakazuje przyjąć, że uprawnienie usunięcia informacji przysługuje konkretnemu podmiotowi danych, którego prywatność została

[656] A. Musiała, *Prawo pracy: prawo publiczne czy prawo prywatne,* „Praca i Zabezpieczenie Społeczne" 2017, nr 12, s. 2-7.

naruszona lub zagrożona. Pewna sfera życia człowieka podlega ochronie wyłącznie z uwagi na jego interes. „Prawo do bycia zapomnianym" w tym założeniu stanowi wyraz godności człowieka, jego honoru, czci, szacunku dla niego, ale jest też przede wszystkim wyrazem wolności. Aparat państwowy, wbrew woli zainteresowanej osoby, nie może wkraczać w sferę życia prywatnego jednostki, nawet przy założeniu, że chce ją objąć bezwzględną ochroną. Państwu przysługuje wyłącznie uprawnienie wyznaczania granic ochrony prywatności, pozostawiając każdemu niezależność w dochodzeniu swoich praw. „Prawo do bycia zapomnianym" jako element prawa do prywatności ze swej istoty należy zaliczyć do dziedziny prawa cywilnego, co może przemawiać za osobistym charakterem tego prawa.

W regulacjach prawnych Rozporządzenia przewidziano możliwość skorzystania przez podmiot danych z „prawa do bycia zapomnianym", co nie jest równoznaczne z nakazem jego zastosowania w przypadku naruszenia prawa do prywatności jednostki. Pozostawiono podmiotowi danych pełną swobodę sumienia, a zatem prawo nie może prowadzić do likwidowania sfery prywatności człowieka.

„Prawo do bycia zapomnianym" ma także objąć swoją ochroną dobra należące do kategorii praw człowieka, a więc nie tylko te chronione przez prawo prywatne. Gdyby to były jedynie cele prywatne, nie byłyby chronione przez Konstytucję RP, a zatem najwyższy akt prawny w państwie, a nawet przez akty normatywne niższego rzędu, tj. ustawę o ochronie danych osobowych. „Prawo do bycia zapomnianym" cechuje się również charakterem publicznym z uwagi na to, że w zakres ochrony wkraczają regulacje określające sposoby zachowania. Składając się na element prawa do prywatności, powinno być rozpatrywane nie tylko w wymiarze podmiotowym pod względem ochrony odbiorców tego prawa, ale również pod względem przedmiotowym. Przez to można rozumieć, że prywatność nie posiada cechy *erga omnes*, tj. prawa bezwzględnego. Wobec tego, człowiek nie ma takich środków, które uprawniałyby go do czynienia wszystkiego, co mu się podoba.

W wymiarze aksjologicznym, prawo pozytywne powinno wyznaczać linię graniczną, która będzie określać moment przeistaczania się prywatności z wymiaru prywatnoprawnego na publicznoprawny. Podmiot nie ma prawa czynić użytku powszechnego z każdej informacji, którą chciałby wprowadzić w obieg. Stąd też w znaczeniu przedmiotowym, prywatność człowieka jest ograniczona z uwagi na dobro wspólne obywateli, tzn. ze względu na interes państwa odpowiedzialny za kształtowanie postaw obywatelskich. Postawy obywatelskie przybierają różne formy i postaci. Najczęściej są to przyjęte w danym środowisku zwyczaje czy uwarunkowania religijne, bądź kulturowe. Można powiedzieć, że wartość w postaci prywatności kończy się tam, gdzie zachodzi potrzeba ochrony szeroko rozumianego dobra

powszechnego.

„Prawu do bycia zapomnianym" można nadać miano prawa o charakterze publicznym jeszcze z innego powodu. Dochodząc przysługujących praw za jego naruszenie, można skorzystać ze stosownych regulacji prawnych, które weszły w życie w wyniku rozwiązań unijnych w 2018 roku. Wykorzystuje się też uregulowania prawne w polskim porządku prawnym, które zostały przyjęte w wyniku tych rozwiązań. Charakteryzują się cechami prawa administracyjnego, a zatem związane są ze sferą publiczną[657]. Dla wykonania norm z zakresu prawa administracyjnego, ważne jest istnienie podstawy prawnej działania, stosowny organ oraz realizacja danych czynności przez organ w przypadku ziszczenia się odpowiednich ku temu przesłanek. Stąd też, jeśli termin „organ" zastąpiony zostanie instytucją czy podmiotem, to okaże się, że Ogólne Rozporządzenie o Ochronie Danych Osobowych spełnia wszystkie wyżej wymienione kryteria.

Za publicznym charakterem norm „prawa do bycia zapomnianym" przemawia ponadto waga interesu publicznego. Nakazuje ono usunięcie niektórych danych z powodu szeroko rozumianego interesu publicznego, np. ze względów psychologicznych i moralnych. Niezareagowanie operatorów nośników informatycznych, na których takie dane zostaną zamieszczone, powinno skutkować wprowadzeniem stosownych regulacji normatywnych, które swoim zasięgiem będą obejmować kary o charakterze administracyjno-karnym poprzez nakładanie obowiązków przez organy państwa powołane do ochrony danych osobowych bez konieczności inicjowania postępowania cywilnego przez zainteresowane osoby.

Można jeszcze poddać pod rozwagę, czy „prawo do bycia zapomnianym" nie ma przypadkiem charakteru *quasi-publicznego.* Coraz bardziej popularne staje się stwierdzenie, że z „prawa do bycia zapomnianym" korzystają głównie osoby, których dane zostały ujawnione w sieci. Tak więc, ujawniając prywatność osób w środkach przekazu cyfrowego, można naruszyć także prawa o zasięgu powszechnym. Ujawniane informacje mogą odnosić się do tych o charakterze np. psychicznym (depresja, samouszkodzenia). Zachowania autodestrukcyjne mogą być zaraźliwe. Rodzi się zatem problem w zakresie ochrony ogółu społeczeństwa przed rozpowszechnieniem pewnych szkodliwych powszechnie wiadomości. Z jednej strony, zainteresowany podmiot może domagać się usunięcia z obiegu tych informacji w Internecie. Z drugiej strony, nie powodują one naruszenia prywatności tylko

[657] Nie byłoby do końca prawdziwym stwierdzenie, że „prawo do bycia zapomnianym" jest prawem administracyjnym *sensu stricte*. Należy raczej do sfery prawa administracyjnego. Rozporządzenie nr 2016/679 w wielu swoich regulacjach prawnych posługuje się władztwem, które przejawia się w nakładaniu kar finansowych, zakazie gromadzenia określonych danych osobowych, regułach przetwarzania danych osobowych, co jest cechą prawa administracyjnego.

konkretnego podmiotu, ale też i społeczności, chociażby z uwagi na to, że mogą na nią oddziaływać.

W mojej ocenie, „prawo do bycia zapomnianym" powinno być w głównej mierze zaliczane do kategorii praw osobistych z dwóch powodów. Po pierwsze, „genetycznie" pochodzi od prawa do prywatności. Po drugie, przysługuje osobie, która ma interes w tym, aby dane jej dotyczące zostały usunięte, jeśli okażą się w jakiś sposób szkodliwe. Dopiero w następnej kolejności, można szukać argumentów, które przemawiają za tym, że „prawo do bycia zapomnianym" można włączyć w zbiór praw o charakterze publicznym.

3.3. Analiza „prawa do bycia zapomnianym" w oparciu o treść art. 17 Rozporządzenia nr 2016/679

3.3.1. Zakres podmiotowy „prawa do bycia zapomnianym" – podmiot uprawniony

Zgodnie z treścią art. 17 RODO, podmiotem uprawnionym do skorzystania z „prawa do bycia zapomnianym" jest „osoba, której dane dotyczą", a zatem tylko osoba fizyczna. Rozporządzenie nie odnosi się do przetwarzania danych osobowych osób prawnych, zwłaszcza przedsiębiorstw uznanych za osoby prawne[658]. Zawężenie zakresu podmiotowego „prawa do bycia zapomnianym" jedynie do osoby fizycznej nie jest tożsame z tym, iż w ramach wskazanej kategorii osób nie można dokonać jakiegoś zróżnicowania. Wniosek ten można wyciągnąć przede wszystkim z treści art. 17 Rozporządzenia, gdzie określono przesłanki warunkujące korzystanie z „prawa do bycia zapomnianym" oraz przesłanki wyłączające to prawo[659].

Przetwarzanie danych w praktyce i ich upublicznianie dotyczy również osób, które nie mają pełnej zdolności do czynności prawnych. Pojawia się kwestia ustalenia, czy i w jakim zakresie osoby takie efektywnie będą mogły dochodzić „prawa do bycia zapomnianym". M. Jabłoński oraz J. Węgrzyn zauważają pewne rozwiązania, które mają polegać na odróżnieniu dwóch płaszczyzn.

Pierwsza płaszczyzna dotyczy sytuacji, w której osoba wyraża zgodę na przetwarzanie jej danych przez administratora, a dotyczy to czynności, jakie można zaliczyć do czynności nieprzekraczających zakresu zwykłego zarządu, to znaczy takich, które mieszczą się w kategorii drobnych bieżących spraw życia codziennego (np. akceptacja regulaminów

[658] Motyw 14 RODO.
[659] M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym…,* s. 145-146.

bezpłatnego dostępu do wyszukiwarki internetowej). Według M. Jabłońskiego i J. Węgrzyn mają one charakter cywilnoprawny, a zatem możliwe jest zgłoszenie żądania niezwłocznego usunięcia danych osobowych, jak również poinformowania innych administratorów przetwarzających te dane o tym zgłoszeniu, co również wiąże się z obowiązkiem usunięcia przez nich wszystkich łączy tych danych, ich kopii, bądź replikacji[660].

Sytuacja ta nie jest już tak oczywista w razie odmowy przez administratora spełnienia żądania i zaistnienia konieczności wystąpienia do organu ochrony danych, jak i nawet do sądu administracyjnego. Wymagane zdaje się być przeprowadzenie oceny zdolności procesowej takiej osoby w kontekście realizacji konstytucyjnego prawa dostępu do informacji publicznej. Sąd administracyjny – badając zdolność siedemnastolatka – zajął stanowisko, że „w sprawach sądowo-administracyjnych zdolność procesową posiadają osoby fizyczne mające pełną zdolność do czynności prawnych”[661]. To zaś oznacza, że z punktu widzenia wykonywania praw w jakimkolwiek postępowaniu sądowym, osoba taka nie będzie mogła zostać uznana za uprawnioną, posiadającą zdolność procesową, w zakresie dochodzenia swoich praw. Ustawa o ochronie danych osobowych nie precyzuje wyjątku, który gwarantowałby takim osobom możliwość skutecznego realizowania praw skonkretyzowanych w RODO, w tym „prawa do bycia zapomnianym”.

Biorąc pod uwagę charakter obowiązujących w Polsce regulacji, tj. przepisów prawa materialnego, nie sposób uznać, że twierdzenie, na podstawie którego każda osoba, której dane dotyczą, niezależnie od tego, czy posiada pełną zdolność do czynności prawnych, czy też nie, będzie uprawniona do realizacji „prawa do bycia zapomnianym” w pełnym zakresie, jest niezgodne z prawdą. Dopóki nie zostaną wprowadzone zmiany, dopóty konieczne staje się podjęcie odpowiednich działań za małoletniego przez jego przedstawiciela ustawowego, tak w odniesieniu do wystąpienia ze skargą do krajowego organu ochrony, jak i później do sądu administracyjnego.

3.3.2. Zakres podmiotowy „prawa do bycia zapomnianym” – podmiot zobowiązany

Zgodnie z treścią art. 17 ust. 1 RODO, adresatem obowiązku uregulowanego w tym przepisie, jest administrator. Przez administratora należy rozumieć „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie

[660] M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym*…, s. 146-147.
[661] Postanowienie NSA z dnia 21 marca 2017 r., sygn. akt: I OSK 2500/16.

z innymi ustala cele i sposoby przetwarzania danych osobowych”[662]. Otrzymanie statusu administratora nie należy utożsamiać z faktycznym posiadaniem danych. Podstawowym kryterium odróżniającym administratora danych osobowych od innych podmiotów przetwarzających dane jest „sprawowanie faktycznej kontroli nad przetwarzaniem danych, a więc decydowanie o celach i sposobach przetwarzania, nie zaś faktyczne przetwarzanie, które może zostać powierzone innemu podmiotowi”[663]. Przymioty te posiada operator wyszukiwarki internetowej. Jego działalność polega na zlokalizowaniu informacji opublikowanych albo zamieszczonych w Internecie przez osoby trzecie, indeksowaniu ich w automatyczny sposób, czasowym ich przechowywaniu oraz udostępnianiu internautom w uporządkowany sposób, zgodnie z określonymi preferencjami, w sytuacji, gdy takie informacje zawierają dane osobowe. Oprócz operatorów wyszukiwarek internetowych, podmiotami zobowiązanymi do realizacji „prawa do bycia zapomnianym” mogą być także inne podmioty świadczące usługi społeczeństwa informacyjnego[664]. Do kategorii osób wykonujących „prawo do bycia zapomnianym” wchodzą też podmioty dokonujące sprzedaży towarów przez Internet, dostarczanych drogą tradycyjną, a nie elektroniczną[665].

Wyróżnia się także podmioty, które nie są obowiązane do realizacji „prawa do bycia zapomnianym”. Do nich zalicza się podmioty, które świadczą usługi hostingowe, czyli prowadzą portale społecznościowe, np. Facebooka. Udostępniają oni „zasoby systemu teleinformatycznego celem przechowywania i udostępniania przez osoby trzecie – usługobiorców (odpowiednio: wypowiedzi w poszczególnych grupach dyskusyjnych, oferty w aukcjach internetowych, zdjęcia lub inne informacje zamieszczone w serwisie społecznościowym, poszczególne wpisy na blogach)”[666]. Wobec tego, nie podejmują samodzielnie „decyzji o celach przetwarzania danych osobowych będących przedmiotem hostingu. Wybór celów przetwarzania danych osobowych rozumiany jako wybór wartości, dla urzeczywistnienia których dochodzić będzie do przetwarzania danych osobowych, dokonywany jest bowiem przez podmiot, który decyduje o przeznaczeniu danych osobowych

[662] M. Jabłoński, K. Wygoda, *Praktyczne znaczenie podstawowych pojęć RODO-wybrane zagadnienia,* Wrocław 2019, s. 9.
[663] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* red. P. Litwiński, Warszawa 2018, s. 217.
[664] Usługa społeczeństwa informacyjnego to każda usługa normalnie świadczona za wynagrodzeniem, na odległość, drogą elektroniczną, a ponadto na indywidualne żądanie odbiorcy usług. Zob. T. Grzegory, *Pamięć absolutna czy kontrolowana amnezja…,* s. 66.
[665] Pod warunkiem, że można im przyznać status administratora, a oprócz tego znajdzie zastosowanie jedna z przesłanek z art. 17 ust. 1 RODO.
[666] P. Litwiński, *Hosting danych osobowych. Zagadnienia podstawowe,* „Monitor Prawniczy” 2008, nr 23, s. 1258.

będących przedmiotem hostingu. W każdym więc przypadku, cele określane są nie przez podmiot, który faktycznie dane przechowuje (dostawca usług hostingowych), lecz przez podmiot, który z usług hostingowych korzysta"[667].

Administratorem jest użytkownik korzystający z usługi hostingowej, zaś dostawca usług hostingowych jest administratorem jedynie danych osoby korzystającej z jego usług. Czy zatem, użytkownik usługi hostingowej może być uznany za administratora według rozwiązań przyjętych przez RODO? Z art. 2 ust. 2 lit. c) w zw. z motywem 18 Rozporządzenia wynika, że nie ma ono zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze, czyli bez związku z działalnością zawodową lub handlową. Działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz na działalności internetowej podejmowanej w ramach takiej działalności. Niniejsze Rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej. To oznacza, iż w przypadku serwisów społecznościowych służących do kontaktów zawodowo-biznesowych, takich jak LinkedIn, jego użytkownik może zostać uznany za administratora, gdy zamieści dane osobowe współpracowników w tym serwisie. Czynności niektórych użytkowników sieciowych serwisów społecznościowych mogą nie mieścić się w ramach działań o czysto osobistym lub domowym charakterze, np. w momencie, gdy są stosowane jako platforma współpracy w ramach stowarzyszenia albo przedsiębiorstwa. Użytkownik przyjmuje wówczas pełnię obowiązków administratora danych ujawniającego dane osobowe innemu administratorowi danych lub osobom trzecim. Użytkownik musi uzyskać zgodę osób zainteresowanych lub wskazać inną podstawę prawną przewidzianą w RODO[668]. Nie jest jednak tak, że używanie serwisu społecznościowego dla innych celów niż cele komercyjne, polityczne lub charytatywne, będzie miało charakter osobisty lub domowy. Już Grupa Robocza Art. 29 sygnalizowała, że „dostęp do danych przekazanych przez użytkownika jest ograniczony do samodzielnie wybranych kontaktów. Jednakże w niektórych przypadkach użytkownicy mogą mieć wiele kontaktów z osobami trzecimi, lecz nie wszystkich mogą faktycznie znać. Duża ilość kontaktów mogłaby wskazywać, że wyłączenie do celów domowych nie obowiązuje,

[667] P. Litwiński, *Hosting danych osobowych*…, s. 1261.
[668] Grupa Robocza Art. 29, Opinia 5/2009 w sprawie portali społecznościowych przyjęta w dniu 12 czerwca 2009 r., WP 163, Bruksela 2009, s. 7.

a więc użytkownika można byłoby uznać za administratora danych”[669]. Biorąc to pod uwagę, można przyjąć, że wyłączenie z art. 2 ust. 2 lit. c) w zw. z motywem 18 RODO nie ma zastosowania, gdy użytkownik serwisu społecznościowego, umieszczając w nim dane innych osób, zmienił ustawienia prywatności na publiczne, dzięki czemu stały się one dostępne dla nieograniczonej liczby osób. Upublicznienie danych przez użytkownika serwisu społecznościowego mieści się w pojęciu działalności czysto osobistej, pod warunkiem, że nie jest związane z celem zarobkowym.

W wyroku z dnia 5 czerwca 2018 r. w sprawie zawisłej pod sygn. akt: C-210/16 Trybunał Sprawiedliwości Unii Europejskiej uznał za administratora spółkę prawa prywatnego świadczącą usługi kształcenia przy wykorzystaniu fanpage’a prowadzonego na portalu społecznościowym Facebook. Podmiot uzyskał anonimowe dane statystyczne dotyczące osób odwiedzających te strony za pomocą funkcji Facebook Insights. Dane tych osób zbierane były za pomocą plików szpiegujących, tzw. cookies, z których każdy zawiera oryginalny kod użytkownika. Pliki te były zapisywane przez Facebooka na twardym dysku komputera osób odwiedzających fanpage’a. Stworzenie fanpage’a na Facebooku jest związane z podjęciem przez jego administratora działań polegających na ustaleniu parametrów zależnych od jego użytkowników docelowych, a także od celów w zakresie zarządzania lub promocji jego działalności, co wpływa na przetwarzanie danych osobowych na potrzeby statystyk przygotowywanych na podstawie liczby osób odwiedzających fanpage’a. Administrator może za pomocą filtrów udostępnionych przez Facebooka zdefiniować kryteria, na podstawie których statystyki te muszą być przygotowywane, a nawet wskazać kategorie osób, których dane osobowe będą wykorzystywane przez Facebooka. W rezultacie administrator fanpage’a przyczynia się do procesu przetwarzania danych osobowych podmiotów odwiedzających jego stronę[670]. Z tego powodu, Trybunał Sprawiedliwości Unii Europejskiej uznał, że administratorem danych w rozumieniu art. 2 lit. d) Dyrektywy 95/46/WE jest administrator fanpage’a. Te orzeczenie, mimo że zostało wydane na tle Dyrektywy 95/46/WE, pozostaje aktualne, gdyż definicja administratora przyjęta w art. 4 pkt 7 RODO nie różni się od definicji administratora danych, która obowiązywała pod rządami Dyrektywy 95/46/WE[671].

Określenie podmiotu zobowiązanego do realizacji „prawa do bycia zapomnianym” nie

[669] *Tamże.*
[670] Wyrok TSUE z dnia 5 czerwca 2018 r. w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH,* sygn. akt: C-210/16, [dostęp:] https://curia.europa.eu/juris/liste.jsf?language=pl&td=ALL&num=C-210/16.
[671] M. Górski, *Właściciel fanpage’a na portalu społecznościowym jako administrator,* „ABI Expert” 2018, nr 3, s. 52.

jest łatwym zadaniem. Nie jest do końca jasne, czy portale społecznościowe, np. Facebook, Twitter uznaje się za administratorów i czy są one zobligowane do usunięcia treści zamieszczonych przez użytkowników na temat innej osoby w ramach czynności o czysto osobistym lub domowym charakterze, gdy wystąpi z takim żądaniem. Konkluzja sprowadza się do tego, że portale społecznościowe są administratorami danych osobowych tylko ich użytkowników.

Art. 4 pkt 7 Rozporządzenia dopuszcza możliwość, aby przepisy kraju członkowskiego wskazywały bezpośrednio administratora lub konkretne kryteria jego wyznaczenia. Praktyka natomiast pokazuje, że ustawodawca polski skorzystał z pierwszego rozwiązania. Niemniej, przyjęcie modelowego schematu ustalenia statusu administratora stanowiłoby uproszczenie w praktyce stosowania regulacji z zakresu ochrony danych osobowych[672].

3.3.3. Zakres usunięcia danych osobowych przez administratora

Administrator danych osobowych powinien niezwłocznie usunąć dane, które zostały objęte wnioskiem o ich usunięcie. Odnosi się to do wszystkich miejsc, w których znajdują się dane osoby, która dochodzi wykonania swojego „prawa do bycia zapomnianym". Najczęściej są to serwery obsługiwane przez administratora, w tym serwery poczty e-mail, dane kontaktowe zarówno w formie cyfrowej, jak i w postaci papierowych kopii danych. Dane powinny być usuwane w taki sposób, aby uniemożliwić jakikolwiek do nich dostęp w przyszłości pozwalający na identyfikację osoby, której dane dotyczą. Jednym z proponowanych sposobów usunięcia danych osobowych z kopii papierowych jest zaczernienie ich w dokumentach zawierających te dane[673].

Nie ma jednolitego wzoru wniosku o usunięcie danych w ramach „prawa do bycia zapomnianym". To oznacza, że panuje pełna swoboda co do jego formy, co może okazać się problematyczne. Niemniej jednak, przydatne jest klarowne opisanie swojego żądania oraz wskazanie, które dokładnie dane należy usunąć i z jakiego powodu.

Usunięcie danych osobowych rozumiane jako całkowite zapomnienie o danych i o podmiocie danych pozostaje w sprzeczności z zasadą rozliczalności. Tak też, np. w obszarze rachunkowości nie istnieje instytucja usunięcia danych. Istnieje jedynie dodanie

[672] M. Jabłoński, K. Wygoda, *Praktyczne znaczenie…,* s. 11.
[673] Wyrok NSA z dnia 11 kwietnia 2017 r., sygn. akt: I OSK 2170/15, LEX nr 2296415.

im stanu negatywnego[674]. Kłopoty związane z tym, jak osiągnąć cel samego prawa do usunięcia danych osobowych i nie narazić ich przy tym na ryzyko uszkodzenia, stanowią nie lada wyzwanie. Kolejnym potencjalnym problemem stają się dane nieustrukturyzowane. W zasadzie, administrator danych osobowych nie ma obowiązku przeszukiwać wszystkich swoich zasobów informacyjnych celem znalezienia i usunięcia danych. Tam, gdzie administrator nie zna tożsamości osób, których dane przetwarza, w tym nie posiada wiedzy na temat treści danych, co do zasady nie ma potrzeby przeszukiwania nieustrukturyzowanych danych tylko po to, żeby wymazać z nich dane osoby, która domaga się usunięcia danych. Sama realizacja „prawa do bycia zapomnianym" powinna być udokumentowana dla potrzeb ewentualnego sporu, jak też w celu zadośćuczynienia rozliczalności. Zatem ciężko też sobie wyobrazić sytuację całkowitego wymazania człowieka z pamięci. Z perspektywy funkcjonalnej, „prawo do bycia zapomnianym" służy temu, aby dana instytucja nie wykonywała niektórych czynności odnoszących się do zainteresowanego oraz nie szerzyła o nim pewnych informacji. Wymazanie informacji z systemów informatycznych nie chroni do końca podmiotu danych przed ponownym wykorzystaniem tych informacji, zwłaszcza gdy informacje wymieniane są pomiędzy różnymi administratorami[675]. Niewykluczone zatem, że niekiedy oprócz usunięcia z systemów informatycznych wszystkich informacji, konieczne będzie umieszczenie osoby na liście wyjątków[676], np. na liście robinsonów[677].

W dniu 10 stycznia 2019 roku Rzecznik Generalny Trybunału Sprawiedliwości Maciej Szpunar sporządził opinię w sprawie „prawa do bycia zapomnianym" w wyszukiwarce internetowej Google[678]. Konkretnie zastanawiano się nad tym, czy jeśli podmiot, którego dane dotyczą, zawnioskuje o „prawo do bycia zapomnianym" w zakresie jego informacji wrażliwych, to czy na Google nałożony jest bezwzględny obowiązek usunięcia danych takiej osoby[679]. W przedmiotowej sprawie, CNIL[680] podzielił stanowisko spółki Google, która odmówiła usunięcia informacji z wyników wyświetlanych w wyszukiwarce internetowej na

[674] Odbywa się to za pomocą storno czarnego lub czerwonego, czyli zapisu anulującego błędną operację księgową, gdzie nie skreśla się przy tym zapisu mylnego. Inaczej mówiąc, jest to zapis oparty na regule podwójnego zapisu.
[675] Dlatego powstał obowiązek poinformowania innych administratorów o usunięciu danych osobowych.
[676] Katalog osób, których dane osobowe objęte są restrykcjami przetwarzania.
[677] Katalog osób, które nie życzą sobie kontaktu.
[678] Opinia Rzecznika Generalnego Macieja Szpunara z dnia 10 stycznia 2019 r., sygn. akt: C-507/17 w sprawie *Google LLC przeciwko CNIL,* ECLI:EU:C:2019:15 koncentrowała się na wyroku Trybunału Sprawiedliwości UE z dnia 24 września 2019 r., sygn. akt: C-136/17 w sprawie *GC i in. przeciwko CNIL* (Dz. Urz. UE Seria C, 2019/C 399/02) wydanym w przedmiocie przetwarzania danych wrażliwych w Internecie.
[679] Sprawa, której dotyczy opinia jest oparta na stanie prawnym obowiązującym przed wejściem w życie unijnego Rozporządzenia, jednak wnioski tam zawarte mają znaczenie dla sposobu wykładni „prawa do bycia zapomnianym" w formie, jaka obowiązuje po dniu 25 maja 2018 r.
[680] Commission Nationale de l'Informatique et des Libertés (francuski organ administracji publicznej odpowiedzialny za regulacje w związku z przetwarzaniem danych osobowych).

podstawie zgłoszonego żądania przez czterech obywateli francuskich[681]. Podmioty danych, dążące do realizacji „prawa do bycia zapomnianym" zaskarżyły decyzję do francuskiej Rady Stanu[682]. Organ ten skierował pytanie prejudycjalne do Trybunału Sprawiedliwości Unii Europejskiej o zakres realizacji „prawa do bycia zapomnianym" w wyszukiwarkach internetowych. Odnosiło się ono konkretnie do obowiązku operatora wyszukiwarki, będącego jednocześnie administratorem danych osobowych, polegającego na regularnym usuwaniu linków do stron internetowych, na których znajdują się dane wrażliwe. W wyroku w sprawie Google Spain i Google (C-131/12) zostało określone, że „prawo do bycia zapomnianym" przysługuje każdej osobie fizycznej, która może zgłosić takie żądanie podmiotom prowadzącym wyszukiwarki internetowe. Z kolei orzeczenie TSUE w niniejszej sprawie (C-136/17) wyjaśnia natomiast, czy „prawo do bycia zapomnianym" i zakaz przetwarzania wrażliwych danych osobowych ma charakter absolutny, czy jednak istnieją takie sytuacje, w których nad prywatnością jednostki przeważają interes publiczny, prawo do informacji i wolność słowa[683]. W ocenie Rzecznika Generalnego, operatorzy wyszukiwarek internetowych powinni uwzględniać żądanie usunięcia danych, jednak muszą też brać pod uwagę czy usunięcie linku nie naruszy ww. wartości publicznych. Rzecznik Generalny w swoich rozważaniach odwołał się do art. 9 Dyrektywy 95/46/WE[684] konkludując, że nawet w przypadku danych wrażliwych nie można automatycznie zadecydować o ich usunięciu za każdym razem, kiedy zażąda tego osoba, której takie dane dotyczą[685]. Trybunał Sprawiedliwości Unii Europejskiej w swoim wyroku stwierdził, że operator wyszukiwarki jest co do zasady zobowiązany do uwzględnienia żądania usunięcia linków prowadzących do stron zawierających szczególne kategorie danych, z zastrzeżeniem wyjątków przewidzianych w Dyrektywie[686]. Odniósł się również do kwestii usunięcia informacji dotyczących przestępstw, które nie są już aktualne. Tak też, na operatora wyszukiwarki internetowej został nałożony obowiązek usunięcia linków, jeśli prawo do ochrony danych osobowych przeważa

[681] Informacje te odnosiły się do różnego rodzaju działalności i wydarzeń z przeszłości tych osób. Były to satyryczne obrazki, orzeczenia o wszczęciu śledztwa, jak również dane o angażowaniu się przez Francuzów w działania na rzecz Kościoła Scjentologicznego.
[682] Odpowiednik Naczelnego Sądu Administracyjnego w Warszawie.
[683] K. Szczudlik, *Granice prawa do bycia zapomnianym,* [dostęp: 29.01.2019] https://newtech.law/pl/granice-prawa-do-bycia-zapomnianym/.
[684] Dotyczy on możliwości niestosowania regulacji w przedmiocie realizacji „prawa do bycia zapomnianym" w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego.
[685] Zaprezentowana interpretacja art. 9 Dyrektywy 95/46/WE i jego wpływu na wykonywanie „prawa do bycia zapomnianym" może mieć znaczenie dla art. 17 ust. 3 RODO na gruncie nowej regulacji.
[686] Jeden z wyjątków [art. 8 ust. 2 lit. e)] pozwalał na przetwarzanie danych wrażliwych, jeżeli zostały one podane do publicznej wiadomości przez sam podmiot danych. W tej sytuacji, operator wyszukiwarki internetowej nie musiał usuwać linków, ale w każdym przypadku musiał sprawdzić, czy z uwagi na względy związane z ważnym interesem publicznym, umieszczenie linku do danej strony internetowej jest niezbędne dla skorzystania przez internautów z prawa do wolności informacji.

nad prawem do informacji potencjalnych interesantów. Natomiast w przypadku nieusunięcia linku, operator powinien w taki sposób zorganizować wyświetlanie wyników w wyszukiwarce, aby linki z najbardziej aktualnymi informacjami znajdowały się na pierwszym miejscu listy wyszukiwania[687].

3.3.4. Podstawy żądania usunięcia danych

Prawodawca unijny w przepisach RODO przewiduje, że każda osoba w dowolnym czasie ma prawo zwrócić się do administratora z żądaniem usunięcia danych. W toku podjętych rozważań nad finalnym kształtem „prawa do bycia zapomnianym" podjęto decyzję o stworzeniu zamkniętego katalogu przesłanek uzasadniających skorzystanie z tego prawa.

Po pierwsze, unijne Rozporządzenie o Ochronie Danych Osobowych daje możliwość żądania usunięcia danych, gdy stały się niezbędne do celów, dla których zostały zebrane lub w inny sposób przetwarzane. Podstawowe znaczenie ma tutaj zasada minimalizacji danych z art. 5 ust. 1 lit. c) RODO, zakładająca przetwarzanie danych osobowych adekwatnych i niezbędnych do osiągnięcia zamierzonego przez administratora celu. Jednym z popularnych przykładów, wyjaśniających to zjawisko, jest wzajemne oświadczenie woli. W momencie, kiedy dane stają się nieprzydatne do wykonywania umowy, ponieważ została już zrealizowana, mogą być w dalszym ciągu konieczne na wypadek roszczeń, aż do czasu upływu okresu przedawnienia. Stąd też, wygaśnięcie podstawowego celu przetwarzania danych, nie musi w gruncie rzeczy oznaczać, że dane stały się zbędne. W tej sytuacji, to administrator danych osobowych musi dokonać oceny przydatności danych osobowych, kierując się regulacjami zawartymi w RODO. Nawiązuje to również do przesłanki z art. 5 ust. 1 lit. e) RODO, w której wyrażona została zasada ograniczenia czasowego. Przejawia się ona w zakazie przechowywania danych w formie umożliwiającej identyfikację podmiotów danych przez dłuższy okres niż jest to niezbędne dla celów, dla których są poddawane procesowi przetwarzania. Administrator powinien określać maksymalny czas przechowywania danych odpowiednio do kategorii i ich podstaw prawnych[688].

Po drugie, osoba, której dane dotyczą, może żądać usunięcia swoich danych po wycofaniu zgody na ich przetwarzanie, jeżeli nie istnieje żadna inna podstawa prawna procesu przetwarzania danych. Analogicznie rzecz biorąc, identycznie, jak w sytuacji ustania

[687] P. Sierzputowski, *Omówienie wyroku Trybunału Sprawiedliwości UE w sprawie C-136/17,* [dostęp: 30.09.2019] https://gdpr.pl/omowienie-wyroku-trybunalu-sprawiedliwosci-ue-w-sprawie-c-136-17.
[688] M. Gawroński, K. Kunda, *RODO. Przewodnik ze wzorami,* red. M. Gawroński, Warszawa 2018, s. 204-205.

celu, dla którego dane zostały zebrane, powinny być usunięte z inicjatywy administratora. Przetwarzanie danych osobowych może się odbywać jedynie w oparciu o jedną z podstaw prawnych przewidzianych przez RODO. Brak takiej podstawy powoduje niemożność dalszego przetwarzania. Praktycznym problemem może okazać się jednak sytuacja, w której powstanie alternatywna przesłanka uprawniająca do przetwarzania danych względem cofniętej zgody. Aby uniknąć wszelkiego rodzaju nieporozumień, do obowiązków administratora danych osobowych, należy dokładne sprawdzanie podstawy prawnej przetwarzania. Często zauważalną pomyłką jest występowanie o zgodę na przetwarzanie danych, kiedy dane osobowe są niezbędne do zawarcia umowy bądź jej wykonania[689]. Wówczas wystarczające jest poinformowanie podmiotu danych o procesie przetwarzania, który dopiero nastąpi. Zgoda na przetwarzanie danych, będzie wymagana często w relacjach z firmami i będzie dotyczyła jakichś danych dodatkowych[690], np. w sytuacji, gdy administrator próbuje sięgnąć po dane, których *de facto* nie potrzebuje, ale z których chętnie skorzysta (przykładem może być zbieranie informacji kontaktowych, m.in. numeru telefonu, jeśli służy to jedynie usprawnieniu komunikacji)[691].

Po trzecie, administrator danych osobowych ma obowiązek ich usunięcia w przypadku skutecznego wniesienia sprzeciwu wobec przetwarzania danych. Jedną z podstaw przetwarzania danych, na których niejednokroć opierają się firmy, jest uzasadniony interes administratora, w tym marketing własnych produktów. Na podstawie przepisów RODO, administrator powinien porównać swój własny interes sprowadzający się m.in. do korzyści wynikających z marketingu ze stopniem naruszenia praw i wolności podmiotów danych, przykładowo sprawdzając, czy nie wkracza nadmiernie w prywatność swoich klientów, śledząc ich lokalizację. Kolejną z podstaw jest dokonanie oceny czy sytuacja, w jakiej znajduje się wnioskodawca ma charakter odbiegający od tych standardowych. To właśnie w takich przypadkach, przysługuje prawo wniesienia sprzeciwu, a zatem zaznaczenia, że osoba, której dane dotyczą, nie wyraża zgody na wykorzystywanie jej danych w tak pojętym interesie administratora, a ponadto posiada uprawnienie do żądania usunięcia profilu marketingowego[692].

---

[689] *Tamże,* s. 205.
[690] K. Szymielewicz, *RODO na tacy. Odcinek IV: O prawie do bycia zapomnianym (sic!) i zabrania danych ze sobą,* [dostęp: 11.04.2018] https://panoptykon.org/wiadomosc/rodo-na-tacy-odcinek-iv-o-prawie-do-bycia-zapomnianym-sic-i-zabrania-danych-ze-soba.
[691] K. Szymielewicz, *RODO na tacy. Odcinek II: Fair play-czyli o szacunku dla naszych wyborów,* [dostęp: 16.02.2018] https://panoptykon.org/wiadomosc/rodo-na-tacy-odcinek-ii-fair-play-czyli-o-szacunku-dla-naszych-wyborow.
[692] K. Szymielewicz, *RODO na tacy. Odcinek IV: O prawie do bycia zapomnianym (sic!) i zabrania danych ze sobą…*

Po czwarte, przetwarzanie danych osobowych zgodnie z prawem jest naczelną zasadą przetwarzania danych. Brak dostosowania tego procesu do wymagań stawianych przez RODO niesie ze sobą ryzyko poważnych konsekwencji, w szczególności finansowych, które mogą wystąpić po stronie administratora danych osobowych. Stąd też, aby uniknąć tych niedogodności, na administratora został nałożony obowiązek tworzenia takich warunków, aby na ich podstawie przetwarzanie danych odbywało się zawsze zgodnie z prawem. Ciężar udowodnienia przetwarzania danych osobowych zgodnie z zasadą legalności spoczywa na administratorze. W związku z tym, procesy rządzące przetwarzaniem danych powinny być na tyle jasne i przejrzyste, aby istniała możliwość w miarę prostego i szybkiego wykazania prawidłowości przetwarzania danych. Administrator w każdej sytuacji powinien być na to gotowy, a przetwarzanie danych powinno być przez niego stale monitorowane, aby niezwłocznie wychwycić wszelkie pojawiające się nieprawidłowości. Prawo się zmienia, a wraz z nim podstawy przetwarzania danych. To, co było legalne, może okazać się problemem. Często zdarza się, że administrator danych osobowych korzysta z danych, których w ogóle nie powinien przetwarzać, powołując się na argument, że konkretnych informacji nie można zaliczyć do kategorii danych osobowych, ponieważ nie zawierają imienia i nazwiska podmiotu danych. W praktyce takie sytuacje mają miejsce w celach marketingowych. Wówczas można zażądać usunięcia bezprawnie przetwarzanych danych, ale też wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych, ewentualnie od razu wprost do sądu[693].

Po piąte, z żądaniem usunięcia danych można wystąpić również w sytuacji, gdy na administratorze ciąży taki obowiązek wynikający bezpośrednio z prawa Unii Europejskiej lub prawa krajowego. Obowiązek powinien zostać wskazany *expressis verbis* w prawie unijnym lub krajowym.

Po szóste, jednym z zamierzeń RODO jest umożliwienie usuwania z Internetu informacji umieszczanych tam przez dzieci. To żądanie otwiera drogę do naprawy podjętych decyzji w okresie dzieciństwa. Unijne Rozporządzenie stawia restrykcyjne wymagania, jeżeli ma się na uwadze przetwarzanie danych osobowych dzieci w obszarze korzystania z usług społeczeństwa informacyjnego. W oparciu o treść motywu 65 Ogólnego Rozporządzenia o Ochronie Danych Osobowych, osoba, której dane dotyczą, ma prawo do żądania usunięcia swoich danych, które udostępniła jako dziecko, w każdym czasie, nawet jeśli dzieckiem już nie jest. Zgodnie z przepisami RODO, dzieciom, które ukończyły 16 lat, przysługuje

[693] O tym będzie szerzej w Rozdziale IV niniejszej rozprawy doktorskiej.

uprawnienie do decydowania o przekazywaniu informacji na temat ich osoby firmom internetowym. Prawodawca, jak daje się zauważyć, wyszedł z założenia, że należy im się szczególna ochrona, ponieważ mogą nie być świadome konsekwencji podejmowanych przez siebie kroków.

Efektywne usuwanie danych nie należy do prostych czynności, w szczególności, jeśli mowa jest o usuwaniu ich z publicznego serwera. W tej sytuacji dostęp do tego ma nieograniczona liczba osób, co powoduje kolejne trudności. Zwykle dochodzi do tzw. nadpisania danych. Jeśli zatem, dane osobowe zostały opublikowane w sieci internetowej, administrator nie ma tak naprawdę żadnej kontroli nad utworzeniem ich kopii. Wówczas niewiele można zrobić. Wnioskując do konkretnej instytucji o usunięcie danych, które wcześniej zostały przez nią upowszechnione, powinna ona podjąć rozsądne działania, mające na celu poinformowanie innych administratorów przetwarzających nasze dane o zgłoszonym żądaniu[694].

Unijne Rozporządzenie, oprócz instytucji usunięcia danych osobowych, przyznaje prawo przeniesienia danych pod dwoma warunkami, a mianowicie, jeśli są przetwarzane w sposób zautomatyzowany oraz zostały dostarczone przez sam podmiot danych albo z własnej inicjatywy na podstawie udzielonej zgody lub w oparciu o treść realizowanej umowy. To oznacza, że nie można wymagać pomocy w przeniesieniu danych, jeżeli konkretna instytucja trzyma je w bazie danych w formie papierowej lub jeżeli są to dane, które nie zostały jej dostarczone przez podmiot danych. Drugi z warunków może nastręczać wiele wątpliwości[695], które próbowała rozwiać Grupa Robocza Art. 29[696]. Podjęto się próby zdefiniowania tej frazy. Należy ją interpretować w znaczeniu *sensu largo*. Zatem chodzi nie tylko o te dane, jakie podmiot danych świadomie podał, tj. imię i nazwisko, adres e-mail i inne, ale także o te, które wygenerowała sama jego aktywność w ramach danej usługi[697]. Skorzystanie z prawa do przenoszenia danych przez użytkownika nie powoduje ograniczenia jego uprawnień względem administratora danych. Nie oznacza też usunięcia danych czy

[694] Chodzi o usunięcie wszelkich linków i kopii, jakie mogą pozostać w Internecie. W praktyce oznacza to jedynie tyle, że zostaje zrealizowana powinność poinformowania o zgłoszonym przez podmiot danych żądaniu usunięcia informacji go dotyczących. Podejmowanie rozsądnych działań nie oznacza jednak pochylania się nad poszukiwaniem prywatnych kopii czy archiwalnych stron.

[695] Pojawia się pytanie, czy chodzi tylko o te dane, które podmiot danych samodzielnie wpisuje do formularza internetowego, czy także o te, które są związane np. z historią transakcji bankowych, czy z zakupami on-line przez Internet. W tych sytuacjach przecież dane osobowe nie są własnoręcznie dostarczane, ale generowane aktywnością osoby, której dane bezpośrednio dotyczą.

[696] Instytucja, która skupia europejskie organy ochrony danych osobowych.

[697] Zgodnie z tą wykładnią, można przenieść dane obejmujące wpisy na portalu społecznościowym, historię wyszukiwania, czy dokonane transakcje płatnicze. Nie można tego uczynić wobec danych wygenerowanych przez samego administratora, czyli w stosunku do danych pochodnych, które można ustalić dzięki profilowaniu i analizie statystycznej (np. wiarygodność kredytowa, zainteresowania, stan konta).

zakończenia świadczenia usługi[698].

3.4. Ograniczenia w stosowaniu „prawa do bycia zapomnianym”

3.4.1. Przesłanki wyłączające korzystanie z „prawa do bycia zapomnianym”

„Prawo do bycia zapomnianym” nie ma charakteru absolutnego. Unijne Rozporządzenie przewiduje w art. 17 ust. 3 RODO wiele wyjątków, które uprawniają do odstąpienia przez administratora danych osobowych od realizacji „prawa do bycia zapomnianym”.

Nie jest wymagane usuwanie danych w zakresie, w jakim przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji[699]. Można zaobserwować kolizję pomiędzy prawami jednostki dotyczącymi jej danych a wolnością wypowiedzi i informacji, która także zaliczana jest do jednych z najbardziej fundamentalnych wolności zawartych w Karcie Praw Podstawowych. Wolność wypowiedzi i informacji zawiera w sobie prawo do otrzymywania i przekazywania informacji. Przy powoływaniu się na ten wyjątek, należy rozważyć, w jaki sposób te wartości na siebie rzutują. Wskazówką może być wspomniany już wyrok Google Spain (C-131/12)[700], w którym TSUE podniósł, że usunięcie linków do pewnych informacji może wywołać kolizję z interesem internautów, podejmujących próby uzyskania dostępu do danej kategorii informacji, a ich interes może być wzmocniony poprzez pełnienie szczególnej roli w życiu publicznym przez osobę, której dane dotyczą. Odmawiając usunięcia danych w oparciu o ten wyjątek, administrator danych osobowych powinien nie tylko skonfrontować przeciwstawne interesy, lecz także szczegółowo uzasadnić swoje zdanie. Ważąc prawa i wolności osób, których dane dotyczą oraz interesy internautów w dostępie do informacji za pomocą dostawców wyszukiwarek internetowych, TSUE stanął na stanowisku, że co do zasady prawa podmiotu danych są nadrzędne w porównaniu z interesami internautów, to jednak równowaga ta może w uzasadnionych przypadkach zależeć od charakteru rozpatrywanych informacji i od tego, jak znaczące są one dla prywatności osoby, której dane dotyczą oraz dla interesu publicznego w korzystaniu z tej informacji, który to z kolei interes może być uzależniony od roli

[698] Grupa Robocza Art. 29, *Wytyczne w zakresie prawa do przenoszenia danych,* przyjęte w dniu 13 grudnia 2016 r., WP 242, s. 6.
[699] Dziennikarstwo trzeba interpretować szeroko, zalicza się do niego także blogi internetowe.
[700] „Prawo do bycia zapomnianym” nie przysługuje sprawcom ataków terrorystycznych, czy afer politycznych.

odgrywanej przez tę osobę w życiu publicznym[701].

Dokonana przez TSUE analiza usuwania z listy wyników wyszukiwania prowadzi do wniosku, że przy ocenie żądań usunięcia z listy wyników wyszukiwania, trzeba uwzględnić w decyzji o utrzymaniu lub zablokowaniu wyników wyszukiwania przez dostawcę wyszukiwarki internetowej to, jaki byłby wpływ decyzji na dostęp dla internautów do informacji[702]. Istnienie takiego wpływu nie musi od razu pociągać za sobą odrzucenia żądania usunięcia z listy wyników wyszukiwania. Jak potwierdził Trybunał Sprawiedliwości Unii Europejskiej, taka ingerencja w fundamentalne prawa podmiotu danych, powinna być umotywowana nadrzędnym interesem szerokiego kręgu odbiorców polegającym na posiadaniu dostępu do konkretnej informacji.

Trybunał dokonał również rozróżnienia pomiędzy legitymacją wydawcy strony internetowej do rozpowszechniania informacji a legitymacją dostawcy wyszukiwarki internetowej. Stwierdził, że wydawca strony internetowej może prowadzić swoją działalność tylko w celach dziennikarskich, gdzie mógłby korzystać z wyłączeń, które kraje członkowskie mogą ustanowić w takich przypadkach na podstawie art. 9 Dyrektywy (art. 85 ust. 2 RODO). Europejski Trybunał Praw Człowieka wskazał, że wyważenie wchodzących w grę interesów może prowadzić do różnych konkluzji, w zależności od złożonej treści wniosku (wobec podmiotu, który pierwotnie opublikował informację, wobec wyszukiwarki, której głównym interesem nie jest publikacja pierwotnych informacji o osobie, ale ułatwianie identyfikacji wszystkich dostępnych informacji na temat podmiotu danych i stworzenie jego profilu)[703].

Trybunał Sprawiedliwości UE wyjaśnił, że art. 17 ust. 3 lit. a) RODO stanowi wyraz tego, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym. Należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych zgodnie z zasadą proporcjonalności[704]. Wyraźnie ustanowiono wymóg zapewnienia równowagi pomiędzy prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych ustanowionymi w art. 7 i 8 KPP a prawem do wolności informacji określonym w art. 11 KPP[705]. Podsumowując, zależnie od okoliczności sprawy, dostawcy wyszukiwarek internetowych uprawnieni są do odmowy usunięcia treści z listy wyników wyszukiwania, gdy są w stanie udowodnić, że pozostawienie ich w wynikach

[701] Wyrok TSUE z dnia 24 września 2019 r., sygn. akt: C-136/17…, pkt 66.
[702] *Tamże,* pkt 56.
[703] K. Warecka, *Strasburg: „prawo do bycia zapomnianym" musi być w równowadze z prawem do informacji. M.L. i W.W. przeciwko Niemcom-wyrok ETPCz z dnia 28 czerwca 2018 r., połączone skargi nr 60798/10 i 65599/10,* [dostęp: 02.07.2018] https://www.prawo.pl/.
[704] Wyrok TSUE z dnia 24 września 2019 r., sygn. akt: C-136/17…, pkt 57.
[705] *Tamże,* pkt 59.

wyszukiwania jest absolutnie konieczne do ochrony prawa internautów do wolności informacji.

Wyrok Naczelnego Sądu Administracyjnego, który został wydany w dniu 9 lutego 2023 roku, a odnoszący się do „prawa do bycia zapomnianym" jest niebezpieczny dla wolności wypowiedzi[706]. Sprawa zaczęła się od odmowy wszczęcia postępowania przez Prezesa Urzędu Ochrony Danych Osobowych. Skarżący domagał się usunięcia danych osobowych z materiału prasowego sprzed kilkunastu lat. Organ stwierdził, że dane te były przetwarzane w ramach działalności dziennikarskiej i nie stosuje się do nich przepisów unijnego Rozporządzenia, w tym art. 17. Sprawa została skierowana do Wojewódzkiego Sądu Administracyjnego w Warszawie, którego zdaniem prawo prasowe choć nie zakreśla czasowej granicy dostępności materiałów prasowych na stronach internetowych wydawcy, to jednak „prawo do bycia zapomnianym" zakłada obowiązek usunięcia danych, gdy ich przetwarzanie nie jest już potrzebne do korzystania z prawa do wolności wypowiedzi, stąd też Urząd Ochrony Danych Osobowych powinien w każdym przypadku oceniać, czy taka konieczność występuje, czy też nie. W reakcji na to orzeczenie, Prezes wniósł skargę kasacyjną do NSA, który przychylił się do stanowiska wyrażonego przez Wojewódzki Sąd Administracyjny.

Naczelny Sąd Administracyjny w składzie sędziego sprawozdawcy Rafała Stasikowskiego uznał, że rozwiązania prawne zawarte w art. 14 (wolność mediów), art. 51 (prawo ochrony danych osobowych) i art. 54 (wolność słowa) Konstytucji RP oraz w art. 85 RODO (przetwarzanie a wolność wypowiedzi i informacji) nakazują przyjąć, że pierwszeństwo wolności prasy nad ochroną prawa do prywatności możliwe jest tylko do chwili, gdy są realizowane cele działalności prasowej, a zatem do momentu, gdy materiał prasowy służy urzeczywistnianiu prawa obywateli do ich rzetelnego informowania, jawności życia publicznego oraz kontroli i krytyki społecznej, czyli do chwili, gdy konkretna informacja zawarta w materiale prasowym posiada przymiot aktualności.

Ponadto, sąd podzielił pogląd, że udostępnianie przez wydawcę publikacji archiwalnej przechowywanej na stronie internetowej nie stanowi działalności prasowej w rozumieniu prawa prasowego, gdyż ta polega na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów. Udostępnianie materiałów prasowych w sieci Internet, tworzących bazę danych osobowych, nie należy do wymienionych wprost ustawowo zadań prasy. Zdaniem Naczelnego Sądu Administracyjnego, materiał opublikowany na stronie wydawcy

[706] Wyrok NSA z dnia 9 lutego 2023 r., sygn. akt: III OSK 6781/21, [dostęp:] https://orzeczenia.nsa.gov.pl/doc/6C317F6401.

utrzymuje aktualność tylko przez pewien czas, zależny od okoliczności. W ocenie sądu, publikacje archiwalne nie są niezbędne do korzystania z wolności wypowiedzi i to prawo zostało już zrealizowane w momencie publikacji. Wobec czego, można zastosować „prawo do bycia zapomnianym".

Wyrok jest groźny dla wolności wypowiedzi, która stanowi jeden z fundamentów demokracji. Odmawia on bowiem archiwom prasowym, po nieustalonym dokładnie przez sąd czasie „aktualności", możliwości objęcia ich wyjątkiem prasowym z ustawy o ochronie danych osobowych. Wyjątek prasowy wyważa w działalności prasy wolność słowa z jednej strony i prawo do ochrony danych osobowych z drugiej. Przepisy Rozporządzenia unijnego przewidują bowiem, że takiego wyważenia dokonuje prawodawca krajowy.

Zasady ochrony danych osobowych nie powinny ingerować w wolność słowa, czy zagrażać funkcjom informacyjnym prasy. W tym celu wprowadzono możliwość korzystania z klauzuli prasowej. Polska klauzula prasowa nie jest jeszcze aż tak restrykcyjna, jak np. w Szwecji, gdzie prawo do ochrony danych osobowych w żaden sposób nie może ograniczyć wolności prasy.

W rozpatrywanej sprawie przez Naczelny Sąd Administracyjny stwierdzono, że internetowe archiwa prasowe nie są objęte tym wyjątkiem, poza aktualnymi materiałami. Przechowywanie danych osobowych w tych archiwach traktuje się, jak każdą inną czynność przetwarzania danych, do której przepisy RODO znajdują swoje zastosowanie. Z tego wynika, że każdy człowiek, którego dane osobowe wymieniono w materiale prasowym, będzie mógł żądać realizacji „prawa do bycia zapomnianym", czyli usunięcia danych z archiwum prasowego. Wydawcy nie będą mogli się powołać na wyjątek prasowy, a co więcej, sąd zabronił w ogóle wskazywać na wolność wypowiedzi, ponieważ jego zdaniem publikacje archiwalne nie są niezbędne do korzystania z tej wolności. Stawia to w niekorzystnej pozycji wydawcę, który w każdym konkretnym przypadku będzie musiał poddać ocenie, czy zaistniały wąsko określone w RODO wyjątki od „prawa do bycia zapomnianym". Gdyby zdecydował się odmówić realizacji prawa, to na nim spoczywa ciężar dowodu. Ten wyrok jest też niebezpieczny w szerszym kontekście, ponieważ wyłącza w odniesieniu do internetowych archiwów wszystkie inne ograniczenia stosowania RODO zawarte w wyjątku prasowym[707].

Skutkiem stanowiska sądu będzie zastosowanie do archiwów art. 5 unijnego

[707] *Wydawcy pod ścianą po wyroku NSA. „Prawo do bycia zapomnianym" działa wstecz,* [dostęp: 02.03.2023] https://www.rp.pl/dane-osobowe/art38050021-wydawcy-pod-sciana-po-wyroku-nsa-prawo-do-bycia-zapomnianym-dziala-wstecz.

Rozporządzenia wprowadzającego zasady przetwarzania danych osobowych, których musi z urzędu przestrzegać każdy administrator danych. Jeśli najnowszy pogląd się utrwali, to wydawca będzie musiał oceniać, czy w archiwalnym tekście prawidłowo zastosowano zasadę celowości, nie czekając na żądania osób, których dane dotyczą[708]. Takie podejście do wolności wypowiedzi w działalności prasowej jest niezgodne ze standardami ustanowionymi przez Europejski Trybunał Praw Człowieka.

Kamieniem milowym jest wyrok Węgrzynowski i Smolczewski przeciwko Polsce z dnia 16 lipca 2013 roku[709]. Trybunał nie pozostawił wątpliwości, że internetowe archiwum prasowe jest objęte prawem do wolności wypowiedzi, chronionym przez art. 10 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności. Co więcej, uznał, że takie archiwa mają ogromne znaczenie dla społeczeństwa. Są ważnym źródłem wiedzy historycznej i edukacji. Odmienne stanowisko mogłoby doprowadzić do przepisywania historii, czyli tworzenia wiedzy o wydarzeniu z przeszłości, bez znajomości wszystkich relacji.

Naczelny Sąd Administracyjny zmierza właśnie w tym kierunku. „Prawo do bycia zapomnianym" w wyroku Naczelnego Sądu Administracyjnego „działa wstecz". Materiały prasowe, które stracą aktualność, będą podlegały nie tylko usunięciu na wniosek osoby, która chce skorzystać z „prawa do bycia zapomnianym", ale być może także z inicjatywy wydawcy, bowiem art. 5 RODO nakazuje po określonym czasie usuwać dane, które nie są już niezbędne do celów, w których były przetwarzane. Usunięcie danych osobowych z materiału oznacza usunięcie części publikacji, po którym tekst może stać się niezrozumiały i niepełny. Naczelny Sąd Administracyjny nie do końca uwzględnił, że prasa pełni istotną funkcję w społeczeństwie. Sprowadza się nie tylko do informowania o różnych wydarzeniach, ale także posiada walor archiwalny. Ta kronika wydarzeń, zdarzeń, historii, sytuacji i osób ma znaczenie nie tylko z aktualnego punktu widzenia. Sięga się też po różne informacje z przeszłości. Usuwanie negatywnych informacji z archiwów prasowych po jakimś czasie doprowadziłoby do sfałszowania przeszłości[710].

Wyrok Europejskiego Trybunału Praw Człowieka zapadł na długo przed wejściem w życie przepisów RODO. Moim zdaniem standardy ochrony danych się nie zmieniły od tamtego czasu, ponieważ wyrok odnosił się do wolności wypowiedzi, a nie bezpośrednio do

[708] K. Żaczkiewicz-Zborska, *NSA: Prawo do zapomnienia obejmuje internetowe archiwa prasowe,* [dostęp: 28.02.2023] https://www.prawo.pl/prawo/prawo-do-zapomnienia-obejmuje-e-archiwa-prasowe,520093.html.

[709] Wyrok ETPCz z dnia 16 lipca 2013 r. w sprawie *Węgrzynowski i Smolczewski przeciwko Polsce,* skarga nr 33846/07,[dostęp:]https://etpcz.ms.gov.pl/etpccontent/$N/990000000000001_I_ETPC_033846_2007_Wy_2013-07-16_001.

[710] *NSA: kasowanie danych osobowych możliwe dla archiwów prasowych. Adam Bodnar: de facto fałszowalibyśmy przeszłość,* [dostęp: 03.03.2023] https://tvn24.pl/polska/nsa-kasowanie-danych-osobowych-mozliwe-dla-archiwow-prasowych-w-internecie-adam-bodnar-de-facto-falszowalibysmy-przeszlosc-st6793664.

przepisów o ochronie danych osobowych. Orzeczenie ma charakter uniwersalny. Jego tłem była sprawa z zakresu dóbr osobistych przed polskimi sądami. Wyrok dotyczył internetowego archiwum „Rzeczpospolitej" i zamieszczonego tam artykułu. Tekst odnosił się do dwóch prawników, którym dziennikarze zarzucili wykorzystanie zajmowanych przez siebie stanowisk ze szkodą dla finansów publicznych. Ostatecznie wygrali oni proces sądowy o naruszenie w publikacji ich dóbr osobistych, ale nie uzasadnia to usunięcia tekstu z archiwum prasowego. W artykule można zamieścić wzmiankę o wyniku procesu cywilnego.

Trybunał zatem opowiedział się za niezmienianiem artykułu zamieszczonego w archiwum, ale za opatrzeniem go sprostowaniem, gdyby się okazało, że zawarte w nim informacje nie są prawdziwe. Stanowi to słuszne podejście, ponieważ artykuł został opublikowany. Stał się punktem odniesienia do kolejnych działań i częścią historii.

Wyrok Naczelnego Sądu Administracyjnego, przyznający prymat prawa do ochrony danych osobowych nad wolnością prasy, zmienia zasady funkcjonowania mediów. Klauzula prasowa miała prowadzić do równowagi pomiędzy ochroną danych osobowych a wolnością wypowiedzi. Sąd jednak przyjął, że do archiwum prasowego stosuje się przepisy o ochronie danych osobowych w pełnym zakresie. Zastosowanie znalazłaby zasada (wyłączona przez klauzulę), że dane osobowe muszą być przechowywane nie dłużej niż jest to niezbędne dla celów ich przetwarzania. Sąd jednak nie określił, czym jest archiwum prasowe i kiedy informacja staje się nieaktualna. Te skumulowane problemy mogą doprowadzić w działaniach wydawców do efektu mrożącego (powstrzymanie się lub zniechęcenie do wykonywania prawnych obowiązków lub realizacji swoich praw z powodu poczucia zagrożenia sankcją lub poniesienia innych konsekwencji prawnych za swoje działanie – terminu tego użył ETPCz).

W ramach drugiego z wyjątków, unijny prawodawca przyznał pierwszeństwo nad prawami jednostki wywiązaniu się z obowiązku prawnego lub zadania, realizowanych w interesie publicznym albo w ramach wykonywania władzy publicznej. Wyjątek ten co do zasady nie znajduje szerokiego zastosowania w sektorze prywatnym, niemniej jednak należy pochylić się nad kwestią wykonywania obowiązku prawnego. Obowiązki prawne w zakresie przetwarzania danych osobowych wynikają głównie z różnych uregulowań, stosownie do rodzaju prowadzonej działalności. Do obowiązków administratora danych osobowych należy zatem znajomość przepisów oraz śledzenie ewentualnych nowelizacji, które mogą spowodować zmiany w procesie przetwarzania danych osobowych[711].

Treść tego wyłączenia sprawia, iż ciężko je zastosować w stosunku do działalności

[711] M. Gawroński, K. Kunda, *RODO. Przewodnik ze wzorami…,* s. 208-209.

dostawców wyszukiwarek internetowych. Trudno wyobrazić sobie przepisy prawa, które nakładałyby na dostawców wyszukiwarek internetowych obowiązek upowszechniania niektórych informacji. Dostawcy wyszukiwarek internetowych nie tworzą ani nie przedstawiają informacji. Zatem, nie jest też prawdopodobne, aby regulacje prawne kraju członkowskiego obligowały do publikowania niektórych rodzajów informacji, w zamian za ustanowienie obowiązku takiej publikacji względem innych stron internetowych, które następnie zostaną powiązane łączem przez dostawcę wyszukiwarki internetowej. Prawo Unii Europejskiej lub państwa członkowskiego umożliwia organowi publicznemu podejmowanie decyzji, które nakładają na dostawców wyszukiwarek internetowych obowiązek bezpośredniego publikowania informacji, nie zaś poprzez adresy URL do strony internetowej zawierające dane informacje. Jeżeli tylko pojawią się takie sytuacje, w których państwo członkowskie ustanawia obowiązek w stosunku do dostawców wyszukiwarek internetowych, w oparciu o który muszą oni publikować decyzje lub dokumenty zawierające dane osobowe, lub na podstawie którego organy publiczne są uprawnione do wymagania takiego publikowania, należy zastosować wyłączenie z art. 17 ust. 3 lit. b) RODO. Zastosowanie takie powinno mieć na uwadze warunki, w jakich jest ustanawiane, a mianowicie to, że przechowywanie informacji jest konieczne do spełnienia prawnego obowiązku publikacji. Odnosi się to do przykładu polegającego na tym, że prawny obowiązek lub decyzja organu uprawnionego do jej przyjęcia może uwzględniać termin publikacji lub cele, których osiągnięcie mogło mieć miejsce w określonym przedziale czasowym. Jeżeli okaże się, że żądanie usunięcia z listy wyników wyszukiwania przekroczyło wyznaczone terminy, to należy uznać, że wyłączenie nie znajduje już dłużej zastosowania. Wręcz przeciwnie, niejednokrotnie zdarza się, że w przepisach państwa członkowskiego przewidziano publikację informacji zawierających w sobie dane osobowe na stronach internetowych. Publikowanie lub przechowywanie opublikowanych informacji nie można zaliczać do odstępstw określonych w art. 17 ust. 3 lit. b) RODO, gdyż obowiązek ten nie jest skierowany do dostawcy wyszukiwarki internetowej, ale do wydawców stron internetowych, których treść jest związana z indeksem dostawcy wyszukiwarki internetowej. Stąd też dostawca wyszukiwarki internetowej nie może powołać się na istnienie obowiązku, by odrzucić żądanie usunięcia z listy wyników wyszukiwania.

Dążąc do równowagi pomiędzy prawami podmiotów danych a interesem osób korzystających z Internetu w dostępie do informacji, warto uwzględnić obowiązek prawny w postaci publikowania skierowany do innych wydawców stron internetowych. Okoliczność, że informacje muszą być publikowane on-line w ramach zalecenia prawnego lub

w następstwie decyzji organu uprawnionego do jej przyjęcia, świadczy o interesie publicznym w dostępie do tych informacji. Takie domniemanie istnienia generalnego interesu publicznego nie ma zastosowania do sieci internetowej, w której zamieszczane są treści, w porównaniu z indeksem rezultatów dostawcy wyszukiwarki internetowej. Choć obowiązek prawny publikowania informacji na danej stronie internetowej może prowadzić do stwierdzenia, że informacji nie należy usuwać z tej strony, to decyzja dotycząca wyników oferowanych przez dostawcę usług wyszukiwania przy przeszukiwaniu źródeł internetowych po wpisaniu imienia i nazwiska może być odmienna[712].

Dostawcy wyszukiwarek internetowych nie zaliczają się do organów publicznych, stąd też nie sprawują samodzielnie uprawnień publicznych. Byłoby to możliwe, gdyby prawo państwa członkowskiego lub prawo Unii Europejskiej przyznawało takie uprawnienia wspomnianym podmiotom (art. 6 ust. 3 RODO). Nie jest raczej możliwe, aby państwa członkowskie przyznały im uprawnienia publiczne albo uznały ich działalność za konieczną do osiągnięcia interesu publicznego ustanowionego zgodnie z przepisami prawa. Jeśli natomiast dojdzie do sytuacji, że prawo państw członkowskich przyzna dostawcom wyszukiwarek internetowych uprawnienia publiczne lub odniesie ich rodzaj działalności do wypełnienia interesu publicznego, to mogą powołać się oni na art. 17 ust. 3 lit. b) RODO. Tak też, potrzebne jest ustalenie czy pozostawienie informacji w wynikach wyszukiwania jest nieodzowne do realizacji interesu publicznego lub do realizowania pełnomocnictwa, by zdecydować o niespełnieniu żądania dotyczącego usunięcia z listy wyników wyszukiwania z powodów związanych z tym wyłączeniem.

Na wyjątek interesu publicznego w ochronie zdrowia publicznego powołuje się administrator danych osobowych, który przetwarza dane potrzebne do zadań profilaktyki zdrowotnej lub medycyny pracy, do oceny predyspozycji pracownika do pracy, diagnozy medycznej, zagwarantowania opieki zdrowotnej albo zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa UE lub prawa kraju członkowskiego, a także w zgodzie z treścią umowy z pracownikiem służby zdrowia, pod warunkiem, że te dane przetwarza osoba, na którą został nałożony obowiązek przestrzegania tajemnicy zawodowej (lekarskiej, pielęgniarskiej).

Ponadto, administrator danych osobowych ma prawo odmówić usunięcia danych, jeśli

[712] Przy dokonywaniu oceny żądania usunięcia z listy wyników wyszukiwania nie należy zakładać, że istnienie obowiązku prawnego publikacji sugeruje, że w kwestii, w jakiej obowiązek ten nałożony jest na pierwotnych wydawców strony internetowej, nie jest prawdopodobne, aby dostawca wyszukiwarki internetowej wyraził aprobatę dla usunięcia z listy wyników wyszukiwania. Co do zasady, decyzję taką należy podejmować wyważając prawa osoby, której dane dotyczą z interesem internautów w dostępie do tych informacji poprzez dostawcę wyszukiwarki internetowej.

ich przetwarzanie jest niezbędne ze względów odnoszących się do interesu publicznego w dziedzinie zdrowia publicznego, tj. objęcie ochroną przed transgranicznymi zagrożeniami zdrowotnymi bądź zapewnienie odpowiednich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów o działaniu leczniczym lub wyrobów medycznych.

Wyjątku tego nie powinno zaliczać się do wyjątków uogólnionych, a jedynie do wyjątków „branżowych", z danej kategorii, znajdujących swe zastosowanie w sektorze medycznym oraz farmaceutycznym. Skorzystanie z uprawnienia do jego zastosowania ograniczone jest faktem istnienia interesu publicznego przy przetwarzaniu danych[713].

Wyłączenie to stanowi szczególny przypadek potwierdzający okoliczność, że przetwarzanie jest konieczne dla realizacji interesu publicznego. W tym przypadku interes publiczny ogranicza się do obszaru zdrowia publicznego, lecz podstawy przetwarzania analogicznie powinny być ustanowione w prawie Unii Europejskiej lub w prawie państwa członkowskiego. Z punktu widzenia stosowania tego wyłączenia, w kontekście działalności dostawcy wyszukiwarki internetowej, wysuwają się podobne wnioski do tych przedstawionych powyżej. Nie wydaje się możliwe, aby prawo państwa członkowskiego bądź prawo Unii Europejskiej mogło ustalać stosunek pomiędzy działalnością dostawcy wyszukiwarki internetowej a przechowywaniem informacji w wynikach wyszukiwania, realizując przy tym cele interesu publicznego w dziedzinie zdrowia publicznego[714].

Proces przetwarzania danych może odbywać się w celach archiwalnych, statystycznych, historycznych oraz badań naukowych, jeśli spełnia warunki przewidziane przez art. 89 ust. 1 RODO. Inaczej mówiąc, przetwarzanie danych podlega stosownym zabezpieczeniom praw i wolności osoby, której dotyczą. Charakteryzują się wdrożeniem odpowiednich środków technicznych i organizacyjnych, których zadaniem jest poszanowanie zasady minimalizacji lub pseudonimizacji danych[715]. Dostawca wyszukiwarki internetowej powinien być w stanie wykazać, że usunięcie pewnych treści z wyników wyszukiwania jest poważną przeszkodą dla osiągnięcia celów badań naukowych lub historycznych lub celów statystycznych, bądź w zupełności to uniemożliwi. Cele te muszą być realizowane przez

[713] Wyjątek zdrowia publicznego częstokroć nadużywany jest na terenie Rzeczypospolitej Polskiej, dlatego wyraża się nadzieję, że organ nadzorczy będzie odważnie bronił prywatności jednostki przed nieuzasadnioną nadmierną ingerencją w jej sferę.

[714] Konkluzja ta jest jeszcze bardziej oczywista z tego względu, że skutkiem usunięcia z listy wyników wyszukiwania jest sytuacja, w której niektóre wyniki są usunięte z wyników wyszukiwania otrzymanych po wpisaniu w kryteria wyszukiwania imienia i nazwiska (informacje te nie są kasowane z indeksów dostawców wyszukiwarek internetowych, więc istnieje możliwość ich pobrania, stosując inne terminy wyszukiwania).

[715] Z brzmienia treści tego przepisu wynika, że administrator danych osobowych może powołać się na ten wyjątek, jeśli przetwarzanie jest zgodne z przesłankami określonymi w art. 89 Rozporządzenia unijnego, a jednocześnie realizacja „prawa do bycia zapomnianym" uniemożliwi lub poważnie utrudni wykonanie celów takiego przetwarzania.

dostawcę wyszukiwarki internetowej w obiektywny sposób[716]. To, że usunięcie wyników mogłoby znacznie wpłynąć na cele badań naukowych lub cele statystyczne realizowane przez użytkowników usługi dostawcy wyszukiwarki internetowej nie ma znaczenia w kontekście stosowania tego odstępstwa.

Środki, przy pomocy których można spełnić wymagania art. 89 RODO, koncentrują się przede wszystkim na zabezpieczeniu systemów IT, w których znajdują się przetwarzane dane, autoryzowaniu dostępu dla osób przeprowadzających badania, a także zawieraniu umów w przedmiocie zachowania poufności z podmiotami biorącymi udział w procesie przetwarzania danych. Skorzystanie natomiast z odpowiednich środków powinno zależeć od rodzaju prowadzonych działań[717].

Ostatnim wyjątkiem jest ustalenie, dochodzenie i obrona roszczeń. Generalnie znajdzie on swoje zastosowanie wówczas, gdy pomiędzy administratorem a podmiotem danych pozostaną nieuregulowane należności lub toczy się inne sporne postępowanie. Ściślej rzecz ujmując, wskazany wyjątek uprawnia administratora do dochodzenia swoich roszczeń do czasu zakończenia egzekwowania zobowiązania ciążącego na podmiocie danych względem administratora[718].

3.4.2. Problemy wynikające z realizacji „prawa do bycia zapomnianym" – kopie zapasowe i archiwalne oraz dane nieustrukturyzowane

Po wejściu w życie przepisów RODO, praktyczne wdrożenie unijnych regulacji dotyka wielu sfer funkcjonowania firmy, w tym przede wszystkim w obszarze IT. Za przykład posłużyć może aplikacja na telefon, przy pomocy której można rezerwować wizyty w zakładach fryzjerskich czy kosmetycznych. Właściciel aplikacji staje się jednocześnie właścicielem danych osobowych osób zakładających konto w aplikacji dla określonego celu. Właściciel aplikacji, będący administratorem danych osobowych, musi być w ciągłej gotowości w razie, gdyby użytkownik aplikacji zgłosił choćby jedno z przysługujących mu

[716] Bez obowiązku powstania zależności pomiędzy imieniem i nazwiskiem osoby, której dane dotyczą a wynikami wyszukiwania.
[717] Np. jeśli dane służą celom statystycznym, które będą odnosić się jedynie do tendencji obecnych w danej grupie osób bez ujawniania ich tożsamości, to administrator danych osobowych winien zagwarantować takie środki, aby tożsamość osób poddanych badaniu pozostała nadal nieznana.
[718] Podstawa ta powinna być wyjątkiem, a nie usprawiedliwieniem dla nieograniczonego przechowywania danych. Rozporządzenie o Ochronie Danych Osobowych w motywie nr 64 wskazuje na niedopuszczalność archiwizowania danych osobowych jedynie w celu odpowiedzi na ewentualne wnioski podmiotów danych, a w praktyce właśnie ten powód podawany jest przez wielu przedsiębiorców jako podstawa gromadzenia danych przez okres przedawnienia roszczeń.

praw. Podczas wykonywania praw przez użytkownika aplikacji może dochodzić do zbiegu dwóch różnych interesów, tj. podmiotu danych oraz administratora. Użytkownik aplikacji posiada pełne prawo zgłoszenia żądania usunięcia danych osobowych w oparciu o art. 17 RODO w sytuacji, gdy właściciel aplikacji tworzył i przechowywał kopie zapasowe aplikacji, w których znajdują się informacje na temat podmiotu danych[719]. Podejmowane przez administratorów działania są częstym środkiem technicznym służącym do zagwarantowania stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych. Przyjęło się, że kopie zapasowe powinny być przechowywane do czasu, kiedy istnieje podstawa prawna ich przetwarzania. W przeciwnym razie, dane osobowe z kopii zapasowej muszą być usunięte lub zanonimizowane.

Na administratorze danych osobowych ciąży obowiązek zagwarantowania dostępności danych i odporności systemów oraz usług nawiązujących do przetwarzania danych, umiejętność szybkiego przywracania i dostępu do danych, a ponadto zapewnienie integralności kopii zapasowej.

Organy nadzorcze wyraziły pogląd, że informacje należy usuwać ze wszystkich źródeł, na których się znajdują, zatem także z kopii zapasowych i archiwalnych[720]. W wydanym przez Ministerstwo Cyfryzacji informatorze o tematyce nawiązującej do RODO[721] jest polecenie, aby usuwać dane z kopii zapasowych i logo, jeśli nie ma innej możliwości, to poprzez ręczne odmrożenie kopii zapasowej, następnie likwidację danych, a kolejno ponowne zamrożenie kopii[722]. Trudno być zwolennikiem tego podejścia w sytuacji, kiedy kopie zapasowe są wykonywane na taśmach magnetycznych. Inaczej jest, gdy dyski są dostępne on-line.

Usuwanie lub modyfikacja pojedynczych danych z kopii zapasowej pozbawia kopię integralności. Może doprowadzić do sytuacji, w której będzie utrudnione, bądź całkowicie uniemożliwione jej następcze odtworzenie. Z tym z kolei wiąże się wysokie

[719] Kopie zapasowe są bazami danych, które pozwalają na odtworzenie danych w nich zapisanych, gdy dane zostaną utracone lub uszkodzone. Kopię zapasową można wykonać nie tylko z danych zgromadzonych w aplikacji, lecz także z informacji zapisanych na dysku, serwerze, stacji, w systemie teleinformatycznym czy operacyjnym. Zob. O. Jaworowska, *Dane osobowe w kopiach zapasowych,* [dostęp: 03.12.2018] https://www.isecure.pl/blog/dane-osobowe-w-kopiach-zapasowych/.

[720] Wyrok NSA z dnia 3 lipca 2009 r., sygn. akt: I OSK 633/08, [dostęp:] https://www.inforlex.pl/dok/tresc%2CNSA.2009.001.300207296%2CWyrok-NSA-z-dnia-3-lipca-2009-r-sygn-I-OSK-633-08.html?utm_source=chatgpt.com.

[721] Ministerstwo Cyfryzacji, *RODO-informator,* [dostęp: 12.01.2018] https://www.gov.pl/cyfryzacja/rodo-informator.

[722] „Dane osobowe muszą być także usuwane ze wszystkich kopii zapasowych oraz logów. Jeżeli usuwanie z kopii zapasowych pojedynczych rekordów grozi naruszeniem integralności pozostałych gromadzonych danych, to administrator może manualnie przywracać kopie do bazy głównej, a następnie usuwać z nich pojedyncze rekordy i backupować bazy zmniejszone o ten rekord, choć jest to dość czasochłonny proces". Zob. *Tamże.*

prawdopodobieństwo niebezpieczeństwa dla integralności i dostępności wszelkich danych osobowych zapisanych na tej kopii. Zachodzi zatem kolizja pomiędzy usuwaniem danych z kopii zapasowych a zasadą bezpieczeństwa danych. Ingerowanie w kopie zapasowe powoduje także problem z rozliczalnością, utrudnia lub uniemożliwia wykorzystanie kopii jako dowodu i daje możliwość do nadużyć.

Koncepcja przepisywania kopii zapasowych może tworzyć problem natury organizacyjnej. Ingerowanie w kopie zapasowe wydaje się skomplikowanym działaniem z perspektywy zasobów i procesu tworzenia kopii zapasowych. Ilość obowiązków nakładanych przez RODO zachęca do korzystania z centralizacji przetwarzania danych osobowych, to zaś powoduje zwiększenie zagrożenia dla prywatności. Usuwanie danych da się jednak pogodzić z bezpieczeństwem informacji przy zachowaniu pewnych warunków:
- co do zasady, obowiązek usunięcia danych jest ograniczony występowaniem innej podstawy przetwarzania (obowiązek usunięcia nielegalnie przetwarzanych danych nie jest równoznaczny z niszczeniem dowodów);
- objęcie ochroną danych osobowych jest dobrą podstawą przetwarzania informacji;
- dane powinny zostać usunięte z systemów służących prowadzeniu działalności;
- jeżeli usuwanie informacji z kopii zapasowych groziłoby bezpieczeństwu danych, należałoby zastanowić się nad stworzeniem procedury wymuszającej ponowne dokonanie usunięcia danych z systemów produkcyjnych w razie przywrócenia danych w oparciu o kopię zapasową[723].

Procedurę usuwania danych wypada zacząć od ich inwentaryzacji. Na ten proces składa się określenie, jakie informacje są przetwarzane, gdzie i w jakiej formie są przechowywane, oraz czy upłynął termin ich ważności. Do tego celu może posłużyć tabela retencji, w której określa się rodzaj przechowywanych danych, ich lokalizację oraz termin ważności regulowany przez przepisy szczegółowe lub wyznaczany indywidualnie. Przy tak wdrożonym systemie, procedura usunięcia danych z systemu informatycznego nie powinna powodować większych problemów. Kłopot może pojawić się w momencie, kiedy właśnie podmiot danych zażąda, aby wymazać informacje go dotyczące także z kopii zapasowych. Z praktycznego punktu widzenia rozróżnia się dwa rodzaje kopii, tj. backup i archiwum. Administrator danych osobowych może bez większych komplikacji nadpisać, inaczej mówiąc – usunąć dane z backupu, który zazwyczaj przechowywany jest przez 72 godziny. Archiwum z kolei zaliczane jest do integralnej części systemu i nie powinno się usuwać z niego

[723] W tym celu powinno utrzymywać się odpowiedni rejestr wyjątków obejmujący dane podlegające usunięciu lub sprostowaniu.

pojedynczych danych, ponieważ zaburzyłoby to działanie całego systemu. Na archiwum składają się wszystkie informacje, które przechowywane są dłużej niż 3 miesiące[724].

Bez wątpienia istnieją informatyczno-techniczne możliwości ponownego usuwania danych bez znajomości treści informacji podlegających usunięciu. Rekord, który ma zostać skasowany, może być odznaczony rzadko spotykanym identyfikatorem. Wówczas, dokonując pierwotnego usunięcia, wystarczające jest zapisanie identyfikatora rekordu na liście wyjątków, a w sytuacji przywrócenia kopii zapasowej, usunąć bądź nadpisać zidentyfikowany rekord wstępnie określoną zawartością zastępczą[725]. Jeżeli system nie oznacza rekordu unikatowym identyfikatorem, można skorzystać z innej metody identyfikacji zakazanej treści (np. z sumy kontrolnej)[726].

Pod względem praktycznym, usuwanie danych na podstawie żądania zgłoszonego administratorowi, stanowi czasami problem. Do takiego wniosku prowadzi sytuacja, że informacje najpierw trzeba wyszukać, zarówno w systemach informatycznych, jak i tradycyjnych, co nierzadko sprowadza się do manualnego przeglądania dokumentów. Twórcy systemów informatycznych tworzą możliwość szybkiego wyszukiwania i usuwania danych dotyczących jednej konkretnej osoby. Wraz z wejściem w życie unijnego Rozporządzenia, funkcja ta została wprowadzona w wielu narzędziach, w których dotychczas jej nie było, natomiast wersje papierowe zostały uporządkowane. Pozostał jeszcze jeden problem faktycznego usunięcia danych, w szczególności biorąc pod uwagę instytucję tworzenia i przechowywania kopii zapasowych. Żaden przepis nie wskazuje bezpośrednio, że dane z kopii zapasowej można zachować, więc dotychczas przeważało stanowisko, że dane należy usunąć zewsząd, w tym z kopii zapasowych. Sprowadzało się to do tego, że wszystkie kopie zapasowe trzeba było przeszukiwać osobno, a dalej usunąć rekordy odnoszące się do podmiotu danych[727].

Na stronie Ministerstwa Cyfryzacji opublikowano przewodnik RODO dla sektora

[724] P. Jagielska, *RODO: Jak usunąć dane osobowe z systemu informatycznego?,* [dostęp: 13.05.2018] https://biznes.gazetaprawna.pl/artykuly/1122751,rodo-usuwanie-danych-osobowych-z-systemu-informatycznego.html.

[725] Pomocne może okazać się zastosowanie tzw. klucza złożonego. Na klucz może składać się ID systemowe oraz numer PESEL klienta. Dzięki temu rozwiązaniu możliwe jest zidentyfikowanie danych w kopii zapasowej, tak aby z kolei na przywróconej kopii dokonać ich automatycznego usunięcia.

[726] Liczba uzyskana według specjalnego algorytmu służąca do zagwarantowania integralności danych, [dostęp: 14.04.2021] https://pl.wikipedia.org/wiki/Suma_kontrolna.

[727] O ile dane były przechowywane w ramach pamięci flash, to takie usuwanie było czasochłonne. Jeśli były przechowywane zaś na płycie CD/DVD to było to jeszcze bardziej problematyczne. Konieczne było wówczas sprawdzenie zawartości niemal każdej płyty, skopiowanie tego, co się na niej znajdowało, usunięcie rekordów (zestawu danych), utworzenie nowego zapisu na innym nośniku bez usuniętych danych, a następnie zniszczenie uprzedniego starego nośnika. Zob. M. Nosowski, *Czy usunięcie danych dotyczy też kopii zapasowych?,* [dostęp: 05.12.2018] https://www.wsroddanych.pl/post/2018/12/05/czy-usuni%C4%99cie-danych-dotyczy-te%C5%BC-kopii-zapasowych.

fintech[728], z treści którego wynika, że obowiązek usunięcia danych z kopii zapasowych co do zasady istnieje, ale nie jest jednak bezwzględny[729]. Oznacza to, że jeżeli ktoś zażąda usunięcia danych, to w ramach kopii zapasowej mogą być na niej przechowywane. Nie powinny być natomiast przetwarzane w jakimkolwiek innym celu. Innymi słowy, należy ją usunąć wraz ze wszystkimi danymi zapisanymi na kopii, gdy stanie się zbędna. Stanowisko to wychodzi naprzeciw potrzebom sygnalizowanym przez administratorów danych.

„Prawo do bycia zapomnianym" powoduje jeszcze jeden problem interpretacyjny, ujawniony na tle wspomnianego stanowiska Ministerstwa Cyfryzacji, a mianowicie „administrator musi zapewnić odpowiednie techniczne i organizacyjne środki pozwalające na całkowite usunięcie danych osoby, która korzysta z „prawa do bycia zapomnianym". Należy usunąć dane ze wszystkich miejsc, czyli m.in. serwera, poczty, plików Word i Excel, dysków zewnętrznych i przenośnych, ale również z papierowych kopii. Samo przechowywanie przez administratora danych nadal kwalifikowane jest jako przetwarzanie danych osobowych"[730]. Ministerstwo Cyfryzacji wskazuje na potrzebę usuwania danych osobowych konkretnych jednostek również z zasobów, których treści można realnie nie znać, tzn. z zasobów zawierających dane nieustrukturyzowane[731]. Jednak na podstawie art. 11 RODO, nie jest konieczne realizowanie praw jednostki w stosunku do takich zasobów do czasu aż osoba, której dane dotyczą się zidentyfikuje.

W praktyce pojawiają się nurtujące pytania, na które trzeba znaleźć odpowiedź. Niejednokroć sprowadzają się one do tego, czy w następstwie otrzymania od podmiotu danych żądania usunięcia informacji, należy przeszukać wszystkie zasoby, przejrzeć e-maile i dokumenty, aby określić miejsca, na jakich się znajdują, i z których następnie trzeba będzie je usunąć. Póki co nie ma na to jednolitej odpowiedzi. Dosłowna wykładnia unijnego Rozporządzenia wskazywałaby na powinność wymazania informacji odnoszących się do

[728] Poradnik ten nie jest objaśnieniem ogólnych zagadnień, a poprzez odpowiedzi na siedem pytań stanowi propozycje dotyczące rozwiązania konkretnych problemów, [dostęp:] https://niezbednikrodo.pl/pl/blog/rodo-poradnik-dla-sektora-fintech/.

[729] „Dane powinny być kasowane przy uwzględnieniu ograniczeń wynikających z technologicznych uwarunkowań kopii zapasowych oraz ryzyka naruszenia praw i wolności wszystkich osób, których dane osobowe są przechowywane w kopii zapasowej. Biorąc pod uwagę te uwarunkowania należy uznać, że akceptowalnym rozwiązaniem jest, aby dane osobowe były kasowane tylko razem z całą kopią zapasową, po ustaniu podstaw przetwarzania wszystkich zawartych w niej danych osobowych lub po ustaniu przydatności kopii zapasowej. Do tego czasu, kopia zapasowa (zapisane w niej dane osobowe) powinny zostać wyłączone z przetwarzania (ang. put beyond use), co oznacza, że mogą być dalej przetwarzane, jednak należy ograniczyć ich przetwarzanie tylko do przechowywania".

[730] Ministerstwo Cyfryzacji, *RODO-informator…*

[731] Dane nieustrukturyzowane to zawartość pola tekstowego w wiadomościach e-mailowych, zawartość platform społecznościowych, pliki obrazów oraz wideo, dane z czujników i wszystkie inne dane złożone. Oba te rodzaje danych mogą być tworzone zarówno przez ludzi, jak i przez maszyny, [dostęp:] https://websensa.com/pl/2020/05/13/strategiczne-pozyskiwanie-danych-jak-stac-sie-firma-ai-czesc-1/.

podmiotu danych z wszelkich systemów. Zdaje się jednak, że zakres usuwania danych ogranicza się jedynie do tych, względem których podmiot danych się zidentyfikuje. Co ważne, nie jest wystarczające podanie imienia i nazwiska, ale też wskazanie zasobów informacyjnych, w jakich może się pojawiać. Kolejny problem powstaje po określeniu zakresu danych. Zagadnienie wykreślenia informacji z dokumentów, można próbować rozwiązać w oparciu o cele przetwarzania danych (np. nadrzędnie prawnie uzasadnione podstawy przetwarzania).

Biorąc powyższe pod uwagę, przede wszystkim powinno dokonywać się regularnego przeglądu danych. Dzięki temu procesowi, można zidentyfikować również te informacje, które nie zostały skatalogowane, a znajdują się na komputerach, w korespondencji lub na nośnikach typu pendrive[732].

3.5. Podsumowanie

Wystąpienie rewolucji cywilizacyjnej można powiązać z ewolucją narzędzi informacji oraz technik informacyjnych[733]. Uwidacznia się to w dynamicznym postępie Internetu, w tym intranetu czy extranetu, jak również portali społecznościowych[734]. Panuje era pospolitego dostępu do informacji o różnym charakterze. Podmiot umieszczający w sieci różne treści nie ma sposobności kontroli, co się z nimi stanie, tj. nie dysponuje możliwością ich zwielokrotniania, wyszukiwania czy pozycjonowania[735]. Dostęp do strony internetowej zazwyczaj nie jest ograniczony terytorialnie. Dane są przesyłane oraz pozyskiwane za pośrednictwem podmiotów prywatnych i publicznych poza granicami kraju. Postęp technologii informacyjnej powoduje, iż pojawiają się wciąż nowe zagadnienia w związku z ochroną danych osobowych – jednym z nich jest „prawo do bycia zapomnianym"[736].

---

[732] Wszystkie te kategorie danych zaliczają się do tzw. danych nieustrukturyzowanych.

[733] M. Kozłowski, *Jak kosmos pomógł Internetowi,* „Rzeczpospolita" z dnia 18.08.2016 r., s. A11.

[734] Intranet jest rodzajem technologii publicznego dostępu do prywatnych sieci komputerowych. Posiada ograniczony zasięg, kierowany do wąskiej grupy osób, ma charakter wewnątrzkorporacyjny. Extranet z kolei jest siecią powstałą w rezultacie połączenia kilku intranetów firm ze sobą współpracujących.

[735] Godnym uwagi jest fakt, że nawet jeżeli informacja uwidoczni się na zastrzeżonym profilu, to regulamin może zawierać postanowienia w przedmiocie użytkowania danych przez innych, bądź transmisji niektórych praw autorskich do konkretnej treści.

[736] Niekiedy można spotkać się z poglądem, że „prawo do bycia zapomnianym" a „prawo do zapomnienia" są to dwie różne instytucje. Pierwsza z nich polega na żądaniu usunięcia danych oraz zaprzestania ich przetwarzania, jeżeli przestały być konieczne do realizacji celów zgodnie z prawem, natomiast druga oznacza „prawo do niepamięci" z powodu upływu czasu. Co do zasady jednak, przyjmuje się, że są to instytucje tożsame. W mojej ocenie, z praktycznego punktu widzenia oba te prawa nie mają znaczenia dla należytego rozumienia „prawa do bycia zapomnianym", zwłaszcza w świetle proponowanych rozwiązań unijnych. Zob. R.H. Weber, *The right to be forgotten: More than a Pandora's Box?,* "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2011, nr 2, s. 120.

„Prawo do bycia zapomnianym" jest zazwyczaj uznawane za prawo prywatne, które istotnie jest powiązane z prawem do ochrony danych osobowych. To prawo jednostki, które daje jej kontrolę nad informacjami dotyczącymi podmiotu danych. Kontrola ta, jakkolwiek pozorna, polega na ochronie prywatności, co czyni „prawo do bycia zapomnianym" bardziej aspektem prawa prywatnego niż publicznego.

Zakres usunięcia danych w ramach „prawa do bycia zapomnianym" zależy od okoliczności każdego konkretnego przypadku. Dotyczy w głównej mierze danych osobowych, czyli informacji, które identyfikują lub mogą zidentyfikować osobę fizyczną. „Prawo do bycia zapomnianym" obejmuje także przerwanie przetwarzania danych osobowych oraz zaprzestanie dalszego udostępniania tych danych osobom trzecim. W sytuacji, gdy dane osobowe zostały rozpowszechnione publicznie, w sieci, „prawo do bycia zapomnianym" może obejmować żądanie usunięcia lub ograniczenia dostępu do tych danych.

„Prawo do bycia zapomnianym" od czasu wydania wyroku w sprawie Google Spain jest przedmiotem szczególnego zainteresowania. Przed dniem 13 maja 2014 r., zakres tego prawa był ograniczony wyłącznie do żądania usunięcia przez operatora wyszukiwarki internetowej linków z listy wyników wyszukiwania. Aktualnie, „prawo do bycia zapomnianym" kierowane jest nie tylko do operatorów wyszukiwarek internetowych, lecz także do innych podmiotów, które posiadają status administratora w rozumieniu art. 4 pkt 7 Rozporządzenia.

Nie do końca wiadomo, czy platformy hostingowe powinny być uznane za administratorów danych osobowych. W przepisach unijnego Rozporządzenia nie można znaleźć dokładnej odpowiedzi, jakie inne podmioty będące dostawcami usług świadczonych za pośrednictwem Internetu, są traktowane jak administratorzy. Trybunał Sprawiedliwości UE w wyroku o sygn. akt: C-131/12 orzekł, że operator wyszukiwarki internetowej jest administratorem danych osobowych. Nie oznacza to jednak, iż rozstrzygnięcie nie może mieć zastosowania do innych podmiotów pośredniczących. Nadal kwestią otwartą pozostaje, czy operatorzy portali społecznościowych (np. Facebook, Twitter), są zobowiązani do usuwania wpisów zamieszczanych przez użytkowników, czy usunięciu podlegają jedynie adresy URL prowadzące do treści opublikowanych na tych portalach. Stroną internetową, której prawie najczęściej dotyczą zgłoszenia usunięcia linków z wyników wyszukiwania wyszukiwarki Google jest Facebook, który uplasował się na drugim miejscu (jeszcze do niedawna na pierwszym). Aktualnie pierwsze miejsce zajmuje francuska strona internetowa zawierająca

katalog czterech milionów specjalistów i firm, natomiast trzecią pozycję – Twitter[737].

Nie ma też jednoznacznej odpowiedzi na pytanie, czy na gruncie „prawa do bycia zapomnianym" rozpatrywane będzie żądanie usunięcia informacji złożone przez osobę, o której osoba trzecia wspomniała w swym poście. Przekonujący jest pogląd przeciwko możliwości nałożenia tego obowiązku na podmioty świadczące usługi hostingu, przy założeniu, że to użytkownik jest administratorem danych, a operator portalu przetwarza dane zgodnie z jego instrukcjami. Pojawiają się też stanowiska odmienne, na podstawie których, „prawo do bycia zapomnianym" ma zastosowanie do podmiotów świadczących usługi hostingu, lecz tylko do tych aktywnie podejmujących działania i dokonujących operacji na danych osobowych[738].

Z „prawem do bycia zapomnianym" jest związany również zamknięty katalog przesłanek, od którego uzależnione jest jego wykonanie. Wobec tego, gdy osoba, której dane dotyczą, wystąpi z żądaniem usunięcia danych, administrator będzie musiał je usunąć z systemu i z innych miejsc, gdzie je przetwarzał, np. chmura, dysk zewnętrzny, dokumentacja papierowa – pod warunkiem spełnienia się jednej z przesłanek z art. 17 ust. 1 RODO.

W regulacjach prawnych RODO nie określono treści, jak i formy wniosku o usunięcie danych osobowych. Z praktycznego punktu widzenia oznacza to przyjęcie różnych rozwiązań w tym temacie. Wydaje się dopuszczalne złożenie wniosku z oznaczeniem danych wnioskodawcy i wyartykułowaniem, że zaszła jedna z okoliczności wskazanych w art. 17 ust. 1 RODO, choć w niektórych sytuacjach nie jest wykluczone złożenie wniosku bez uzasadnienia. Formę wniesienia żądania może charakteryzować dowolna postać. Wystąpienie z żądaniem usunięcia informacji wymaga indywidualnego rozpoznania. Nie jest wykluczone, że żądanie zostanie wykonane jedynie częściowo[739].

Na osoby, których dane dotyczą, nie został nałożony obowiązek ani udowodnienia, ani uprawdopodobnienia zasadności swojego żądania. Zatem istnieje konieczność podejmowania decyzji w oparciu o takie informacje, jakie zostaną zaprezentowane przez samych

[737] Całkowita liczba żądań otrzymana od 29 maja 2014 r. do 19 kwietnia 2024 r. wynosi 1 576 009. Całkowita liczba żądań usunięcia adresów URL otrzymana w tym samym okresie wynosi 6 127 262. Na stronie źródłowej istnieje możliwość uzyskania dostępu do żądań (po usunięciu informacji umożliwiających identyfikację), jakie otrzymuje wyszukiwarka Google od osób prywatnych z różnych krajów, w tym z Polski. Podczas analizy każdej sprawy, należy wziąć pod uwagę prawa każdej osoby, a także interes publiczny. Zob. *Żądania usunięcia treści zgodnie z europejskim prawem dotyczącym prywatności,* [dostęp:] https://transparencyreport.google.com/eu-privacy/overview.

[738] D. Keller, *The final draft of Europe's "Right to be forgotten law",* "The Center for Internet and Society", [dostęp: 17.12.2015] https://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law.

[739] B. Fischer, *Prawo do usunięcia danych,* [w:] *Realizacja praw osób, których dane dotyczą, na podstawie RODO,* red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 211.

zainteresowanych. Nie wyklucza to częściowej arbitralności decyzji, bowiem administratorzy danych nie mają legitymacji, czy technicznych możliwości weryfikacji twierdzeń przedstawionych we wniosku. Może to skutkować brakiem spójności w ocenie wniosków przez administratorów, przez co zwiększy się liczba skarg składanych na administratorów do właściwych organów ochrony danych.

Lektura wyroku wydanego w sprawie C-131/12 nie odpowiada na pytania kierowane przez użytkowników sieci (podmioty uprawnione) i administratorów wyszukiwarek internetowych (podmioty zobowiązane), a odnoszące się do praktycznej realizacji „prawa do bycia zapomnianym"[740]. Wypełnienia luk podjęły się podmioty zobligowane do wykonania przedmiotowego prawa oraz organy powołane do ochrony danych osobowych obywateli krajów unijnych za pośrednictwem Grupy Roboczej Art. 29. Ciężar oceny zasadności żądań, w tym możliwości zastosowania „prawa do bycia zapomnianym" został nałożony na podmioty prywatne, dostawców usług wyszukiwania.

Niemniej jednak, potencjalna skłonność administratorów do podejmowania decyzji zgodnych z wnioskiem podmiotu danych może wynikać z samej konstrukcji „prawa do bycia zapomnianym". Regulacje prawne są sformułowane w sposób zachęcający administratorów do podejmowania decyzji korzystnych dla wnioskodawcy[741].

Podczas realizacji „prawa do bycia zapomnianym", istotnym z punktu widzenia podmiotu danych jest termin. Powinno to nastąpić bez zbędnej zwłoki[742]. W praktyce, przedmiotowe prawo ma zapobiegać przetrzymywaniu danych osobowych, które utraciły swoją aktualność lub stały się dla administratora zbędne. Regulacja nie zapewnia przejrzystych wskazówek dla administratorów danych, w jaki sposób mają dokonywać oceny, czy np. dane nie są już niezbędne dla celów, do których zostały zgromadzone, co stanowi obciążenie dla administratorów. Kryteria oceny nie odnoszą się też do prawdziwości danej informacji. Stanowi to możliwość żądania usunięcia danych, które opublikowano zgodnie z prawem. Może to prowadzić do zjawiska „przepisywania historii"[743].

Podmioty, które posiadają należyte procedury analizowania takich, bądź podobnych

[740] Między innymi: czy osoby pełniące funkcje publiczne mogą żądać usunięcia prawdziwych i opublikowanych zgodnie z prawem, ale niewygodnych dla siebie faktów historycznych? Jakie kryteria pozwalają ocenić, że dana informacja stała się ze względu na upływ czasu niewłaściwa, niestosowna, czy też nadmierna w stosunku do celu, w jakim została zebrana?

[741] Wystarczy zaznaczyć, że przepisy przewidują wysokie kary pieniężne dla administratorów za podjęcie błędnej decyzji odmownej, podczas gdy usunięcie treści, nawet bez dostatecznej podstawy faktycznej i prawnej, nie jest usankcjonowane (art. 83 ust. 5 lit. b) RODO).

[742] Nie należy tego utożsamiać z terminem natychmiastowym, o czym przesądza treść art. 12 ust. 3 Rozporządzenia.

[743] Z ang. *rewriting history.*

wniosków, nie mają problemów z dotrzymaniem wyżej wskazanego terminu. Realne też jest dla nich dokonanie oceny zgodności takiego wniosku z przewidzianymi prawem przesłankami. Z kolei podmioty, które nie były zobowiązane nigdy wcześniej do takich działań, mogą zatem nie być przygotowane do samodzielnego przeprowadzenia takiej oceny w zakreślonym terminie. Dodatkowym utrudnieniem jest brak praktycznych wskazówek odnoszących się do zakresu usuwania treści. Bezpośrednią konsekwencją może być automatyzm podejmowanych decyzji w kwestii rozpatrywania żądań, przy czym administratorzy są zobligowani do działania zgodnie z wnioskiem osoby, której dane dotyczą, z pominięciem odpowiedniego wyważenia interesów i wolności.

Wobec powyższego, z punktu widzenia podmiotów, na jakich spoczywa obowiązek realizowania żądań w zakresie „prawa do bycia zapomnianym", istotną rolę odgrywa dysponowanie określonymi kryteriami oceny zasadności żądania usunięcia. Trybunał Sprawiedliwości UE powierzchownie odniósł się do tego problemu, nie określając, w jaki sposób dokonywać wyważenia prawa do prywatności i prawa do informacji czy wolności wypowiedzi. Nie wskazał przejrzystych warunków. Powołał liczne klauzule generalne. Z orzeczenia można wyinterpretować jednak pewne wskazówki. Jedną z okoliczności, która powinna być brana pod uwagę, jest rola odgrywana przez daną osobę w życiu publicznym. W szczególności dotyczy to sytuacji, kiedy ingerencja w prawa podstawowe takiej osoby jest umotywowana nadrzędnym interesem odbiorców, którym przysługuje prawo dostępu do danej informacji. Kolejną przesłanką, na którą powołuje się TSUE, jest czas, jaki upłynął od momentu publikacji.

Przepisy Rozporządzenia nr 2016/679 nie wskazują, w jaki sposób należałoby dokonać oceny czy proces przetwarzania danych jest niezbędny do korzystania z prawa do wolności wypowiedzi i informacji. Co prawda, źródła prawa UE mogą służyć za drogowskazy wyznaczające ogólne kierunki. Powinny być jednak traktowane w kategoriach zasad generalnych, a nie jako zerojedynkowe kryteria mogące stanowić podstawę analizy wpływających żądań[744]. Zarówno art. 11 KPP, jak i art. 10 EKPCz, przewidują szeroko zdefiniowane prawo do wyrażania opinii, które swoim zakresem obejmuje również prawo do otrzymywania i przekazywania informacji.

W punkcie 153 preambuły Rozporządzenia oraz w art. 85 RODO przewidziano możliwość przyjęcia przez kraje członkowskie regulacji pozwalających na pogodzenie prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji. Trudno jednak ocenić

[744] M.L. Rustad, S. Kulevska, *Reconceptualizing the right to be forgotten to enable transatlantic data flow,* "Harvard Journal of Law&Technology" 2015, nr 2, s. 371.

efekty wprowadzenia takiego ustawodawstwa na poziomie krajowym. Można jedynie domniemywać, iż jednym ze skutków może być rozbieżność zarówno w obszarze stosowanych przez poszczególnych administratorów procedur regulujących sposoby składania wniosków o usunięcie informacji, ale także i w ramach różnych jurysdykcji na poziomie ustawowym.

Kształt przepisów RODO wprowadzających „prawo do bycia zapomnianym" pozwala przypuszczać, że więcej przywilejów posiada grono obrońców prawa do prywatności użytkowników Internetu. Osłabiona jest natomiast pozycja obrońców prawa do wolności słowa i swobody wyrażania opinii.

Istotną uwidaczniającą się różnicą pomiędzy „prawem do bycia zapomnianym" z wyroku Google Spain C-131/12, a tym finalnie przyjętym w art. 17 Rozporządzenia nr 2016/679 jest to, że osoba, której dane dotyczą mogła żądać usunięcia linków z listy wyników wyszukiwania mającej za punkt wyjścia jej imię i nazwisko. Natomiast w treści wskazanego przepisu brak jest takiego dodatkowego kryterium.

Z realizacją „prawa do bycia zapomnianym" związane są też problemy z kopiami zapasowymi i archiwalnymi oraz danymi nieustrukturyzowanymi. Kopie zapasowe i archiwalne są trudne do zarządzania z uwagi na niemożność ich całkowitego zlokalizowania i usunięcia. Dane nieustrukturyzowane (np. pliki tekstowe, e-maile) również mogą stanowić wyzwanie w kontekście prawnej implementacji „prawa do bycia zapomnianym". Znalezienie i usunięcie wszystkich wystąpień danych osobowych w takich nieustrukturyzowanych źródłach może okazać się czasochłonne i skomplikowane. Niekiedy istnieje obowiązek zachowania pewnych danych przez określony czas ze względów regulacyjnych, prawnych lub biznesowych. W takich przypadkach, usunięcie danych osobowych w ramach „prawa do bycia zapomnianym" może być sprzeczne z wymaganiami dotyczącymi zachowania danych. Konieczne jest zatem znalezienie równowagi pomiędzy przestrzeganiem „prawa do bycia zapomnianym" a zachowaniem zgodności z obowiązującymi regulacjami.

Pomimo pewnych zastrzeżeń, „prawo do bycia zapomnianym" wyznacza nowy standard ochrony danych osobowych. Uwzględnienie tego prawa w przepisach Rozporządzenia należy ocenić pozytywnie, zwłaszcza w kontekście zaproponowanych rozwiązań na poziomie unijnym, tj. zwiększenia kontroli nad sposobem wykorzystania informacji, zagwarantowania wdrożenia przejrzystych mechanizmów ochrony danych oraz promowania tego w sieci. Regularne realizowanie tych idei przyczynia się do powstawania cybergeneracji praw człowieka, wśród których jednym z fundamentalnych jest „prawo do bycia zapomnianym", stanowiące kolejny krok ku adaptacji systemów prawnych do

dynamicznych przemian technologicznych[745].

[745] M.L. Ambrose, *It's about time: Privacy, Information Life Cycles, and the Right to be Forgotten,* "Stanford Law Review" 2013, nr 2, s. 371.

Rozdział 4. Zakres oddziaływania „prawa do bycia zapomnianym" na krajowy porządek prawny

4.1. Uwagi wstępne

Po wejściu w życie postanowień Ogólnego Rozporządzenia o Ochronie Danych Osobowych, w porządku prawnym Rzeczypospolitej Polskiej przestała obowiązywać ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., obejmująca szerszy zakres niż RODO. Potrzeba wypełnienia tej luki oraz obowiązek implementacji Dyrektywy 2016/680[746] spowodowały konieczność wprowadzenia, jak też pozostawienia czy znowelizowania obowiązujących przepisów w systemie prawa odnoszących się do zagadnienia przetwarzania danych osobowych na potrzeby procesów nieobjętych Rozporządzeniem[747].

Warunkiem należytego funkcjonowania administratorów danych i podmiotów przetwarzających dane osobowe zgodnie z przepisami Ogólnego Rozporządzenia o Ochronie Danych Osobowych jest stworzenie takiej sytuacji, w której w systemie prawa krajowego nie będą występowały regulacje pozostające w kolizji z tym aktem prawnym[748]. Jej wykreowanie jest skomplikowane, ponieważ wiele procesów związanych z przetwarzaniem danych osobowych jest regulowanych w przepisach szczególnych, które mają pierwszeństwo przed przepisami rangi ogólnej w myśl zasady *lex specialis derogat legi generali.* Ich umiejscowienie i systematyka są ważne w kontekście funkcjonowania równolegle do przepisów RODO, choć nie zawsze uda się przeprowadzić ich reinterpretację w taki sposób, aby była zgodna z unijnymi normami. Istnienie krajowych norm szczególnych samo w sobie, w zakresach bezpośrednio regulowanych w RODO, utrudnia realizację jednego z podstawowych założeń reformy, tj. jednolitości stosowania postanowień, w przypadku braku zezwolenia na zmianę szczególnych uregulowań przez państwa członkowskie. Zasada pierwszeństwa stosowania rozporządzeń Unii Europejskiej nie zapewnia wystarczającej sprawności działania systemu ochrony danych osobowych na poziomie ich przeciętnego

[746] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L.2016.119.89).

[747] Wydaje się, że ustawodawca nie miał na celu stworzenia żadnego wspólnego aktu prawnego mającego wypełnić ową lukę, pozostawiając to do wykonania wielu regulacjom o charakterze szczególnym.

[748] To wynika z tego, że rozstrzygnięcia są bezpośrednio podejmowane na podstawie RODO. Jedynie tam, gdzie ustawodawca w samym Rozporządzeniu dopuścił taką możliwość, państwa członkowskie mogą daną kwestię uregulować odmiennie, np. art. 6, art. 9 RODO.

administratora[749].

Rozporządzenie stało się pierwszoplanową regulacją, definiującą zasady i sposoby przetwarzania danych, a także obowiązki administratorów oraz uprawnienia organów nadzoru. RODO posiada zasięg ogólny, wiąże w całości co do wszystkich zawartych w nim postanowień i jest wprost stosowane we wszystkich krajach członkowskich. Wskutek tego, staje się ono częścią krajowych systemów prawnych bez konieczności dokonywania czynności transpozycyjnych i wywiera bezpośrednie skutki wobec jednostek. W pewnym zakresie, unijne Rozporządzenie przewiduje uzupełnienie własnych regulacji przepisami krajowymi. Zawarte odesłania mają na celu doprecyzowanie lub ograniczenie stosowania w prawie krajowym przepisów RODO.

W związku z powyższym, zaistniała potrzeba stworzenia nowego aktu prawnego, którego przepisy będą adekwatne do standardów przyjętych na poziomie Unii Europejskiej[750]. W dniu 22 maja 2018 roku Prezydent RP podpisał ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych. Nowa ustawa weszła w życie 25 maja 2018 roku. Uchwalenie tej ustawy było związane przede wszystkim z potrzebą doprecyzowania przepisów RODO oraz dostosowania ich do polskiego porządku prawnego.

Ważne jest określenie zakresu podmiotowego obowiązującej ustawy. Przepisy Rozporządzenia unijnego wprowadziły pojęcie „administratora" oraz „podmiotu przetwarzającego". Na pierwszy rzut oka, wydawać by się mogło, że Rozporządzenie unijne odnosi się wyłącznie do osób fizycznych. Takie założenie jest błędne, ponieważ przez administratora należy rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Podmiotem przetwarzającym jest zaś osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO). Krąg podmiotów jest zbieżny, niemniej jednak inaczej prezentuje się zakres czynności przez nich podejmowanych. Zakres podmiotowy ustawy o ochronie danych osobowych z 2018 roku kształtuje się odmiennie od tego zaprezentowanego powyżej i odnosi się tylko do osób fizycznych.

W przeciwieństwie do poprzednio obowiązującej ustawy z dnia 29 sierpnia 1997 roku, w tej z dnia 10 maja 2018 roku nie uregulowano podstawowych definicji, zasad przetwarzania

[749] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym,* Wrocław 2017, s. 136.
[750] *Nowa ustawa o ochronie danych osobowych od 25 maja 2018 r.,* [dostęp: 23.05.2018] https://ksiegowosc.infor.pl/wiadomosci/783642,Nowa-ustawa-o-ochronie-danych-osobowych-od-25-maja-2018-r.html.

danych, obligatoryjnych elementów obowiązku informacyjnego, czy praw przysługującym osobom, których dane dotyczą[751]. Byłoby zatem błędem powoływanie się na ustawę jako podstawę prawną dla przetwarzania danych.

Z punktu widzenia administratorów, znaczenie mają wprowadzone postanowienia, w których zastąpiono Generalnego Inspektora Ochrony Danych Osobowych nowym organem. Istotny jest także tryb postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, przebieg kontroli przestrzegania przepisów o ochronie danych osobowych, tryb dochodzenia przed sądem roszczeń cywilnych związanych z naruszeniem przepisów o ochronie danych osobowych, ograniczenia w wysokości administracyjnych kar pieniężnych nakładanych na podmioty publiczne oraz sankcje karne za naruszenie przepisów RODO. Przedmiotem analizy tego Rozdziału będzie przedstawienie motywów, jakimi kierował się ustawodawca, wprowadzając nową ustawę oraz próba wyrażenia oceny w przedmiocie zasadności i skuteczności nowych uregulowań.

Pomimo udoskonalania przepisów w zakresie ochrony danych osobowych, istnieje ryzyko naruszenia praw i wolności osób, których te dane dotyczą. W dobie rewolucyjnych zmian technologicznych nie sposób go całkowicie wyeliminować. W przepisach RODO wyszczególniono przykładowy katalog zagrożeń, do którego zalicza się dyskryminację, kradzież lub oszustwo z wykorzystaniem tożsamości, stratę finansową, naruszenie dobrego imienia czy poufności danych osobowych chronionych tajemnicą zawodową, jak też nieuprawnione odwrócenie pseudonimizacji. Lista tych zagrożeń może się rozszerzać. W tym Rozdziale zostanie zbadana zależność pomiędzy występującymi ryzykami. Warte uwagi jest sprawdzenie kwestii, na czym polegają wymienione ryzyka, czy każde z nich posiada taką samą wartość i odnosi analogiczny skutek w przypadku naruszenia ochrony danych osobowych. W mojej ocenie, nie można przyjąć, że jedno zagrożenie jest poważniejsze od drugiego. Różnica polega jedynie na sposobie dokonania naruszenia danych osobowych. Być może intensywność podejmowanych działań też jest różna, niemniej rezultat pozostaje niezmienny.

Przepisy Rozporządzenia o Ochronie Danych Osobowych zniosły obowiązek posiadania polityki bezpieczeństwa oraz innych procedur. Uregulowania są niemalże elastyczne w temacie bezpieczeństwa. Administrator danych powinien zdecydować, jakie wprowadzić zabezpieczenia i reguły postępowania, tak żeby były one odpowiednie. W przepisach RODO nie określono polityki bezpieczeństwa. Posłużono się w nich polityką

[751] M. Szkutnik, *Przepisy o ochronie danych osobowych, czyli nie tylko RODO,* [dostęp: 29.09.2020] https://blog-daneosobowe.pl/przepisy-o-ochronie-danych-osobowych-czyli-nie-tylko-rodo/.

ochrony danych. Pomimo tego, że terminologia jest inna, należy opowiedzieć się za stanowiskiem prezentującym pogląd, że chodzi o jeden dokument[752]. Polityka bezpieczeństwa nie jest obowiązkowa, lecz warto ją posiadać. Aczkolwiek, w mojej ocenie, należy uznać ten dokument za niezbędny. Za tym stwierdzeniem przemawia również zasada rozliczalności. Przepisy RODO nie zaliczają polityki bezpieczeństwa do dokumentacji o charakterze obligatoryjnym, ale nakładają na administratora obowiązek udokumentowania przestrzegania przepisów w zakresie ich ochrony. Uregulowania unijnego Rozporządzenia nie narzucają żadnego szablonowego wzoru. Rozwiązanie to wydaje się słuszne, ponieważ działalność przedsiębiorstw się od siebie różni, a zatem administrator powinien dopasować odpowiednie zabezpieczenia do zachodzących procesów.

Na administratora danych osobowych został jednak nałożony obowiązek wdrożenia stosownych środków technicznych i organizacyjnych. Jednym z nich jest pseudonimizacja danych. Instytucja ta została oficjalnie wprowadzona do obrotu prawnego przez przepisy Rozporządzenia unijnego. Pseudonimizacja, często błędnie, utożsamiana jest z anonimizacją. Pojęcia te, choć są podobne, znacznie się od siebie różnią.

Ataki cybernetyczne są zjawiskiem dosyć popularnym. Pomimo stosowania zabezpieczeń, często dochodzi do naruszenia ochrony danych osobowych. Łamane są też prawa osób, których dane są przetwarzane. W przepisach RODO wskazano konkretne procedury służące realizacji prawa do ochrony danych.

Pierwszym z mechanizmów prawnych mającym służyć zagwarantowaniu praw podmiotu danych jest skarga do organu nadzorczego. Stroną skarżącą może być osoba przebywająca na terenie UE. Podmiot danych nie może być reprezentowany przez osoby fizyczne. Właściwość miejscowa organu, do którego skarga może zostać wniesiona, nie została określona. Wskazuje to na dowolność w wyborze organu nadzorczego. Złożenie skargi do danego organu nadzorczego nie jest równoważne z tym, że to właśnie ten organ będzie prowadził sprawę, której skarga dotyczy.

Organ nadzorczy posiada prawo do nakładania administracyjnych kar pieniężnych. Kara powinna być skuteczna, proporcjonalna i odstraszająca. Kary finansowe mogą być stosowane samoistnie lub obok innego środka ochrony prawnej.

W art. 79 RODO przewidziano możliwość skorzystania z ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu. Pomimo woli ujednolicania przepisów państw członkowskich zgodnie z polityką RODO, środek ten nie

[752] I. Przetacznik, *RODO: Polityka Bezpieczeństwa-czy muszę ją mieć?,* [dostęp: 10.05.2018] https://legalnybiznesonline.pl/rodo-polityka-bezpieczenstwa/.

musi być tożsamy dla wszystkich krajów członkowskich Unii Europejskiej. Zalicza się go do samodzielnych środków ochrony prawnej przysługujących osobie fizycznej. Nic nie stoi na przeszkodzie, aby ustawodawca krajowy, dla wykonania przedmiotowego środka prawnego mógł zastosować przepisy proceduralne dotyczące rozpoznawania spraw w postępowaniu procesowym. W świetle regulacji RODO, dopuszczalne jest złożenie pozwu o usunięcie danych osobowych. Odpowiedzialność administratora lub podmiotu przetwarzającego została oparta na zasadzie bezprawności działania. Nieco inaczej została ukształtowana zasada odpowiedzialności za poniesioną szkodę na skutek przetwarzania danych osobowych w sposób naruszający przepisy RODO. Ustawodawca wprowadził w tym przypadku zasadę odpowiedzialności na zasadzie winy oraz domniemanie zawinienia.

W art. 82 RODO wprowadzono zasady odpowiedzialności odszkodowawczej. W celu uniknięcia odpowiedzialności nie wystarczy tylko wykazać, że administrator lub podmiot przetwarzający nie ponosi w określonym zakresie winy za dane zdarzenie, ale że nie ponosi jakiejkolwiek winy. Co istotne, odpowiedzialność administratora danych osobowych jest szersza w stosunku do odpowiedzialności podmiotu przetwarzającego.

4.2. Implementacja przepisów Ogólnego Rozporządzenia o Ochronie Danych Osobowych do polskiego systemu prawnego

4.2.1. Przesłanki uchwalenia nowych regulacji krajowych, usunięcia kolizji i możliwości pozostawienia dotychczasowych norm prawnych

Rozporządzenie unijne zaczęło obowiązywać w polskim porządku prawnym od dnia 25 maja 2018 roku. Od tego momentu, przepisy państwa członkowskiego, m.in. Polski, musiały zapewniać skuteczne stosowanie przepisów RODO, nie powielając jego rozwiązań, ani też nie pozostając z nim w sprzeczności. Zakres kompetencji wdrażania regulacji prawnych przez kraje członkowskie wyznacza co do zasady samo Rozporządzenie[753].

Konieczne stało się zatem opracowanie zupełnie nowej regulacji. Miała ona odpowiadać standardom ochrony danych osobowych przyjętym na poziomie Unii Europejskiej. Przepisy ustawy stanowią uzupełnienie RODO, w zakresie, w jakim ustawodawca unijny zezwolił na doprecyzowanie pewnych zagadnień wprowadzonych przez Rozporządzenie.

[753] P. Kozik, *Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego,* „Europejski Przegląd Sądowy" 2017, nr 5, s. 18-22.

Przepisy ustawy z dnia 29 sierpnia 1997 roku zawierały regulacje odmienne od tych, które przewidywało RODO, chociażby w odniesieniu do definicji zgody podmiotu danych. Porównując definicję zgody na gruncie ustawy i RODO można dojść do kilka wniosków. Po pierwsze, z treści przepisów Rozporządzenia wynika, że zgoda może mieć formę nie tylko oświadczenia, ale również wyraźnego działania potwierdzającego, co było niedopuszczalne przez ustawę z 1997 roku. Po drugie, na gruncie przepisów Rozporządzenia unijnego wskazano formy udzielenia zgody – pisemne, elektroniczne, ustne. Po trzecie, w przepisach RODO wyjaśniono, jaki minimalny zakres informacji o procesie przetwarzania danych trzeba przekazać osobie wyrażającej zgodę, aby była ona świadoma. Po czwarte, możliwe jest zbieranie jednej zgody na przetwarzanie danych osobowych w kilku różnych celach. Według nieobowiązującej już ustawy z 1997 r. na każdy cel przetwarzania należało uzyskać odrębną zgodę[754].

W ustawie brak było przepisów dotyczących m.in. certyfikacji. Certyfikat zgodności to instrument mający zwiększyć przejrzystość i poprawić przestrzeganie regulacji unijnych w obszarze ochrony danych osobowych. Ideą tego instrumentu jest poddanie się weryfikacji zewnętrznemu, niezależnemu podmiotowi przez administratora danych lub podmiot przetwarzający celem zbadania, czy spełniono wymogi z RODO i w przypadku uzyskania pozytywnej oceny, otrzymanie certyfikatu. Korzyścią płynącą z posiadania zaświadczenia jest wzrost zaufania do administratora lub podmiotu przetwarzającego, zarówno ze strony kontrahentów, jak i osób, których dane są przetwarzane, wynikający ze świadomości minimalizacji ryzyka naruszeń ochrony danych osobowych[755].

W Rozporządzeniu wyeliminowano artykuły dotyczące rejestracji zbiorów danych. Obowiązek wprowadzony przez ustawę o ochronie danych osobowych z 1997 roku na podstawie poprzednio obowiązującej Dyrektywy 95/46/WE nie sprawdził się ani w Polsce, ani w innych państwach członkowskich. Zbiory nie były zgłaszane, nie informowano o dokonywaniu zmian. W związku z tym, w przepisach RODO ustanowiono obowiązek prowadzenia przez administratora i podmiot przetwarzający rejestru czynności przetwarzania. Rejestr czynności ma charakter wewnętrzny. Nie podlega notyfikacji. Należy go jednak przekazać organowi nadzorczemu – na jego żądanie. Zmieniono zatem sposób kontroli. W ustawie z dnia 1997 roku miała ona charakter profilaktyczny, zgodnie z ideą RODO ma

[754] *Zgoda na przetwarzanie danych osobowych według RODO,* [dostęp: 19.05.2017] https://blog-daneosobowe.pl/zgoda-przetwarzanie-danych-osobowych-rodo/.
[755] https://gdpr.pl/artykuly/certyfikacja-rodo.

charakter *ex-post*[756].

W ustawie z dnia 10 maja 2018 roku ustanowiono nowy organ nadzorczy, a mianowicie Prezesa Urzędu Ochrony Danych Osobowych, w miejsce Generalnego Inspektora Ochrony Danych. Do nadania takiej nazwy skłoniła treść przepisów Rozporządzenia, a decyzja w tej kwestii ma wyłącznie wymiar porządkujący. RODO wprowadziło funkcję inspektora ochrony danych. Pozostawienie nazwy „GIODO" mogłoby okazać się mylne w zakresie pozycji ustrojowej. Zgodnie z art. 38 ust. 3 Rozporządzenia inspektorzy ochrony danych pozostają niezależni. Poza tym, powstałaby konieczność nazwania inspektorami pracowników biura, którzy w imieniu organu przeprowadzają postępowanie kontrolne. Na kanwie przepisów ustawy z 1997 roku funkcjonowali w strukturze organizacyjnej inni inspektorzy, względem których był on inspektorem generalnym. To przesądziłoby o tym, że w systemie ochrony danych osobowych byłyby dwie kategorie inspektorów – pracownicy organu nadzorczego oraz osoby mające inny status, powoływane wewnątrz struktury organizacyjnej administratorów i podmiotów przetwarzających[757].

Na drodze postępowania cywilnego, w art. 79 RODO wprowadzono prawo do ubiegania się o ochronę prawną przed sądem w sytuacji uznania, że prawa podmiotu danych zostały naruszone. Każda osoba fizyczna może uzyskać odszkodowanie za poniesioną szkodę od administratora lub podmiotu przetwarzającego. Nowa ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku doprecyzowuje, że do roszczeń z tytułu naruszenia przepisów RODO należy stosować przepisy kodeksu cywilnego, a właściwym organem do rozpatrywania roszczeń z tego tytułu jest Sąd Okręgowy.

Na drodze postępowania administracyjnego, unijny ustawodawca dał Prezesowi UODO prawo do nakładania kar pieniężnych na podstawie art. 83 RODO. Ustawa o ochronie danych osobowych z 2018 roku ograniczyła wysokość kar w odniesieniu do jednostek sektora finansów publicznych, instytutów badawczych oraz Narodowego Banku Polskiego, z wyjątkiem państwowych i samorządowych instytucji kultury.

Na drodze postępowania karnego, katalog przepisów prawnych w nowej ustawie jest węższy od tego zawartego w ustawie o ochronie danych osobowych z 1997 roku. Ustawodawca penalizuje przetwarzanie danych osobowych, gdy jest to niedopuszczalne oraz

[756] J. Kamińska-Kasjaniuk, *Rejestr czynności przetwarzania danych osobowych zastąpi rejestrację zbiorów w GIODO,* [dostęp: 12.03.2018] https://odoserwis.pl/a/1175/rejestr-czynnosci-przetwarzania-danych-osobowych-zastapi-rejestracje-zbiorow-w-giodo.

[757] Uzasadnienie do projektu ustawy o ochronie danych osobowych z dnia 13 września 2017 r., druk sejmowy nr 2410, Sejm VIII kadencji, [dostęp:] https://www.sejm.gov.pl/.

gdy dane przetwarza osoba do tego nieupoważniona. Drugim przypadkiem penalizacji jest udaremnianie lub utrudnianie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych[758].

Okoliczność kompleksowego stosowania regulacji unijnego Rozporządzenia, nie powinna też być jednoznacznie odczytywana jako przesłanka usunięcia przepisów krajowych, które wprawdzie wpływają na proces przetwarzania danych osobowych, to jednak zabezpieczają inne cele[759]. Ustawodawca powinien wprost ustalić, w jakim stopniu dokonuje ograniczenia stosowania regulacji unijnych, określając przy tym zasady przetwarzania danych. Brak podjęcia takiej aktywności może doprowadzić do konfliktu pomiędzy prawem krajowym a pochodnym z uwagi na pierwszeństwo zasady, w myśl której najpierw stosuje się przepisy rozporządzeń Unii Europejskiej. W praktyce zjawisko to napotyka na wiele trudności, głównie z powodu respektowania zasady legalizmu działania i domniemania konstytucyjności prawa krajowego.

4.2.2. Charakter obowiązku informacyjnego administratora danych

Zauważalna jest zmiana w kwestii ustanawiania reguł ogólnych przesyłania informacji pomiędzy administratorem i podmiotem przetwarzającym a osobami, których dane dotyczą. W stosunkach z krajowym organem ochrony danych taka modyfikacja nie następuje, znikają poprzednie obowiązki i pojawiają się nowe[760].

Administrator danych osobowych powinien poinformować osobę, której dane dotyczą o okresie przetwarzania danych, bądź kryteriach jego ustalenia najpóźniej w momencie pobierania danych. Obowiązek informacyjny należy określić w rejestrze czynności przetwarzania. Co jakiś czas należy dokonywać odpowiedniego przeglądu i usuwać dane, których okres przetwarzania się zakończył. W sytuacji, jeśli dane osobowe mogą być przetwarzane przez różne okresy, warto usunąć je lub zniszczyć po upływie najdłuższego

[758] *Omówienie ustawy o ochronie danych osobowych z 10 maja 2018 roku,* [dostęp:] https://gdpr.pl/omowienie-ustawy-o-ochronie-danych-osobowych-z-10-maja-2018-roku.

[759] Za przykład może posłużyć gałąź prawa administracyjnego. Przepisy RODO nie doprowadziły do likwidacji procedur w przedmiocie uzyskiwania zaświadczeń czy decyzji. W takich wypadkach przetwarza się zazwyczaj dane osobowe, chociaż służy to określonym celom ustanowionym w normach prawa materialnego, a wszelkiego rodzaju regulacje formalne, muszą być traktowane jako autonomiczne w odniesieniu do RODO. W oparciu o RODO można sprawdzić zakres przetwarzanych danych, ale już dostęp do akt konkretnego postępowania, tryb sprostowania czy zmiany informacji w nich ujawnionych nadal wymaga stosowania przepisów Kodeksu postępowania administracyjnego (Dz. U. 2024, poz. 572, dalej: k.p.a.).

[760] Mam tu na myśli np. art. 33 unijnego Rozporządzenia, tj. zgłaszanie naruszenia ochrony danych osobowych krajowemu organowi nadzorczemu, czy art. 36 regulujący przeprowadzanie uprzednich konsultacji z takim organem. Jednocześnie, co za tym idzie, wygasa istniejący dotąd w Polsce obowiązek rejestracji zbiorów w Rejestrze centralnym prowadzonym przez GIODO.

z nich[761]. Pomimo że nie jest to *expressis verbis* wyrażone przez RODO, informując podmiot o przysługujących mu prawach, administrator w ramach dobrych praktyk powinien także wskazać mu, jakie kroki powinien on podjąć, aby móc z tego prawa rzeczywiście skorzystać[762].

Informowanie osób, których dane dotyczą o przetwarzaniu ich danych osobowych zalicza się do podstawowych obowiązków administratora danych. Tylko podmiot danych, który został należycie poinformowany jest w stanie podejmować racjonalne decyzje w związku z przetwarzaniem danych osobowych i prawidłowo reagować na ewentualne nieprawidłowości w tym zakresie. Na gruncie tej tematyki, należy z bliska przyjrzeć się art. 12 RODO, który w znaczący sposób rzutuje na realizację praw i obowiązków informacyjnych określonych w Rozporządzeniu. Refleksja po wykładni tego przepisu sprowadza się do wyznaczenia reguł odpowiedzialności administratora za rozpowszechnianie informacji podmiotom danych w sposób umożliwiający im zrozumienie kierowanych do nich wiadomości. Zamierzeniem twórców nowej regulacji było pokazanie, że to nie podmiot danych ma się dostosować do poziomu i sposobu ich przekazywania, ale to właśnie administrator ma tak formułować komunikaty, aby nie stwarzać problemów poznawczych, zarówno w sferze formalnej, jak i znaczeniowej[763]. Administratorzy danych do tej pory lakonicznie podchodzili do obowiązków informacyjnych, wykorzystując standardowe, ogólnie przyjęte formuły. Nowa regulacja zmusiła ich do przeprowadzenia analizy możliwości poznawczych wszelkich kategorii podmiotów danych, przez których odbierane są komunikaty i dostosowywania ich treści oraz formy do jej rezultatów.

Podstawowym warunkiem wykonania zasady przejrzystego informowania jest dokonanie przez administratora danych racjonalnego wyboru w zakresie docelowych grup osób, których dane będzie przetwarzał. Mając na uwadze transgraniczność procesu przetwarzania danych, należy traktować normy unijnego Rozporządzenia jako należyte także w przypadku interakcji z obcokrajowcami. Nawet, jeśli przetwarzanie miało miejsce na terenie państwa polskiego, to i tak mogłoby dochodzić do gromadzenia danych osobowych ludzi, którzy nie władają językiem polskim, w związku z czym administrator musi posiadać

---

[761] *Prawo do bycia zapomnianym-obowiązki administratora danych,* [dostęp: 27.01.2021] https://spoldzielniaalbert.pl/2021/01/27/prawo-do-bycia-zapomnianym-obowiazki-administratora-danych/.

[762] Na przykład podając dane kontaktowe do organu nadzoru. Zob. M. Gudfinnsson, *Obowiązek informacyjny w RODO,* [dostęp: 05.04.2018] https://blog-daneosobowe.pl/obowiazek-informacyjny-rodo/.

[763] Jedyną dyspozycją obowiązującą na terenie Polski o analogicznym przesłaniu był obowiązek podania w powszechnie używanej formie treści danych osoby, której one dotyczą, co nie powodowało jednak potrzeby dostosowania się do możliwości poznawczych odbiorcy komunikatu i nie było przesłanką wprowadzenia generalnego standardu jakościowego odnoszącego się do ogółu przekazów kierowanych do podmiotu danych. Niniejsze wynikało z art. 32 ust. 1 pkt 3 u.o.d.o.

umiejętność wypełniania obowiązków informacyjnych w zgodzie z RODO, tzn. w języku władnym dla podmiotu danych.

Pojawia się zatem istotne zagadnienie, a więc potrzeba dostosowywania się administratora danych do poziomu percepcji odbiorcy informacji. Posiada on taki obowiązek też w stosunku do dzieci, co zostało wskazane wprost w art. 12 ust. 1 oraz motywie 58 RODO, tak aby mogło ono bez trudu zrozumieć dany przekaz[764]. Można przypuszczać, że część administratorów, chociażby z obawy przed nadmiernymi karami, przeprowadzi wśród różnych grup wiekowych testy porównawcze kilku wersji uprzednio sporządzonych komunikatów i w zależności od wyników – wprowadzi do obiegu te najbardziej zrozumiałe.

Niejasność formalna przekazywanej informacji jako ewentualna czynność naruszająca przesłankę legalności, może powodować wątpliwość czy obowiązek informacyjny został zrealizowany w taki sposób, aby administrator miał możliwość uniknięcia odpowiedzialności za naruszenie praw podmiotów danych w postępowaniach zainicjowanych, chociażby na podstawie art. 79 RODO, czy art. 83 ust. 5 lit. b) RODO. Stan ten można osiągnąć dzięki podejmowaniu odpowiednich do sytuacji działań i przestrzeganiu kryteriów jakościowych dotyczących formy, dostępności i sposobu wyrażania treści komunikatów wysyłanych do podmiotów danych.

4.2.3. Ryzyka na gruncie przepisów RODO związane z „prawem do bycia zapomnianym"

Każda działalność człowieka, zarówno ta indywidualna, jak i zinstytucjonalizowana pociąga za sobą szereg zjawisk, które można uznać za ryzykowne, a więc takie, które będą budzić obawy przed pojawieniem się negatywnych skutków. Ryzyko jest zatem kombinacją możliwości zaistnienia zdarzeń, które będą oddziaływać na realizację wcześniej wyznaczonych celów. Z tego też powodu, ryzyko powinno być oceniane prawdopodobieństwem możliwości, a następnie skutków ich wystąpienia. Ryzyko, jak określają je wytyczne Grupy Roboczej Art. 29, jest „scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka"[765]. Administrator danych osobowych powinien oszacować ryzyko i przeprowadzić jego analizę w sytuacjach tego wymagających już na etapie projektowania danej czynności.

[764] Należy zauważyć, że nie dotyczy to wszystkich dzieci, ale tych powyżej 13. roku życia, czyli mających przywilej udzielania samodzielnej zgody na przetwarzanie danych osobowych na podstawie art. 8 ust. 1 RODO, co oznacza, że w przypadku pozostałych dzieci komunikaty będą kierowane do ich dorosłych opiekunów.
[765] https://giodo.gov.pl/261 [dostęp: 15.04.2018].

W unijnym Rozporządzeniu nie określono, co należy rozumieć pod pojęciem ryzyka. RODO wskazuje jedynie, jak rozumieć ryzyko w kontekście praw i wolności osób, mając na uwadze skutki ich naruszenia. W RODO, zgodnie z Motywem 75, do ryzyka zaliczono dyskryminację, kradzież lub oszustwo z wykorzystaniem tożsamości, stratę finansową, naruszenie dobrego imienia czy poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnione odwrócenie pseudonimizacji, a także inną znaczną szkodę gospodarczą lub społeczną. Lista ta stanowi katalog otwarty, posłużono się tylko przykładami.

Dyskryminacja może być warunkowana poprzez błędne dane. Informacje nie są zbierane od wszystkich po równo, mogą być niekompletne i powtarzać uprzedzenia. Z dyskryminacją związane jest profilowanie. Ryzyko powstaje, gdy z analizy danych statystycznych wynika, że u konkretnej osoby występuje nieznana dotąd cecha. Profilowanie zazwyczaj jest oparte na wzorach matematycznych, które nie uwzględniają trudnych sytuacji życiowych. Za przykład może posłużyć udzielanie pomocy osobom bezrobotnym przez Powiatowy Urząd Pracy. Kobiety, opiekujące się dziećmi lub osobami starszymi, dostawały mniej punktów, stąd też znajdowały się w gorszej kategorii, co blokowało im dostęp do niektórych instrumentów udzielanych przez tę instytucję[766].

Najprostsza definicja kradzieży tożsamości sprowadza się do nieuprawnionego wykorzystania danych osobowych w Internecie. Przestępcy próbują przechwycić informacje dotyczące rachunków bankowych, loginów do portali, poczty elektronicznej, czy instytucji finansowej. W tym celu wykorzystują kilka sposobów, m.in. *phishing* (podszywanie się pod inną osobę lub instytucję, by wyłudzić potrzebne informacje), wykorzystywanie złośliwego oprogramowania (konie trojańskie, programy szpiegujące), stosowanie taktyk typu *low-tech* (bez używania skomplikowanych systemów informatycznych)[767]. Skradzione dane można wykorzystać do wyrządzenia szkody majątkowej, np. wyłudzenia kredytu, zakupów w sieci, zmiany loginów konta bankowego. Czyn zabroniony może też polegać na zniszczeniu cudzego wizerunku lub dobrego imienia[768].

Uchybienie przepisom o ochronie danych osobowych stanowi naruszenie dobra osobistego, w tym dobrego imienia. Za przykład może posłużyć kazus, gdzie powód zawarł z pozwanym bankiem umowę kredytu konsumpcyjnego odnawialnego. Umowa ta uprawniała stronę pozwaną do przekazania instytucjom kredytowym informacji o powstałych na jej

[766] K. Żaczkiewicz-Zborska, *Komputer może dyskryminować, a RODO temu zapobiega,* [dostęp: 13.02.2018] https://www.prawo.pl/prawnicy-sady/komputer-moze-dyskryminowac-a-rodo-temu-zapobiega,73866.html.
[767] *Kradzież tożsamości vs. oszustwo tożsamościowe,* [dostęp: 14.05.2019] https://ochronatozsamosci.pl/blog/kradziez-tozsamosci-vs-oszustwo-tozsamosciowe-o35gc3-one.html.
[768] *Kradzież danych osobowych w Internecie,* [dostęp: 13.04.2023] https://lexdigital.pl/kradziez-danych-osobowych-w-internecie.

podstawie zobowiązaniach finansowych za pośrednictwem Biura Informacji Kredytowej. Powód wypowiedział umowę i uregulował dług. Bank nie poinformował jednak BIK-u o wygaśnięciu zobowiązania, co spowodowało, że powód nadal figurował w systemie jako dłużnik pozwanego. W związku z tym, powodowi odmówiono udzielenia kredytu w innym banku na zakup sprzętu komputerowego. Powód zwrócił się do pozwanego z prośbą o przekazanie stosownej informacji do Biura Informacji Kredytowej, skutkiem czego było usunięcie informacji o zadłużeniu powoda. Sąd Najwyższy w wyroku z dnia 11 lutego 2015 r. wskazał, że „naruszenie przez pozwanego obowiązków wynikających z przepisów ustawy o ochronie danych osobowych spowodowało, że niezaktualizowane dane przez kilkumiesięczny okres prezentowały powoda w kontaktach z bankami jako osobę niedającą gwarancji rzetelnego wywiązywania się z zobowiązań kredytowych, co przełożyło się na odmowę udzielania mu kredytu przez banki". W ocenie Sądu Najwyższego, ograniczenie dostępu do usług kredytowych „w wyniku wytworzenia obrazu powoda jako niewiarygodnego klienta, naruszało jego godność, narażając go na traktowanie przez banki jako osoby o wątpliwej wiarygodności i niezrozumiałe dla niego odmowy udzielenia kredytu"[769]. Stanowisko to poparto również w wyroku Sądu Apelacyjnego w Warszawie z dnia 29 marca 2018 r., gdzie zwrócono uwagę na to, że „jeżeli w okresie kilku miesięcy w BIK-u ujawnione były nieaktualne dane, które mogły podważać wiarygodność powoda jako uczciwego klienta banków, to mogą być odbierane w sposób wskazujący na nieposzanowanie dóbr osobistych powoda, jak godność i dobre imię"[770]. Argumentacja ta jest nadal aktualna po wejściu w życie przepisów Rozporządzenia oraz ustawy o ochronie danych osobowych z 2018 roku.

Naruszenie poufności danych oznacza niedopuszczalne bądź przypadkowe ujawnienie lub dostęp do danych osobowych, np. wysłanie wiadomości e-mail z załączonymi danymi osobowymi do nieuprawnionego adresata[771].

Kolejnym ryzykiem jest ryzyko finansowe. Sprowadza się do ewentualnej sytuacji, w której dochodzi do utraty pieniędzy albo cennych aktywów. Ryzyko to nie polega na rzeczywistej stracie, ale odnosi się do tego, co finalnie można utracić. Proces zabezpieczenia się przed tym problemem określa się angielskim *risk management*, czyli zarządzanie

[769] Wyrok SN z dnia 11 lutego 2015 r., sygn. akt: I CSK 868/1426, LEX nr 1677121.
[770] Wyrok SA w Warszawie z dnia 29 marca 2018 r., sygn. akt: I ACa 2267/15, LEX nr 2466241.
[771] M.A. Bernacka, *Naruszenie ochrony danych osobowych,* [dostęp: 24.06.2022] https://www.parp.gov.pl/component/content/article/81837:naruszenie-ochrony-danych-osobowych.

ryzykiem[772].

Ostatnim z ważniejszych i jednym z najbardziej zagrażających ryzyk jest nieuprawnione odwrócenie pseudonimizacji. Pseudonimizacja to proces odwracalny, polegający na odłączeniu tożsamości osoby od danych, które jej dotyczą. Proces ten polega na zamianie na pseudonim jednego identyfikatora osobistego lub kilku, np. imienia, adresu e-mail, numeru PESEL. Celami pseudonimizacji są ukrycie prawdziwej tożsamości podmiotu danych, utrudnienie możliwości powiązania danych z różnych domen, minimalizacja danych i ograniczenie dostępu osobom, którym wystarczy pseudonim, zagwarantowanie prawidłowości danych, takich jak kody kreskowe, kody QR. Pseudonimy zatem nie powinny pozwalać na odwrócenie pseudonimizacji przez innego administratora danych osobowych tak, aby zataić pierwotne identyfikatory. Nie powinno dojść także do reprodukcji pseudonimów w prosty sposób, tak aby uniknąć wykorzystania identycznych pseudonimów w różnych domenach[773].

Wykonywanie obowiązków odnoszących się do realizacji „prawa do bycia zapomnianym" przez administratora wiąże się z kolejnymi obciążeniami dla przedsiębiorców. Z powodu bariery technologicznej i społecznej podważana jest efektywność tego uprawnienia[774]. Już sam kształt „prawa do bycia zapomnianym" zdaje się być kontrowersyjny w kontekście fundamentalnych praw i wolności, a zwłaszcza, gdy bierze się pod uwagę wolność wypowiedzi i dostępu do informacji. Artykuł 17 RODO pozostawia „prawo do bycia zapomnianym" niedoprecyzowane. Nie zostały wyznaczone dokładne procedury usuwania danych oraz informowania podmiotów trzecich o skorzystaniu przez podmiot danych z „prawa do bycia zapomnianym". To, w jaki sposób powyższe zjawisko wpływa na skorzystanie z „prawa do bycia zapomnianym" pokazuje kazus osoby, która zgłosiła na policję pożar. Nagranie z tego zgłoszenia, pomimo że znajdowały się tam pełne dane personalne i adresowe zawiadamiającej, trafiło do satyrycznych serwisów internetowych. Kobieta, której dobra osobiste zostały naruszone, w tym prawo do prywatności, wskutek ujawnienia nagrania, żądała jego usunięcia z portali internetowych. W toku zainicjowanego postępowania sądowego pojawiły się problemy związane z roszczeniem usunięcia treści

[772] *Ryzyko finansowe-dogłębne wyjaśnienie zagadnienia,* [dostęp: 28.10.2019] https://academy.binance.com/pl/articles/financial-risk-explained.
[773] *Pseudonimizacja-czym jest, jakie są jej cele i kiedy jest efektywna?,* [dostęp: 03.02.2020] https://odo24.pl/blog-post.pseudonimizacja-wytyczne-enisa-rzucaja-nowe-swiatlo-na-jej-uzytecznosc.
[774] M. Krzysztofek, *„Prawo do bycia zapomnianym" i inne aspekty prywatności…,* s. 33-34.

opublikowanych w sieci internetowej w oparciu o treść art. 24 k.c.[775].

Na pierwszym planie uwidoczniła się konieczność szczegółowego określenia żądania oraz konstrukcji sentencji orzeczenia w sposób kategoryczny, eliminujący pozostawienie swobody stronom[776]. Zobowiązanie do podjęcia czynności mających na celu usunięcie danych z portali internetowych, w tym zwrócenie się z należytym żądaniem do właścicieli lub administratorów portali nie czyni zadość tym wymogom. Judykatura nie dookreśliła czynności, które mogłyby pomóc w usunięciu skutków naruszenia dobra osobistego w Internecie. Ciężar szczegółowego sformułowania żądania, wystarczającego do jego realizacji, spoczywa na osobie, która chce skorzystać z „prawa do bycia zapomnianym". Z powodu braku ujednoliconych procedur, a także dostępności zwielokrotniania treści, precyzyjniejsze oświadczenie woli o chęci skorzystania z „prawa do bycia zapomnianym" jest utrudnione. W kontekście art. 17 RODO brak regulacji procedury usuwania danych może przesądzać o niskiej użyteczności praktycznej uprawnienia.

W przedmiotowej sprawie, rozważania były także skoncentrowane na zasadności uznania zachowań osób trzecich za przyczynę naruszenia dobra osobistego w oparciu o treść art. 24 k.c. przez stronę pozwaną. Ostatecznie stwierdzono, że dostępność treści godzącej w dobra osobiste skarżącej, nie jest następstwem jedynie bezprawnych działań naruszającego, ale wynika także z postępowania podmiotów trzecich, które uzyskały dostęp do treści wskutek jej pierwotnego upublicznienia. Sąd Najwyższy w wyroku z dnia 15 stycznia 2015 roku podniósł, że nie wolno uznać zachowań anonimowych osób trzecich, korzystających z Internetu za skutek naruszenia w myśl treści art. 24 k.c. Prowadzi to do wniosku, że żądanie podjęcia działań zmierzających do usunięcia treści z portali internetowych, na jakich pojawiło się nagranie, nie mieści się w granicach środków zmierzających do usunięcia skutków naruszenia w rozumieniu art. 24 k.c.

W świetle powyższego możliwe jest natomiast domaganie się, aby zobowiązać pozwanego do poinformowania zarządzających portalami internetowymi, że znajduje się na nich treść, która prawomocnym orzeczeniem sądowym została uznana za naruszającą dobra osobiste, czyli o charakterze bezprawnym. Powiadomienie to wyłączy możliwość powoływania się przez podmiot zarządzający portalem internetowym na ograniczenie

[775] Dotyczyły one dokładności żądania pozwu, precyzyjności rozstrzygnięcia o tym żądaniu, wskazania czynności, których może domagać się strona powodowa celem usunięcia skutków naruszenia jej dobra osobistego. Zob. Wyrok SN z dnia 14 stycznia 2015 r., sygn. akt: II CSK 747/13…
[776] Wyrok SN z dnia 19 stycznia 1982 r., sygn. akt: IV CR 500/01, OSNCP 1982, nr 8-9, poz. 123.

odpowiedzialności wynikające z art. 14 ust. 1 u.ś.u.d.e.[777]. Podobne rozwiązanie zostało ugruntowane w Rozporządzeniu nr 2016/679, przy czym z wyroku Sądu Najwyższego wynika, że to żądający usunięcia treści powinien wskazać portale, które mają zostać poinformowane o tym, że znajduje się na nich dana informacja, natomiast ustawodawca unijny w art. 17 ust. 2 RODO obowiązkiem ustalenia administratorów przetwarzających treść obciążył administratora, do którego najpierw zostało skierowane żądanie usunięcia treści. Operator powinien zastosować w stosunku do osoby, która chce skorzystać z tego uprawnienia blokowanie profilu, a więc poinformować ją o zastosowaniu procedury *notice and takedown*[778].

Obowiązek poinformowania administratorów przetwarzających dane o żądaniu ich usunięcia, może być uzależniony od możliwości technicznych i środków, jakimi dysponuje zobowiązany administrator. Taki obowiązek z jednej strony okazuje się być bardzo szeroko zakreślony i wymaga znaczących nakładów od administratora, a z drugiej strony bacząc na to, że został wyznaczony w nieostry sposób, może okazać się z praktycznego punktu widzenia niemożliwy do wykonania. Stąd też, pojawia się szereg problemów technicznych. Po pierwsze, z jakiego źródła administrator danych osobowych ma posiadać wiedzę, że informacje przez niego udostępnione zostały skopiowane przez inny podmiot. Kontrola nad zwielokrotnianiem treści wydaje się być bardzo utrudniona. Istnieje wiele różnych możliwości, które mogą prowadzić do rozpowszechniania się zbioru informacji[779]. Może to doprowadzić do powstania uszczerbku w postaci właśnie szkód majątkowych lub niemajątkowych osób fizycznych, utraty kontroli nad zgromadzonymi danymi, sfałszowania tożsamości czy naruszenia poufności[780]. Z tego też powodu, wykładnia art. 17 ust. 2 Rozporządzenia nie daje się pogodzić z założeniem racjonalności ustawodawcy. Czy zatem obowiązek administratora sprowadza się jedynie do poinformowania podmiotów, którym udzielił on zgody na skopiowanie danych? Najbardziej sensownym wydaje się poszukiwanie kopiujących przez administratora. Wobec tego, jakie działania musi podejmować administrator, aby można było uznać, że obowiązek z art. 17 ust. 2 RODO został

[777] Art. 14 ust. 1 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2024, poz. 1513, dalej: u.ś.u.d.e.) „Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych".
[778] Z ang. zawiadomienie o usunięciu.
[779] Sposobem powielania treści może być kopiowanie przy użyciu narzędzi elektronicznych, skorzystanie z aparatu fotograficznego, czy z czytnika pozwalającego na konwertowanie zdjęć, a nawet przepisywanie ręczne.
[780] J. Żołyński, *RODO. Prawo do zapomnienia…,* s. 241.

zrealizowany, pomimo braku wykrycia podmiotów, które przetwarzają dane osobowe pobrane z jego strony? Tak też zakres przedmiotowego obowiązku powinien być wyznaczony przy uwzględnieniu możliwości technologicznych, kosztów i postulatu proporcjonalności. W zależności od rodzaju danych osobowych, dopuszczalne jest różnicowanie poziomu ich ochrony i postawy administratora. Warto zauważyć pewną występującą tu zależność – w polskim porządku prawnym przyjęło się, że jeśli treść naruszająca dobro osoby została udostępniona w sposób umożliwiający dotarcie jej do nieograniczonego kręgu osób, to czynności mające doprowadzić do zaprzestania naruszeń, także powinny obejmować ten obszar. Innymi słowy, jeżeli osoba, której dane osobowe zostały udostępnione w sieci internetowej, skorzystała z „prawa do bycia zapomnianym", informacja o tym również powinna znaleźć się na stronie internetowej. W orzecznictwie został zaakcentowany pogląd, według którego „wymóg złożenia m.in. w odpowiedniej formie oświadczenia oznacza zachowanie adekwatności z uwzględnieniem m.in. miejsca i czasu dokonanego naruszenia dobra osobistego, a nie jest warunkowany oceną prawdopodobieństwa i szansy dotarcia do oświadczenia przez przeciętnego jego adresata oraz jego czasu i skłonności do lektury informacji niedostatecznie wyeksponowanych, choć opublikowanych w tożsamym miejscu, w którym doszło do publikacji inkryminowanych tekstów"[781]. Niemniej, taka interpretacja bierze się z braku umiejętności zrozumienia specyfiki funkcjonowania medium, ponieważ ilość osób, która mogła zapoznać się z materiałem zawierającym dane osobowe, a ilość osób, do których trafi informacja o skorzystaniu z „prawa do bycia zapomnianym" jest nieporównywalna. Administrator danych osobowych powinien pamiętać o swych obowiązkach w stosunku do danych osobowych, a więc o ryzyku ich wycieku. Bez odpowiedzi pozostają ponadto kwestie odnoszące się do zakresu zastosowania „prawa do bycia zapomnianym". Wątpliwe jest, czy obejmują portale społecznościowe, typu Facebook[782].

W uzupełnieniu unijnego Rozporządzenia, uregulowania polskiego prawa powinny nadawać państwowym organom nadzorczo-kontrolnym uprawnienie do ingerencji w sytuacji zaistnienia naruszenia „prawa do bycia zapomnianym". Rozpatrując zagadnienia ponoszenia ryzyka, należy mimo wszystko mieć też na uwadze postanowienia samego Rozporządzenia. Zgodnie z RODO to nie przepisy prawa powszechnie obowiązującego mają określać środki techniczne i organizacyjne wykorzystywane w celu zagwarantowania bezpieczeństwa przetwarzania danych osobowych, ale sami administratorzy bądź podmioty przetwarzające.

[781] Wyrok SN z dnia 19 maja 2011 r., sygn. akt: I CSK 497/10…
[782] Wyrok WSA w Warszawie z dnia 26 lutego 2009 r., sygn. akt: II SA/Wa 1685/08, LEX 519827.

W świetle regulacji RODO, eliminacją ryzyka jest ponadto przetwarzanie danych osobowych do celów innych niż cele, dla których dane te zostały zebrane, ale jedynie w przypadkach, gdy jest to zgodne z celami, w jakich te dane osobowe zostały pierwotnie zgromadzone. Co prawda, niektórych ryzyk nie da się całkowicie ominąć, niemniej jednak ich ocena pozwala na zwrócenie szczególnej uwagi i prowadzi do oszacowania ryzyka w analizowanym przedsięwzięciu. Ryzyko musi być oszacowane na podstawie obiektywnej oceny, gdzie stwierdza się, czy z operacjami przetwarzania danych wiąże się przeciętne ryzyko, czy też o wysokim stopniu[783].

4.3. Środki ochrony prawnej, zasady odpowiedzialności i administracyjne kary pieniężne za naruszenie „prawa do bycia zapomnianym"

4.3.1. Prawo do wniesienia skargi do organu nadzorczego

Jednym z mechanizmów prawnych, który ma służyć zagwarantowaniu i egzekwowaniu praw podmiotu danych jest skarga do organu nadzorczego. Legitymacja czynna, tj. prawo do wniesienia skargi do organu nadzorczego, przysługuje, wobec tego osobie, której ochroną objęte są dane osobowe. Podstawą wniesienia skargi jest subiektywne przekonanie, że proces przetwarzania danych osobowych osoby, której dotyczą jest niezgodny z przepisami Rozporządzenia unijnego. Skarga do organu nadzorczego nie jest ostatecznym środkiem prawnym chroniącym prawa danego podmiotu[784]. Osobie, której dane dotyczą przysługuje również zgodnie z art. 78 RODO prawo do posiadania skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego.

W praktyce można już zauważyć wykorzystywanie na terenie państw należących do Unii Europejskiej tego instrumentu prawnego w celu obrony swoich praw. Jako przykład może posłużyć sprawa, gdzie norweski pracownik złożył skargę do Urzędu Ochrony Danych na swojego pracodawcę, który automatycznie przesyłał e-maile. Pracodawca nakazał pracownikowi ustawienie przekazywania wiadomości ze swojej skrzynki pocztowej na wspólne konto firmowe. Jak argumentowano, miało to służyć względom operacyjnym. Po zbadaniu sprawy, organ nadzorczy wydał w dniu 13 maja 2021 roku decyzję, w której stwierdził, że firma nie posiada podstawy prawnej do żądania przesyłania wiadomości e-mail.

[783] Motyw 76 preambuły RODO.
[784] A. Mednis, *Prawo do wniesienia skargi do organu nadzorczego,* [w:] *Realizacja praw osób, których dane dotyczą, na podstawie rodo,* Wrocław 2017, s. 347-348.

Wskazał, iż odbyło się to z naruszeniem przepisów dotyczących dostępu pracodawcy do kont i innych materiałów elektronicznych. Firma nie opracowała również procedur dostępu do poczty elektronicznej. Norweski organ nadzorczy podniósł, że usprawnienie procedur może zapobiegać bezprawnemu dostępowi[785].

Zgodnie z art. 3 ust. 2 Ogólnego Rozporządzenia o Ochronie Danych, skarżącym może być obywatel państwa członkowskiego, jak i państwa trzeciego, ponieważ ochroną objęte są dane osób, które przebywają na terenie Unii Europejskiej. Osoba, której przysługuje prawo do wniesienia skargi, może również umocować do wykonania tego uprawnienia podmiot, organizację lub zrzeszenie niemających charakteru zarobkowego[786]. Instytucje te muszą jednak spełniać łącznie trzy cechy, a mianowicie być ustanowione zgodnie z prawem państwa członkowskiego, posiadać cele statutowe leżące w interesie publicznym oraz działać w dziedzinie ochrony praw i wolności osób, których dane dotyczą[787]. Z tego wynika, że osoby fizyczne nie mogą reprezentować podmiotu danych. Z kolei zaś, mając na uwadze inne rodzaje podmiotów i organizacji, to zdaje się, iż nie jest potrzebne posiadanie osobowości prawnej. Kraje członkowskie powinny przewidywać sytuacje, w których podmiot, organizacja lub zrzeszenie będą zamierzały złożyć w tym państwie skargę do organu nadzorczego bez stosownego upoważnienia, jeśli tylko uznają, że podczas procesu przetwarzania naruszone zostały prawa konkretnej osoby, np. „prawo do bycia zapomnianym".

Właściwość miejscowa organu, do którego skarga może zostać złożona, nie została w precyzyjny sposób określona. Art. 77 ust. 1 RODO reguluje, że skargę można wnieść do organu nadzorczego każdego państwa członkowskiego. Może być to organ właściwy ze względu na miejsce zwykłego pobytu podmiotu danych, miejsce pracy, ale też miejsce popełnienia naruszenia. Posłużenie się sformułowaniem „w szczególności" wskazuje na dowolność organu nadzorczego, do którego osoba, której dane dotyczą może wnieść skargę. Powinien jednak zaistnieć związek pomiędzy osobą bądź czynem a krajem, gdzie znajduje się siedziba wybranego organu nadzorczego. Taki sposób określenia jest przydatny w sytuacji skargi na podmiot, który nie ma jednostek organizacyjnych na terenie Unii Europejskiej. Pokrzywdzony będzie uprawniony do wniesienia skargi w państwie miejsca zamieszkania, pracy lub tam, gdzie w jego ocenie nastąpiło ewentualne naruszenie. Jeżeli pokrzywdzonym będzie osoba, mająca obywatelstwo państwa trzeciego, przebywająca na terenie Unii Europejskiej w celach np. turystycznych, to powinna kierować się ostatnim z wymienionych

[785] *Norwegian DPA: Company fined for illegal forwarding of e-mail,* [dostęp: 13.05.2021] https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-company-fined-illegal-forwarding-e-mail_pl.
[786] Ang. *not-for-profit body, organisation or association.*
[787] Art. 80 ust. 1 RODO.

kryteriów. Z drugiej strony, definicja organu, którego sprawa dotyczy może sugerować, iż skargę można wnieść w wybranym organie nadzorczym[788].

Złożenie skargi do danego organu nadzorczego nie jest tożsame z tym, że to właśnie ten organ będzie prowadził sprawę, której skarga dotyczy. Takie rozwiązanie jest wynikiem jednego z głównych założeń reformy prawa ochrony danych, sprowadzającego się do mechanizmu obsługi transgranicznych przedsiębiorstw przez jeden organ nadzorczy. Przedsiębiorstwa, które prowadziły działalność w wielu krajach Unii Europejskiej, zwłaszcza przy pomocy Internetu, i też w związku z tym przetwarzały dane osobowe, podlegały organom różnych państw członkowskich. Rozporządzenie nr 2016/679 wprowadziło jednolite zasady ochrony danych osobowych na terenie całej Unii Europejskiej. W pierwszym projekcie do RODO, Komisja zaproponowała punkt kompleksowej obsługi[789]. Finalnie, idea ta została zmodyfikowana i ostatecznie wprowadzono mechanizm kompleksowej współpracy[790].

Ilość wyjątków powoduje, że w praktyce dochodzi do sporów kompetencyjnych, które ma rozstrzygać nowo powołany organ, tzn. Europejska Rada Ochrony Danych. EROD nie jest uprawniona do rozwiązywania jakichkolwiek sporów, a jedynie tych, które odnoszą się do statusu organu wiodącego. W kontekście właściwości organu, który prowadzi postępowanie, w unijnym Rozporządzeniu prawodawca używa kilku różnych terminów. Organem nadzorczym, zgodnie z definicją z art. 4 pkt 21 RODO, jest co najmniej jeden niezależny organ publiczny, odpowiedzialny za ochronę podstawowych praw i wolności obywatelskich. Odrębną kwestią jest pojęcie organu nadzorczego, którego sprawa dotyczy. Takim organem staje się wtedy, gdy administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego albo proces przetwarzania wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, zamieszkujące w państwie członkowskim tego organu nadzorczego. Obok tych przesłanek, wymienia się jeszcze jeden powód, jakim jest wniesienie skargi.

W przepisach art. 55 Rozporządzenia i następnych wymieniono szereg czynników, które wpływają na właściwość organu. Najważniejszymi kryteriami, które bierze się pod uwagę, jest to, czy administrator lub podmiot przetwarzający ma jednostkę organizacyjną w jednym kraju członkowskim czy w kilku, oraz czy sprawa dotyczy przetwarzania

[788] A. Mednis, *Prawo do wniesienia skargi…,* s. 349.
[789] Ang. *one stop shop.*
[790] M. Piech, *One stop shop. Mechanizmy podejmowania decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE,* [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych,* red. G. Sibiga, Warszawa 2016, s. 82.

o charakterze jedynie lokalnym. Nie w każdej sytuacji czynniki te będą uwzględniane. Po pierwsze, gdy dane przetwarza organ publiczny, to właściwym organem nadzorczym państwa będzie ten, gdzie funkcjonuje ów organ. Po drugie, kiedy dane przetwarza podmiot prywatny zgodnie z art. 6 ust. 1 lit. c) RODO, tzn., jeżeli podstawą przetwarzania jest wykonanie obowiązku prawnego ciążącego na administratorze. A po trzecie, w sytuacji, gdy przetwarzanie jest wynikiem realizacji zadania wykonywanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi będącemu podmiotem prywatnym[791]. W motywie 45 preambuły RODO wskazuje się, że w obu przypadkach podstawę przetwarzania powinno stanowić prawo Unii Europejskiej lub prawo krajowe. Zadanie realizowane w interesie publicznym z praktycznego punktu widzenia będzie trudne do zidentyfikowania. Interes publiczny nie jest wyraźnie zaakcentowany w przepisach, jego zakres odczytuje się z wielu norm prawnych. W pozostałych przypadkach bierze się pod uwagę transgraniczny charakter przetwarzania oraz strukturę organizacyjną administratora lub podmiotu przetwarzającego.

Bez względu na regulacje konkretnych procedur, w unijnym Rozporządzeniu są zawarte ogólne zasady wzajemnej pomocy. Wzajemna pomoc obejmuje swym zakresem wnioski o udzielenie informacji oraz wnioski o przeprowadzenie kontroli i postępowań wyjaśniających[792]. Unijny prawodawca ustanawia nakaz współpracy pomiędzy organem wiodącym a organami nadzorczymi, których sprawa dotyczy, w celu wypracowania wspólnego stanowiska i wymiany wszelkich stosownych informacji. Organ wiodący opracowuje projekt decyzji. Sposób postępowania jest dość skomplikowany. Projekt decyzji należy przedłożyć innym organom, aby uzyskać ich opinię, a następnie uwzględnić ewentualne uwagi. Wyrażony w stosunku do projektu sprzeciw został zdefiniowany w art. 4 pkt 24 jako sprzeciw wobec projektu decyzji odnoszącej się do tego, czy doszło do naruszenia RODO, bądź czy planowane działanie w stosunku do administratora lub podmiotu przetwarzającego jest zgodne z przepisami Rozporządzenia. Sprzeciw musi wskazywać na ryzyko naruszenia podstawowych praw i wolności osób, których dane dotyczą. Wiodący organ nadzorczy może się przychylić do sprzeciwu wyrażonego przez inny organ nadzorczy, którego sprawa dotyczy. Jeżeli natomiast ma zastrzeżenia co do treści wniesionego sprzeciwu, to zobowiązany jest przekazać sprawę do Europejskiej Rady Ochrony Danych. Decyzja wydana przez EROD powinna odnosić się do wszystkich kwestii, które zostały poruszone

[791] Art. 6 ust. 1 lit. e) RODO.
[792] Zgodnie z art. 61 ust. 2 RODO, organ nadzorczy powinien udzielić informacji bez zbędnej zwłoki i nie później niż w terminie miesiąca od otrzymania wniosku od innego organu nadzorczego.

w sprzeciwie, a zwłaszcza rozstrzygać, czy doszło do naruszenia przepisów Rozporządzenia unijnego[793]. Decyzja nie kończy postępowania. Łącznie z uzasadnieniem, powinna zostać skierowana do wiodącego organu nadzorczego i wszystkich organów nadzorczych, których sprawa dotyczy. Przyjmują oni ostateczną decyzję na podstawie decyzji EROD. W chwili, gdy organ nadzorczy uzna, że istnieje nagła konieczność podjęcia działań w celu ochrony interesów osób, których dane dotyczą można zastosować tzw. tryb pilny. Do środków tymczasowych zalicza się np. nakaz ograniczenia przetwarzania danych osobowych[794].

Z tego powodu, że regulacje RODO nie określają procedury rozpatrywania skargi, istnieje konieczność stosowania krajowych przepisów proceduralnych, m.in. na podstawie ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku, w której Rozdział VII został poświęcony temu zagadnieniu[795].

4.3.2. Ochrona prawna przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu za naruszenie „prawa do bycia zapomnianym"

Celem art. 79 Rozporządzenia o Ochronie Danych Osobowych jest wzmocnienie ochrony prawnej osób fizycznych. Ten cel przesądza o treści całego RODO, co zostało wyrażone w art. 1 ust. 1 i 2 unijnego Rozporządzenia, a także w jego dalszych postanowieniach. W motywie 7 zwrócono uwagę na praktyczny aspekt ochrony danych osobowych, stanowiący, że osoby fizyczne powinny mieć zapewnioną kontrolę nad swoimi danymi osobowymi i uzyskać większe poczucie pewności prawa i jego stosowania w praktyce. Podkreślono, że aby ochrona danych osobowych w UE była efektywna, to należy wzmocnić prawa osób, których dane dotyczą. W motywie 59 preambuły RODO, europejski ustawodawca dostrzegł potrzebę przewidzenia procedur ułatwiających osobie, której dane dotyczą, realizację praw przysługujących jej na mocy RODO. Specyfika art. 79 RODO polega na tym, że wzmocnienie ochrony danych osobowych ma nastąpić przez wprowadzenie produktywnego sądowego środka ochrony prawnej, ale nie tożsamego dla wszystkich krajów członkowskich Unii Europejskiej, przy zachowaniu harmonizacji uregulowań krajowych,

[793] Nie jest do końca jasne, czy EROD ma zająć stanowisko w przedmiocie naruszenia RODO przez administratora lub podmiot przetwarzający, czy w projekcie decyzji. Z jednej strony ciężko mówić o naruszeniu regulacji w odniesieniu do projektu, zaś z drugiej, punktem wyjścia rozstrzygnięcia EROD jest sprzeciw wobec propozycji rozwiązań zaproponowanych w projekcie przez organ wiodący.

[794] Tryb pilny może polegać na przyjęciu środka tymczasowego na terenie konkretnego państwa w stosunku do administratora lub podmiotu przetwarzającego. Zob. A. Mednis, *Prawo do wniesienia skargi…,* s. 360.

[795] G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych-wybrane zagadnienia,* dodatek do „Monitora Prawniczego" 2016, nr 20, s. 19.

z poszanowaniem istniejących odrębności proceduralnych.

Regulacja dotycząca środków ochrony prawnej, razem z zagadnieniami proceduralnymi, ma charakter odesłania obligatoryjnego, potrzebnego do dostosowania prawa krajowego do RODO, jak również do ujednolicenia we wskazanym kierunku uregulowań przyjętych w państwach członkowskich, będących proceduralnym uzupełnieniem RODO. W takim znaczeniu treść odesłania powinna być wykładana bardzo rygorystycznie[796].

Z tego środka prawnego skorzystał m.in. użytkownik portalu pożyczkowego. Wystąpił do sądu z pozwem przeciwko spółce, która była właścicielem portalu, a jednocześnie administratorem danych osobowych (art. 4 RODO). Powód wskazał, że w dniu 14 marca 2020 roku otrzymał informację od pozwanej o rozpoczęciu automatycznego resetowania hasła dostępu do konta użytkownika, pomimo że resetowanie zabezpieczenia nie było zalecane przez spółkę. Po dwóch dniach, pozwana przekazała powodowi, że dane zapisane na jego koncie zostały ujawnione osobie trzeciej na skutek błędu popełnionego przez pracownika podmiotu, któremu powierzono przetwarzanie danych osobowych. Dane dotyczyły wniosku o pożyczkę, m.in. imienia i nazwiska, adresu e-mail, adresu zameldowania, miejsca urodzenia, numeru PESEL, NIP, numeru dowodu osobistego, numeru telefonu kontaktowego, paszportu, hasła oraz numeru rachunku bankowego. Sąd Okręgowy w Warszawie wywiódł, że bezspornym jest fakt, iż doszło do wycieku danych osobowych klientów posiadających konto na portalu pożyczkowym, zaś administratorem danych osobowych jest pozwana spółka. Zgodnie z art. 4 pkt 7 Rozporządzenia, za administratora można uznać osobę fizyczną, osobę prawną (pozwaną spółkę), organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych. Natomiast w pkt. 12 potwierdzono, że nieuprawnione ujawnienie lub dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych stanowi naruszenie ochrony danych osobowych[797].

Artykuł 79 ust. 1 unijnego Rozporządzenia[798] wprowadza sądowy środek prawny, ale bez zdecydowania o jego konkretnym kształcie. Sprowadza się to do tego, że w państwie członkowskim najpierw powinno nastąpić doprecyzowanie kształtu środka ochrony prawnej, a dopiero potem zastosowanie obowiązujących już przepisów proceduralnych. Unijny prawodawca w przepisach RODO nie definiuje pojęcia „sąd". Posiłkując się innymi

[796] *Tamże,* s. 16.
[797] Wyrok SO w Warszawie z dnia 7 lutego 2023 r., sygn. akt: III C 280/22, [dostęp: 29.03.2023] https://orzeczenia.warszawa.so.gov.pl/details/$N/154505000000903_III_C_000280_2022_Uz_2023-02-28_001.
[798] Każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna, że prawa przysługujące jej na mocy RODO zostały naruszone w wyniku procesu przetwarzania danych osobowych.

regulacjami europejskiego prawa procesowego przyjęto, iż w rozumieniu Rozporządzenia, sądem będą sądy państwa członkowskiego, z wyjątkiem sądów polubownych[799]. Kognicja sądów powszechnych gwarantuje skuteczność środka i możliwość jego przymusowego egzekwowania, co wypełnia oczekiwania europejskiego ustawodawcy[800].

Analizowany przepis usytuowany jest w rozdziale zatytułowanym „Środki ochrony prawnej, odpowiedzialność i sankcje". Poprzedzony jest m.in. regulacjami stanowiącymi o prawie do wniesienia skargi do organu nadzorczego. Art. 79 RODO stanowi zaś o skutecznym środku ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu. W świetle wykładni systemowej środek ten jest niezależny – zalicza się do samodzielnych środków ochrony prawnej przysługujących osobie fizycznej. Skorzystanie z tego środka nie wymaga uzyskania innych orzeczeń o charakterze administracyjnym lub sądowo-administracyjnym. Unijny prawodawca kreuje środek przysługujący do sądu jako odrębny od dostępnych administracyjnych lub pozasądowych środków ochrony prawnej. Można go porównać w polskim porządku krajowym ze środkiem przysługującym do sądu powszechnego. Środek ten podlega rozpoznaniu w sprawie cywilnej[801].

Ustawodawca krajowy dla realizacji przedmiotowego środka prawnego może wykorzystać obowiązujące przepisy proceduralne dotyczące rozpoznawania spraw w trybie procesowym. Za ukształtowaniem środka ochrony prawnej w porządku krajowym w trybie procesu przemawia sformułowanie w art. 79 RODO, wskazujące na to, że środek ten ma zostać wykorzystany przeciwko administratorowi lub podmiotowi przetwarzającemu. Harmonizacja ustawodawstw krajowych na najwyższym poziomie wymaga ścisłej interpretacji odesłania z art. 79 unijnego Rozporządzenia. Różnice występujące pomiędzy porządkami krajowymi nie powinny być przeszkodą w dochodzeniu roszczeń, co może mieć niebywałe znaczenie w sytuacji ochrony realizowanej w sporach o charakterze transgranicznym. Rozpatrzenie niniejszego środka prawnego może nastąpić w ramach procesowego postępowania rozpoznawczego i nie wymaga przygotowania odrębnej regulacji

[799] Motyw 11, 12 preambuły i art. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz. Urz. UE L 351 z 20.12.2012).

[800] Motyw 13 preambuły RODO stanowi między innymi o tym, że „aby zapewnić spójny stopień ochrony osób fizycznych w Unii oraz zapobiegać rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten sam poziom prawnie egzekwowalnych praw oraz obowiązków i zadań administratorów i podmiotów przetwarzających".

[801] Nie posiada charakteru karnego. Rozumowanie takie jest poparte odwołaniem się w motywie 147 preambuły RODO do europejskiego aktu normatywnego w przedmiocie jurysdykcji w sprawach cywilnych.

ustawowej.

W świetle regulacji materialnoprawnej RODO, dopuszczalne jest wniesienie powództwa o usunięcie danych osobowych. Osoba fizyczna, domagająca się ochrony prawnej w drodze powództwa wniesionego do sądu powszechnego, nie jest zobowiązana do udowodnienia winy administratora lub podmiotu przetwarzającego jej dane osobowe. Odpowiedzialność tych podmiotów została oparta na zasadzie bezprawności działania – obiektywnej niezgodności z prawem[802], co zbliża ochronę danych osobowych do instytucji ochrony dóbr osobistych[803]. Ciężar dowodu z art. 6 k.c. spoczywający na osobie fizycznej dochodzącej ochrony prawnej, jest ograniczony do wykazania sprzeczności postępowania strony przeciwnej z porządkiem prawnym krajowym i europejskim. Pozwany, w celu skutecznej obrony swoich praw, będzie musiał udowodnić, iż przetwarzanie danych osobowych trzeba uznać za zgodne z prawem, gdyż jest ono niezbędne dla ochrony interesu osoby, której dane te dotyczą. Sąd powszechny będzie zobligowany w każdej sytuacji ocenić, czy w czasie, w którym są gromadzone dane osobowe, osoba, której dane dotyczą posiada obiektywne przesłanki, aby domniemywać, że może nastąpić przetwarzanie danych w tym celu. Interesy i fundamentalne prawa osoby, której dane dotyczą mogą być nadrzędne w stosunku do interesu administratora danych, w szczególności, gdy dane osobowe są przetwarzane w sytuacji, w jakiej osoby, których dane dotyczą nie powinny spodziewać się dalszego przetwarzania, ponieważ brak jest rozsądnych przesłanek. Nieco odmiennie została ukształtowana zasada odpowiedzialności za szkodę, którą poniosła dana osoba na skutek przetwarzania jej danych osobowych w sposób naruszający przepisy RODO. Ustawodawca europejski wprowadził w tym wypadku zasadę odpowiedzialności na zasadzie winy, a oprócz tego wprowadził domniemanie zawinienia. Domniemanie to powinno zostać obalone przez stronę pozwaną[804].

Przyjmując, iż środek ochrony prawnej uregulowany w art. 79 unijnego Rozporządzenia jest powództwem cywilnym osoby fizycznej o prawa niemajątkowe i łącznie z nimi dochodzone roszczenie majątkowe odszkodowawcze lub tylko o jedno z nich, brakuje podstaw do przyjęcia odrębności w ukształtowaniu właściwości rzeczowej, funkcjonalnej i miejscowej powszechnego sądu krajowego. Zwracając uwagę na charakter przedmiotu

[802] O tym stanowi motyw 40 preambuły RODO: „aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie zgody osoby, której dane dotyczą lub na innej uzasadnionej podstawie przewidzianej prawem".

[803] A. Cisek, *Komentarz do art. 23-24,* [w:] *Kodeks cywilny. Komentarz do artykułów 1-534,* red. E. Gniewek, tom I, Warszawa 2004, s. 93.

[804] W. Kuberska, *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu,* [w:] *Realizacja praw osób, których dane dotyczą na podstawie rodo,* red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 391.

ochrony prawnej, sprawy te w pierwszej instancji powinny być zastrzeżone do wyłącznej właściwości sądów okręgowych. Dodatkowym argumentem przemawiającym za takim rozwiązaniem jest częsty spór przybierający postać sporu transgranicznego i prawnomaterialna regulacja dokonana w Rozporządzeniu unijnym, co wymaga większego doświadczenia zawodowego sądu rozpoznającego sprawę w I instancji. Konieczne zdaje się być jednoznaczne wskazanie przez ustawodawcę krajowego, że właściwość sądu okręgowego będzie zastrzeżona w sytuacji wystąpienia z powództwem o prawo niemajątkowe, prawo niemajątkowe wraz z prawem majątkowym, jak i prawo majątkowe bez względu na wartość przedmiotu sporu[805].

4.3.3. Prawo do odszkodowania

Za naruszenie przepisów w przedmiocie ochrony danych osobowych, prawodawca unijny zaproponował szczegółową regulację prawną. Ułatwia to osobom poszkodowanym dochodzenie roszczeń, przy czym należy pamiętać, iż poszerzono o podmiot przetwarzający krąg podmiotów odpowiedzialnych za szkodę, a z kolei ograniczono odpowiedzialność odszkodowawczą administratorów i podmiotów przetwarzających do zdarzeń, za które ponoszą winę. Obowiązuje jednak domniemanie winy, podlegające obaleniu. Regulacja RODO ma na celu uwzględniać jak najszerszy zakres szkody i zapewnić osobie poszkodowanej odszkodowanie w całości za poniesioną szkodę. Unijny prawodawca w art. 82 RODO wprowadził zasady odpowiedzialności odszkodowawczej w stosunku do administratora danych osobowych, jak i podmiotu przetwarzającego.

O odpowiedzialności odszkodowawczej można mówić, gdy administrator bądź podmiot przetwarzający niezgodnie z przepisami unijnego Rozporządzenia przetwarzają dane osobowe, a zatem dopuszczają się czynu bezprawnego (niedozwolonego). Odpowiedzialność odszkodowawcza obejmuje swym zasięgiem naruszenie nie tylko regulacji RODO, ale także aktów krajowych, które zostały wydane w celu pełnej realizacji postanowień Rozporządzenia. Chociaż, nawet, jeśli zostanie naruszony przepis polskiego prawa doprecyzowujący RODO, to reguły odpowiedzialności, tak czy inaczej, zostały zawarte w Rozporządzeniu w sposób wyczerpujący[806].

[805] Rozwiązaniem legislacyjnym mogłoby być dodanie w art. 17 Ustawy z dnia 17 listopada 1964 r.-Kodeks postępowania cywilnego (Dz. U. 2025, poz. 620, dalej: k.p.c.) kolejnego punktu o treści: „o roszczenia o ochronę danych osobowych wynikające z Rozporządzenia nr 2016/679".

[806] Odpowiedzialność w oparciu o przepisy polskiego kodeksu cywilnego zachodzi jedynie w przypadku kumulatywnego zbiegu roszczeń. Warto zaznaczyć, że w ramach naprawienia szkody, na podstawie RODO

Odpowiedzialność odszkodowawcza stała się przedmiotem rozstrzygnięć polskich sądów. W jednej ze spraw, powódka będąca asesorem komorniczym w pozwie skierowanym przeciwko Skarbowi Państwa – Naczelnemu Sądowi Administracyjnemu wniosła o zasądzenie od pozwanego na jej rzecz określonej kwoty pieniężnej z ustawowymi odsetkami za opóźnienie za brak dokonania anonimizacji danych osobowych w wyroku NSA z dnia 17 marca 2016 r., sygn. akt: III GSK 2320/14. Sąd Okręgowy w Warszawie zasądził od strony pozwanej na rzecz strony powodowej kwotę 20.000,00 zł wraz z ustawowymi odsetkami za opóźnienie. Przyjął, że podstawą rozstrzygnięcia jest naruszenie nie tylko przepisów RODO, ale także art. 24 k.c., bowiem doszło do naruszenia dóbr osobistych powódki. Sąd Okręgowy zgodził się z powódką, że jako osoba wykonująca szczególny zawód może być narażona na negatywne reakcje ze strony społeczeństwa. Opublikowanie treści orzeczenia, które kwestionuje nieposzlakowaną opinię powódki oraz odnosi się do okoliczności skreślenia jej z listy asesorów komorniczych, a co za tym idzie, udostępnienie tych informacji nieograniczonej liczbie odbiorców przez okres od 2016 do 2021 roku, naraziło powódkę na stres i ujemne przeżycia emocjonalne. Sąd zwrócił uwagę na okoliczność, że zasady doświadczenia życiowego nakazują przypuszczać, że wiele osób mogło zapoznać się z tym wyrokiem. Sama świadomość powódki, że taka sytuacja mogła mieć miejsce, nawet gdy w rzeczywistości nie miała, spowodowała u niej załamanie nerwowe. Powódka zdała sobie sprawę, że każdy mógł dowiedzieć się o jej historii zawodowej i o toczącym się przeciwko niej postępowaniu dyscyplinarnym w przeszłości. Oprócz dobrego imienia, naruszono także jej prawo do prywatności[807].

Odpowiedzialność administratora oraz podobnie wprowadzona po raz pierwszy w RODO, odpowiedzialność podmiotu przetwarzającego, została w znaczny sposób ograniczona względem obowiązującej uprzednio Dyrektywy 95/46/WE, a nawet pierwotnego projektu Rozporządzenia[808]. Wymienione podmioty mają możliwość uwolnienia się od odpowiedzialności, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które wywołało szkodę. Prawodawca unijny wprowadził jednak domniemanie winy, przenosząc ciężar dowodu na administratora i podmiot przetwarzający[809]. Ustanowienie domniemania wynika z faktu, że administrator danych osobowych posiada większą wiedzę

przysługuje tylko odszkodowanie, co oznacza, że nie można zastosować innych środków krajowych, chociażby jak przy szkodzie niematerialnej-roszczenie o zasądzenie odpowiedniej sumy pieniężnej na wskazany przez pokrzywdzonego cel społeczny.

[807] Wyrok SO w Warszawie z dnia 5 grudnia 2022 r., sygn. akt: XXV C 559/22, [dostęp:] https://orzeczenia.ms.gov.pl/content/$N/154505000007503_XXV_C_000559_2022_Uz_2022-12-05_002.

[808] Wniosek z 25 stycznia 2012 r. dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych…

[809] Przepisy k.c. wymagają, aby to pokrzywdzony wykazał winę naruszyciela.

o okolicznościach przetwarzania przez niego danych, w przeciwieństwie do osoby poszkodowanej.

W kontekście przesłanek odpowiedzialności odszkodowawczej za naruszenie zasad ochrony danych osobowych należy pochylić się nad zmianą sformułowania, tylko z pozoru niezbyt istotną, art. 82 ust. 3 RODO w stosunku do art. 23 ust. 2 Dyrektywy 95/46/WE. Art. 23 ust. 2 Dyrektywy wskazuje, że administrator może zostać zwolniony od odpowiedzialności w całości lub w części, jeśli udowodni, że nie jest odpowiedzialny za zdarzenie, które spowodowało powstanie szkody. Art. 82 ust. 3 RODO stanowi z kolei, że administrator lub podmiot przetwarzający zostaną zwolnieni z odpowiedzialności, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które spowodowało szkodę. Sformułowania te nawiązują do stopnia przyczynienia się do powstania i rozmiaru szkody.

Analiza przepisów Dyrektywy 95/46/WE i Rozporządzenia unijnego pozwala na konkluzję, że zasadniczo w celu zachowania ciągłości w zakresie ochrony danych osobowych, RODO w sposób dosłowny odtwarza postanowienia Dyrektywy wszędzie tam, gdzie sprawdziły się one w praktyce. Zatem, modyfikacja sformułowań wykorzystanych w RODO w kontekście instytucji przyczynienia się, powinna mieć doniosłe znaczenie prawne. Literalnie rzecz ujmując, na podstawie RODO, tylko udowodnienie, że administrator danych osobowych lub podmiot przetwarzający w żadnym wypadku nie ponosi winy za zdarzenie wywołujące szkodę, pozwala im na uniknięcie odpowiedzialności odszkodowawczej. Rozumowanie to, pomimo że w pełni odpowiada celowi RODO, jakim jest poprawa ochrony osób, których dane dotyczą, to jednak należy zauważyć, że jest to daleko idąca interpretacja. Przyjęcie takiego założenia oznacza odpowiedzialność tych dwóch podmiotów za całość szkody – częściowo na podstawie winy, a częściowo na zasadzie samego ryzyka, nawet jeżeli konkretne zdarzenie jest w minimalnej tylko części zawinione[810]. Aby wobec tego uchronić się od odpowiedzialności, nie wystarczy jedynie wykazać, że administrator lub podmiot przetwarzający nie ponosi w określonym zakresie winy za dane zdarzenie, ale co więcej, że nie ponosi jakiejkolwiek winy. Takie rozumienie tego przepisu znacząco utrudnia obronę, przy jednoczesnym zwiększeniu szansy podmiotu danych na uzyskanie odszkodowania[811].

Z prawem do odszkodowania nierozerwalnie związane jest pojęcie szkody.

[810] Przyjęcie takiego rozwiązania jest zgodne z motywem 146 preambuły RODO, gdzie zwraca się uwagę na zagwarantowanie całościowego odszkodowania osobie, której dane dotyczą, a ponadto z art. 82 ust. 4 RODO, w którym wprowadzono odpowiedzialność solidarną współprzetwarzających.

[811] A. Błaszczyńska, *Prawo do odszkodowania i odpowiedzialność,* [w:] *Realizacja praw osób, których dane dotyczą na podstawie rodo,* red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 415-416.

Prawodawca unijny w art. 82 ust. 1 RODO wskazuje, że obejmuje ona zarówno szkodę materialną, jak i niematerialną, którą w polskim porządku prawnym określa się mianem krzywdy[812]. Przysługujące dotychczas roszczenie o zasądzenie odpowiedniej sumy pieniężnej na wskazany cel społeczny przez pokrzywdzonego na zasadzie art. 448 k.c. nie przysługuje na gruncie przepisów RODO, a jedynie w ramach samodzielnego powództwa na podstawie przepisów kodeksu cywilnego. Roszczenie to spełniało funkcję represyjno-wychowawczą względem naruszyciela, dlatego można to uznać za pewien słaby punkt unijnej regulacji[813].

W zakresie interpretacji normatywnej pojęcia szkody, kluczowe znaczenie ma motyw 146 preambuły RODO. Zgodnie z jego treścią, podmiotowi danych powinno przysługiwać pełne i skuteczne odszkodowanie za poniesione szkody. Terminologię związaną ze szkodą należy interpretować *sensu largo* w świetle orzecznictwa Trybunału Sprawiedliwości. Oznacza to, że bierze się pod uwagę nie tylko orzecznictwo TSUE odnoszące się do odszkodowania za naruszenie zasad ochrony danych osobowych, ale wszelkie orzecznictwo, gdzie TSUE wypowiadał się w przedmiocie szkody[814]. Może to wynikać z faktu, iż w unijnym porządku prawnym brakuje generalnych zasad odpowiedzialności odszkodowawczej, w przeciwieństwie do porządków prawnych poszczególnych krajów Unii Europejskiej[815]. Niemniej, pojęcie to podlega także ograniczeniom wynikającym z orzecznictwa TSUE. Należy je zawęzić, jeżeli odmówiono określonemu uszczerbkowi przymiotu szkody i jednocześnie w żadnym innym orzeczeniu nie dokonano włączenia tego typu uszczerbku do pojęcia szkody. Zdekodowanie tego pojęcia jest niezwykle skomplikowanym zadaniem. Treść tego motywu nadaje orzecznictwu TSUE prawotwórczą moc[816]. Przyznanie tego charakteru może spowodować poważne wątpliwości dotyczące treści obowiązujących w danym czasie norm, bowiem może dojść do sytuacji, że później powstałe orzeczenie wyeliminuje z zakresu pojęcia szkody określony uszczerbek. Ustanowiona przepisem norma prawna powinna mieć charakter stały. Co najwyżej, może zmieniać się rozumienie tego przepisu[817]. Wartym rozważenia zagadnieniem jest uregulowanie wprost przez prawodawcę unijnego podstawowych elementów definiujących pojęcie szkody. Można

[812] Pojęcie zadośćuczynienia za doznaną krzywdę należy zastąpić pojęciem odszkodowania za poniesioną szkodę niematerialną.
[813] J. Gudowski, *Komentarz do kodeksu cywilnego. Księga trzecia. Zobowiązania,* red. G. Bieniek, t. 2, Warszawa 2011, s. 864.
[814] Chodzi o całokształt dorobku Trybunału Sprawiedliwości Unii Europejskiej w tym zakresie, także sprzed wejścia w życie przepisów RODO.
[815] D. Kornobis-Romanowska, J. Łacny, A. Wróbel, *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz,* t. 3, Warszawa 2012, s. 156.
[816] P. Marcisz, *Koncepcja tworzenia prawa przez Trybunał Sprawiedliwości Unii Europejskiej,* Warszawa 2015, s. 99.
[817] *Tamże.*

wskazać, że szkoda obejmuje zarówno stratę[818], jak i utracone korzyści[819]. Zapewne okazałoby się, że nie jest to idealne rozwiązanie, niemniej potrzeba każdorazowego badania orzecznictwa TSUE w kontekście treści normatywnej pojęcia szkody przysparza nieco więcej kłopotów[820].

Obowiązującą regułą, również na gruncie przepisów Rozporządzenia unijnego, jest wykazanie szkody przez poszkodowanego, zarówno co do zasady, jak i co do wysokości. Domniemanie ułatwiające dochodzenie odszkodowania jest związane wyłącznie z winą administratora lub podmiotu przetwarzającego. Rozwiązanie to ma charakter uniwersalny i nie odbiega od dotychczasowego stanu prawnego w polskim porządku prawnym, a nawet w Dyrektywie 95/46/WE. W motywie 146 wskazano także, że prawo do odszkodowania, które przysługuje na podstawie RODO, nie ma wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii Europejskiej lub prawa kraju członkowskiego. Oznacza to dopuszczalność kumulatywnego zbiegu roszczeń[821].

Z uwagi na okoliczność, że Rozporządzenie unijne rozszerza względem Dyrektywy 95/46/WE krąg podmiotów odpowiedzialnych odszkodowawczo, dzięki ustanowieniu odpowiedzialności podmiotu przetwarzającego, konieczne jest rozdzielenie odpowiedzialności pomiędzy tym podmiotem a administratorem danych osobowych. Podmiot przetwarzający przetwarza dane osobowe w imieniu ich administratora, toteż jego odpowiedzialność musiała zostać zawężona. Na podstawie art. 82 ust. 2 RODO, każdy administrator odpowiada za szkody spowodowane przetwarzaniem naruszającym przepisy Rozporządzenia, zaś podmiot przetwarzający tylko wtedy, gdy nie dopełnił obowiązków, które na niego nałożono, albo gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew takim instrukcjom[822]. Niezależnie od tego, odpowiedzialność odszkodowawcza podmiotu przetwarzającego zaktualizuje się także w momencie naruszenia instrukcji administratora, ale jedynie tych zgodnych z prawem. To oznacza, *a contrario*, że należyte wykonywanie przez podmiot przetwarzający niezgodnych z przepisami prawa instrukcji administratora nie może powodować odpowiedzialności podmiotu przetwarzającego. Działanie naruszające zgodne z prawem instrukcje administratora może polegać zarówno na działaniu poza nimi, a zatem przekroczeniu zakresu instrukcji w sposób

[818] Łac. *damnum emergens.*
[819] Łac. *lucrum cessans.*
[820] A. Błaszczyńska, *Prawo do odszkodowania…,* s. 419.
[821] W polskim porządku prawnym należy uwzględnić ewentualną dopuszczalność zbiegu roszczeń z RODO z tymi, które wynikają z przepisów o ochronie dóbr osobistych. Zdaje się jednak, że stosowanie przepisów k.c. jest mniej korzystne dla poszkodowanego z uwagi na wykazanie przesłanki winy.
[822] Z zakresu jego odpowiedzialności będzie zatem wyłączone naruszenie obowiązków, które ciążą wyłącznie na administratorze.

bezprawny, jak i na działaniu w sposób sprzeczny z instrukcjami. Wobec tego, ograniczenia odpowiedzialności podmiotu przetwarzającego są więc daleko idące. Niebagatelne znaczenie ma kwestia współprzetwarzania i odpowiedzialności poszczególnych podmiotów biorących udział w tym procesie. W tym przypadku wprowadzono instytucję solidarności z możliwością dochodzenia regresu od pozostałych współprzetwarzających. W rezultacie, ma to zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

4.3.4. Procedura nakładania przez organ nadzorczy administracyjnych kar pieniężnych jako skutek naruszenia „prawa do bycia zapomnianym"

Każdy podmiot danych posiada uprawnienie do ochrony jego danych osobowych. Na straży tego prawa czuwa organ nadzorczy. Stosowanie administracyjnych kar pieniężnych jest jednym z praw przysługujących organowi nadzorczemu. Nakładane są one samodzielnie bądź z pozostałymi środkami naprawczymi, w zależności od okoliczności każdego indywidualnego przypadku. Egzekwowanie prawa do nakładania kar przez organ nadzorczy podlega kontroli sądowej[823].

Jednym z przykładów jest sytuacja, gdzie na stronie internetowej wyświetlano pełne adresy, a czasem nawet numery telefonów komórkowych osób, które nie wiedziały, w jaki sposób ich dane umieszczano na międzynarodowej platformie o nazwie Locatefamily.com, służącej do odnajdywania członków rodziny, z jakimi utracono kontakt. Każdy, kto chciał usunąć swoje dane z tej witryny, nie mógł tego zrobić, ponieważ platforma nie posiadała swojego przedstawiciela w UE, co stanowi naruszenie RODO. W związku z tym, decyzją z dnia 12 maja 2021 roku holenderski organ nadzorczy nałożył na Locatefamily.com karę pieniężną w kwocie 525 tysięcy Euro[824].

Administracyjna kara pieniężna w każdym indywidualnym przypadku musi być skuteczna, proporcjonalna i odstraszająca. Kryteria te mają ogólny charakter. Powinny być brane pod uwagę łącznie z okolicznościami każdego przypadku, zarówno w kwestii podjęcia samej decyzji w przedmiocie zastosowania kary pieniężnej, jak też jej wysokości. Kara, która nie spełnia przewidzianych wymogów z art. 83 ust. 1 RODO pozostaje sprzeczna z Rozporządzeniem. Grupa Robocza Art. 29 wskazywała, że dokonanie oceny tego, co jest skuteczne, proporcjonalne, a co odstraszające musi uwzględniać cel wybranego środka

[823] https://omnimodo.com.pl/ogolne-warunki-nakladania-administracyjnych-kar-pienieznych.
[824] *Dutch DPA imposes fine of €525,000 on Locatefamily.com,* [dostęp: 12.05.2021] https://edpb.europa.eu/news/national-news/2021/dutch-dpa-imposes-fine-eu525000-locatefamilycom_pl.

naprawczego, jakim jest przywrócenie zgodności z przepisami prawa lub ukaranie za bezprawne zachowanie, jak też oba te cele jednocześnie[825]. Zamierzeniem nie jest traktowanie kar pieniężnych jako ostateczności, czy też powstrzymywanie się od ich stosowania, lecz nakładanie ich w taki sposób, żeby uniemożliwiały podważanie ich skuteczności jako narzędzia do osiągnięcia powyżej wymienionych celów[826]. O skuteczności sankcji można mówić, jeżeli pozwala osiągnąć cel, dla którego ją wprowadzono, natomiast o proporcjonalności, jeśli nie przekracza progu dolegliwości określonego poprzez uwzględnienie okoliczności danego przypadku. Sankcja jest z kolei odstraszająca, jeśli realizuje względy prewencji indywidualnej i generalnej, czyli nie pochwala takiego postępowania, które może być uznane przez społeczeństwo, jak też przez samego adresata sankcji za naruszenie[827].

Niezmienną zasadą jest to, że stosowanie administracyjnych kar pieniężnych musi odbywać się zgodnie z zasadą proporcjonalności, według której środki stosowane w prawie Unii Europejskiej powinny być proporcjonalne do celów, dla których są stosowane[828]. Administracyjne kary pieniężne powinny być nakładane w wysokości proporcjonalnej do wagi stwierdzonych naruszeń przepisów RODO. Analiza decyzji Prezesa Urzędu Ochrony Danych Osobowych (UODO)[829] nakładających administracyjną karę pieniężną pozwala wysnuć wniosek, że spełnienie wymogu proporcjonalności takich kar przysparza organowi kłopotów[830], choć większym problemem zdaje się być samo egzekwowanie obowiązku zapłaty nałożonej kary pieniężnej. Łukasz Wojciechowski zwrócił się w trybie art. 61 ustawy zasadniczej z wnioskiem do PUODO o udzielenie informacji publicznej w zakresie nakładania administracyjnych kar pieniężnych na podmioty zobowiązane do ich uiszczenia.

---

[825] Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów Rozporządzenia nr 2016/679*, przyjęte w dniu 03 października 2017 r., WP 253.

[826] *Tamże.*

[827] Wyrok TSUE z dnia 10 kwietnia 1984 r. w sprawie *Sabine von Colson and Elisabeth Kamann przeciwko Land Nordrhein-Westfalen,* sygn. akt: C-14/83, EU:C:1984:153.

[828] Oznacza to, że muszą być odpowiednie, współmierne i niezbędne. Zob. Wyrok TSUE z dnia 24 września 1985 r. w sprawie *The Queen, ex parte E.D.&F.Man (Sugar) Ltd przeciwko Intervention Board for Agricultural Produce (IBAP),* sygn. akt: 181/84, EU:C:1985:359.

[829] Na podstawie Motywu 117 Rozporządzenia „zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, uprawnionych do wypełniania zadań i wykonywania uprawnień w sposób całkowicie niezależny". Kraje członkowskie mają prawo ustanowić niezależny aparat państwowy, nadzorujący przestrzeganie przepisów Rozporządzenia unijnego.

[830] Np. Prezes Urzędu Ochrony Danych Osobowych nałożył karę pieniężną w maksymalnej wysokości (tj. w kwocie 100.000,00 zł) na Głównego Geodetę Kraju za udostępnienie danych osobowych na portalu internetowym bez podstawy prawnej, a także na Krajową Szkołę Sądownictwa i Prokuratury za wyciek danych osobowych w ilości ponad 50.000,00. Zob. Decyzja PUODO z dnia 24 sierpnia 2020 r., znak sprawy: DKN.5112.13.2020, [dostęp: 21.02.2021], https://uodo.gov.pl/decyzje/DKN.5112.13.2020; Decyzja PUODO z dnia 11 lutego 2021 r., znak sprawy: DKN.5130.2024.2020, [dostęp: 19.02.2021], https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020.

Przedmiotem rozważań było poszukiwanie odpowiedzi na pytania, na ile podmiotów i na jaką łączną kwotę PUODO nałożył kary pieniężne, począwszy od dnia 25 maja 2018 roku, ile podmiotów faktycznie uregulowało tę kwotę oraz ile z nich skorzystało z możliwości wniesienia odwołania albo złożenia skargi do sądu administracyjnego. W odpowiedzi na wniosek, Prezes Urzędu Ochrony Danych Osobowych wskazał, że na dzień 31 lipca 2022 roku, 44 podmioty zostały ukarane na kwotę wynoszącą 15 551 891,70 zł łącznie. Karę pieniężną zapłaciło jedynie 8 podmiotów. Uregulowana suma wyniosła 365 720,44 zł. Z przysługujących środków ochrony prawnej skorzystały 22 podmioty[831].

Odwołując się do innego przepisu unijnego Rozporządzenia, a mianowicie do art. 58 ust. 6 zd. 1, każde państwo członkowskie może postanowić w swoich przepisach krajowych, że jego organowi nadzorczemu przysługują również inne uprawnienia niż te wymienione w przepisach RODO. Posługując się wykładnią literalną, zawężającą art. 83 ust. 2 zd. 1 RODO, należy zauważyć, że powyższym uprawnieniom wprowadzonym przez krajowe porządki prawne, nie mogą towarzyszyć sankcje w postaci kar pieniężnych, jak też kary pieniężne nie mogą stanowić zamienników środków prawnych, wynikających z tych dodatkowych uprawnień organów nadzorczych. Chodzi więc o zastosowanie kar oprócz lub zamiast środków prawnych, które stanowią odzwierciedlenie uprawnień naprawczych organów nadzorczych. Kary pieniężne mogą zatem towarzyszyć bądź zastąpić m.in. nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych działaniach odbiorców.

Ogólne Rozporządzenie o Ochronie Danych Osobowych posiada otwarty katalog okoliczności, na które organ nadzorczy zobowiązany jest zwracać uwagę w każdym indywidualnym przypadku. Zostały one uwzględnione w art. 83 ust. 2 RODO. Podzielono je na działania lub zaniechania podmiotu w ramach konkretnej sprawy i ich skutków dla osób poszkodowanych, kategorie naruszonych danych osobowych, stopień współpracy z organem nadzorczym i uprzednią działalność podmiotu. W ramach pierwszej grupy okoliczności wymienia się umyślny lub nieumyślny charakter naruszenia. Grupa Robocza Art. 29 w Wytycznych WP 253[832] wskazała, że umyślne naruszenia są znacznie poważniejsze od tych o charakterze nieumyślnym, co w rezultacie prowadzi do częstszego nakładania administracyjnych kar pieniężnych[833]. Odnośnie do drugiej grupy okoliczności[834], Grupa

[831] Ł. Wojciechowski, *Kary RODO nie działają,* [dostęp: 04.09.2022] https://statuo.pl/2022/09/04/kary-rodo-nie-dzialaja/.
[832] Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych…*
[833] Okolicznością, która przybiera postać umyślnych naruszeń może być niezgodne z prawem przetwarzanie danych osobowych wbrew opinii inspektora ochrony danych lub pozostając w sprzeczności z istniejącymi

Robocza Art. 29 wyjaśniła, że chodzi zwłaszcza o przybliżenie, jakich danych dotyczy naruszenie, m.in. danych pozwalających na bezpośrednią lub pośrednią identyfikację danych, których rozpowszechnienie spowoduje bezpośrednią szkodę, bądź zagrożenie osób, czy też danych dostępnych bez technicznych zabezpieczeń lub zaszyfrowanych.

W art. 83 RODO przewidziano trzy rodzaje kar pieniężnych i dwa progi ich wysokości, z czego dwa rodzaje, tj. wyższa i niższa mają charakter samoistny, a ich maksymalna wysokość jest uzależniona od rodzaju stwierdzonego przez organ naruszenia. Trzeci rodzaj kary pieniężnej jest następczy wobec wcześniej już zastosowanego przez organ środka prawnego naprawczego z art. 58 ust. 2 RODO. Na gruncie RODO wyodrębniono karę niesamoistną, samoistną niższą i samoistną wyższą.

Prezes Urzędu Ochrony Danych Osobowych (PUODO) nakłada na administratora, naruszającego „prawo do bycia zapomnianym" karę finansową w drodze decyzji[835]. Karę uiszcza się w terminie 14 dni, licząc od dnia upływu terminu na wniesienie skargi lub od dnia uprawomocnienia się orzeczenia sądu administracyjnego. Zgodnie z uzasadnionym wnioskiem, można odroczyć termin płatności kary pieniężnej, czy też rozłożyć ją na raty, jeśli przemawia za tym ważny interes wnioskodawcy. Rozstrzygnięcie w tym przedmiocie następuje w drodze postanowienia.

4.4. Obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych

4.4.1. Polityka bezpieczeństwa zgodnie z przepisami RODO

Administrator danych osobowych musi tak prowadzić swoją działalność i stosować środki bezpieczeństwa (techniczne oraz organizacyjne), aby chronić w jak najlepszy sposób dane osobowe przez siebie przetwarzane. W tym celu należy przygotować wewnętrzną dokumentację, zawierającą sposób postępowania w ramach przetwarzania danych osobowych. Przepisy RODO nie nakładają na administratorów obowiązku prowadzenia

---

regułami. Jednym z przykładów takich działań według Grupy Roboczej Art. 29 jest handel danymi osobowymi w celach marketingowych, a mianowicie sprzedaż danych jako wybranych bez sprawdzenia poglądów, ale też ignorując poglądy osób, których dane dotyczą w kontekście sposobu użycia tych danych.

[834] Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych…*

[835] Decyzją PUODO z dnia 16 października 2019 r., znak sprawy: ZSPR.421.7.2019, [dostęp:] https://uodo.gov.pl/decyzje/ZSPR.421.7.2019, nałożono na ClickQuickNow sp. z o.o. z/s w Warszawie karę pieniężną w wysokości ponad 200 tys. zł za stwierdzenie naruszenia art. 17 ust. 1 lit. b) Rozporządzenia nr 2016/679. Zob. M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne,* Warszawa 2020, s. 139.

polityki bezpieczeństwa i instrukcji zarządzania[836]. W motywie 78 unijnego Rozporządzenia wskazano, że „aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych".

Na definicję polityki bezpieczeństwa składa się katalog zasad regulujących sposób zarządzania, ochrony i rozpowszechniania danych osobowych[837]. Punktem wyjścia jest art. 24 ust. 2 unijnego Rozporządzenia. Wymienia on wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających zgodność przetwarzania danych osobowych z RODO. W sytuacji kontroli, przedstawienie sporządzonej polityki bezpieczeństwa może okazać się bardzo pomocne. Wewnętrzna polityka bezpieczeństwa jest z pewnością znana każdej osobie fizycznej prowadzącej jednoosobową działalność gospodarczą. Powinność posiadania odpowiedniej dokumentacji, w tym polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, wynikała wprost z uchylonych przepisów u.o.d.o. z 1997 roku. Określone wówczas reguły przydały się w nowym porządku prawnym w zakresie ochrony danych osobowych, jednak wymagały nielicznych aktualizacji i poprawek celem dostosowania do uregulowań wprost z nowego Rozporządzenia.

Polityka bezpieczeństwa powinna być oparta na czterech filarach. Bez znaczenia jest to, czy będzie ona dopiero tworzona, czy jedynie aktualizowana. Te podstawowe filary to nic innego jak zgodność z zasadą *privacy by design*[838], *privacy by default*[839], proporcjonalność wobec czynności przetwarzania danych oraz klarowność języka, którym zostanie scharakteryzowana.

Pierwsza z wymienionych zasad wiąże się ściśle z przyszłościowym myśleniem. Administrator danych osobowych jest niewątpliwie zobowiązany zastosować środki techniczne oraz organizacyjne, które należy uznać za adekwatne do ryzyka naruszenia praw i wolności osób objętych procesem przetwarzania. Powinien to zrobić już w fazie wyboru technologii, dostawcy i procesu przetwarzania, jak również w toku jego trwania. Głównym założeniem tej zasady jest zabezpieczenie przetwarzania oraz zagwarantowanie jego całkowitej legalności. Oprócz tego, do celów tej zasady zalicza się minimalizację wiedzy

[836] A. Sztuwe, *Polityka bezpieczeństwa zgodnie z RODO-czy trzeba ją nadal prowadzić?,* [dostęp: 16.04.2018] https://www.poradyodo.pl/aktualnosci-rodo/polityka-bezpieczenstwa-zgodnie-z-rodo-czy-trzeba-ja-nadal-prowadzic-8491.html#.

[837] Definicja ta pomimo tego, że jest zaczerpnięta z uchylonych już przepisów, to jej treść jest nadal aktualna i wpisuje się w wytyczne RODO. Zob. *Polityka bezpieczeństwa danych,* [dostęp: 08.11.2018] https://lexdigital.pl/polityka-bezpieczenstwa-danych-osobowych-rodo.

[838] Z ang. ochrona danych osobowych na etapie projektowania.

[839] Z ang. domyślna ochrona danych osobowych.

o osobie, której dane są przedmiotem przetwarzania. Przeprowadzenie analizy ryzyka oraz oceny skutków dla ochrony danych osobowych nierzadko uznaje się za nieodzowny element procesu tworzenia sfery prywatności.

Druga z wymienionych zasad oznacza, że administrator danych osobowych przy pomocy stosownych środków technicznych i organizacyjnych zapewni, że przetwarzaniu poddane zostaną tylko te dane, które uważane są za absolutnie niezbędne. Cecha niezbędności zależy od ilości pobieranych danych osobowych, obszaru przetwarzania, czasu przechowywania oraz ich dostępności. Z praktycznego punktu widzenia oznacza to, że podczas dokonywania rejestracji konta użytkownika konkretnej aplikacji czy danego portalu, wymagane jest podanie niezbędnych danych, natomiast o ujawnieniu pozostałych informacji może w dowolnej chwili zadecydować sam użytkownik. Odpowiednie środki techniczne i organizacyjne dostosowane są do charakteru prowadzonej działalności. Z tego wynika, że nie ma uniwersalnych środków, zabezpieczeń, metod i procedur. Zależą one przede wszystkim od branży, zasad i technologii obowiązujących u konkretnego administratora danych osobowych. Stąd też, nie obowiązuje żaden jedyny określony wzór. Polityka bezpieczeństwa nie może posiadać uniwersalnego charakteru. Praktyka, po wejściu w życie Ogólnego Rozporządzenia o Ochronie Danych Osobowych, wykształciła pewne elementy, które ułatwiają stworzenie dopasowanej do danych potrzeb polityki bezpieczeństwa.

Nie mniej ważny od powyższych zasad jest sposób wyrażenia polityki bezpieczeństwa. Język i sformułowania prawne powinny być zrozumiałe dla czytających odbiorców. Nie mogą budzić wątpliwości w przedmiocie należytego postępowania w zakresie przetwarzania danych osobowych.

Niewątpliwie treść dokumentu determinują źródła prawa. Na samym początku należy wymienić, jakie obowiązujące przepisy prawa są wykorzystane[840]. Następnie warto wskazać cel dokumentu. Z reguły polityka bezpieczeństwa ma za zadanie określać środki techniczne i organizacyjne, procedury i zasady, które zagwarantują ochronę przetwarzanych danych osobowych przed zagrożeniem. Ponadto, nadmienia się, aby w tym miejscu wyartykułować grupy osób, których dane osobowe są przetwarzane (pracownicy, klienci, potencjalni klienci) oraz wypunktować zasady, które zapewnią bezpieczeństwo przetwarzania danych. Warto stworzyć definicje najważniejszych pojęć, które używane będą przy tworzeniu polityki bezpieczeństwa. Powinny zostać wytłumaczone role i funkcje poszczególnych osób

[840] Należy wymienić regulacje prawne Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

w procesie przetwarzania danych osobowych, tj. administrator danych osobowych, inspektor ochrony danych osobowych wraz z opisem ich zakresu odpowiedzialności oraz terminy związane z operacjami przeprowadzanymi na danych osobowych i z naruszeniami danych. Następnie, jeżeli wymagane jest wyrażenie zgody, warto opisać proces jej zbierania i dokumentowania. Ważnym punktem są prawa osób. Należy wskazać, jakie prawa przysługują podmiotowi danych, kto jest odpowiedzialny za prawidłową ich realizację oraz wyszczególnić etapy ich wykonania. Kolejnym elementem jest skonkretyzowanie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych. W sytuacji, jeśli dochodzi do powierzenia przetwarzania danych osobowych osobom trzecim, trzeba ustalić obowiązkowe postanowienia zawieranej umowy. W ustanawianiu wewnętrznej polityki bezpieczeństwa istotna jest reakcja na zachodzące incydenty. Wobec tego, zaleca się stworzenie katalogu podejmowania stosownych działań, w przypadku zaistnienia niepożądanych zdarzeń związanych z bezpieczeństwem przetwarzania danych osobowych. W momencie planowania rozpoczęcia nowego procesu biznesowego każdy powinien pamiętać o ocenie skutków dla ochrony danych osobowych. Trzeba wyjaśnić, co inicjuje konieczność przeprowadzenia oceny, kto jest zaangażowany w jej dokonanie oraz wskazać obszar ocenianych właściwości danych osobowych. Godzi się ponadto zawrzeć informacje o rodzajach audytów, które mogą być przeprowadzane w zakresie weryfikacji stanu ochrony danych osobowych, uwzględniając przy tym podmioty, biorące udział w ich realizacji. W tym punkcie warto wskazać także, w jaki sposób audyt jest planowany oraz jakiemu podmiotowi przekazywane są wskazówki oraz raport po dokonanym audycie. Finalnym etapem jest wymienienie załączników. W tym punkcie istnieje możliwość przedstawienia wszystkich dokumentów, jakie składają się na politykę bezpieczeństwa[841]. Warto mieć na uwadze, że nie jest konieczne fizyczne dołączanie załączników do polityki bezpieczeństwa. Zamiast tego, można wskazać miejsca, gdzie można się z nimi zapoznać.

W praktyce, polityka bezpieczeństwa jest sprawdzana i egzekwowana, biorąc pod uwagę działania podejmowane przez odpowiednie organy. Stąd też wydaje się, że nie jest to instytucja zawieszona w próżni, lecz systematycznie podlegająca kontroli. Tak też, organ nadzorczy wszczął z urzędu postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych przez Fortum Marketing and Sales Polska S.A. Na spółkę została nałożona administracyjna kara pieniężna w wysokości ponad 4,9 miliona złotych za

[841] Przede wszystkim chodzi tutaj o zastosowane procedury, opis systemów informatycznych, wzory upoważnień do przetwarzania danych osobowych, rejestr czynności przetwarzania.

brak wdrożenia odpowiednich środków technicznych i organizacyjnych oraz nieprzeprowadzenie weryfikacji działań podmiotu przetwarzającego. Podmiot przetwarzający otrzymał karę w wysokości 250 tysięcy złotych. Naruszenie ochrony danych osobowych miało polegać na skopiowaniu danych klientów administratora przez nieuprawnione osoby. Do tego incydentu doszło podczas wprowadzania zmian w środowisku teleinformatycznym. Zmianę nanosił podmiot przetwarzający, z którym administrator współpracował w oparciu o umowę powierzenia przetwarzania danych osobowych. W trakcie prac, została utworzona dodatkowa baza danych klientów spółki, która została skopiowana przez nieuprawnione do tego podmioty, ponieważ serwer nie posiadał należycie skonfigurowanych zabezpieczeń. Administrator danych osobowych dowiedział się o tym zdarzeniu dopiero od dwóch internautów, którzy poinformowali go, że mają dostęp do bazy danych. W toku przeprowadzonego postępowania, Urząd Ochrony Danych Osobowych ustalił, że Fortum Marketing and Sales Polska S.A. określiła z podmiotem przetwarzającym wymogi w zakresie bezpieczeństwa danych osobowych, które należało stosować, tj. pseudonimizację i szyfrowanie danych osobowych. Jak ustalono, w systemie użyto rzeczywistych danych osobowych klientów spółki. Co więcej, podmiot przetwarzający działał wbrew postanowieniom własnej polityki bezpieczeństwa. Administrator wyjaśnił, że zastosowanie rozwiązania, mającego poprawić wydajność usług, powinno być poprzedzone analizą korzyści i zagrożeń dokonaną przez podmiot przetwarzający. Administrator nie otrzymał jednak wyników analizy ani innych alternatywnych rozwiązań. Jak się potem okazało, administrator nie żądał też tej dokumentacji od podmiotu przetwarzającego. Spółka nie wymagała od podmiotu przetwarzającego realizacji umów, nie stosowała się do własnej praktyki wdrażania zmian w środowisku IT opartej o wewnętrzne regulacje, a także nie weryfikowała czynności prowadzących do usprawnienia funkcjonowania usługi, pomimo tego, że to administrator wdraża odpowiednie środki techniczne i organizacyjne, aby proces przetwarzania był zgodny z przepisami RODO. Zarówno wprowadzenie odpowiednich środków bezpieczeństwa, jak i ich sprawdzanie nie powinno być jednorazowym działaniem, lecz procesem ciągłym, gdzie administrator danych osobowych dokonuje przeglądu, a w razie konieczności uaktualnia przyjęte zabezpieczenia. W ten sposób zostałoby zminimalizowane ryzyko naruszenia praw lub wolności podmiotów danych[842].

Z powyższych rozważań należy wysnuć wniosek, że w obecnym porządku prawnym nie istnieje jedna, szablonowa polityka bezpieczeństwa. Każda z osobna musi być ściśle

[842] *Rekordowa kara dla administratora za naruszenie ochrony danych,* [dostęp: 28.02.2022] https://uodo.gov.pl/pl/138/2389.

dopasowana do charakteru organizacji i uwzględniać potencjalne zagrożenia. Tylko po przeanalizowaniu ryzyka, podmiot odpowiedzialny za politykę bezpieczeństwa, jest w stanie sporządzić dokumentację zgodną z Rozporządzeniem, którą w razie potrzeby przedstawi jako dowód bezpiecznego przetwarzania danych osobowych.

4.4.2. Pseudonimizacja i szyfrowanie danych

Z motywu 26 preambuły Rozporządzenia unijnego wyraźnie wynika, że zasady ochrony danych osobowych powinny dotyczyć wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Aby się dowiedzieć, czy dana osoba fizyczna, jest możliwa do zidentyfikowania, powinniśmy brać pod uwagę wszystkie prawdopodobne sposoby, które mogą zostać użyte przez administratora w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Jeśli znajdujemy się w posiadaniu jedynie imienia i nazwiska, to zdając sobie sprawę z tego, jak wiele osób o tych danych zamieszkuje na terytorium Polski, nie możemy założyć, że te dane dotyczą możliwej do zidentyfikowania osoby fizycznej. Dodając ponadto adres zamieszkania albo numer telefonu komórkowego, może się okazać, że procesowi przetwarzania poddawane są dane zidentyfikowanej osoby fizycznej, której należy zapewnić bezpieczeństwo.

Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia stosownych środków technicznych i organizacyjnych. Przepisy Rozporządzenia wskazują, o jakie środki chodzi. Przykładowo, wymienia się minimalizację przetwarzania danych osobowych (art. 5 ust. 1 lit. c) RODO), monitorowanie przetwarzania danych, czy wreszcie pseudonimizację danych osobowych (art. 4 pkt 5 RODO).

Pseudonimizacja została oficjalnie wprowadzona do prawa ochrony danych osobowych przez przepisy Rozporządzenia nr 2016/679[843]. Pseudonimizowane dane osobowe są to takie dane, które przy wykorzystaniu dodatkowych informacji można przypisać osobie fizycznej[844]. Obowiązek pseudonimizacji wprowadza art. 25 ust. 1 Rozporządzenia unijnego. Ten przepis, choć bardzo rozbudowany w wersji tekstowej, reguluje, że posługując się stanem wiedzy technicznej, kosztami wdrażania, a zarazem charakterem, zakresem, kontekstem

[843] Nie występowała w nieobowiązujących już przepisach Dyrektywy 95/46/WE.

[844] Na podstawie art. 4 pkt 5 RODO, termin „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, aby nie można było ich przypisać konkretnej osobie, której dane dotyczą bez wykorzystania dodatkowych informacji, pod warunkiem, że są przechowywane osobno oraz objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

i celami przetwarzania oraz ryzykiem naruszenia praw lub wolności osób fizycznych, wdrażane są stosowne środki techniczne i organizacyjne, tj. pseudonimizacja, zaprojektowane w celu należytej realizacji zasad ochrony takich danych, jak ich minimalizacja, oraz aby nadać procesowi przetwarzania niezbędnych zabezpieczeń w celu spełnienia wymagań niniejszego Rozporządzenia oraz ochrony praw osób, których dane dotyczą. Następnie, zgodnie z motywem 28 preambuły RODO, pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą i pomóc administratorom i podmiotom przetwarzającym wykonać obowiązek ochrony danych. Tym samym, wprowadzenie wprost pojęcia pseudonimizacji w Rozporządzeniu nie powoduje wykluczenia innych środków ochrony danych. Motyw 29 preambuły RODO wskazuje, że aby skorzystać z pseudonimizacji podczas przetwarzania danych osobowych, należy umożliwić u tego samego administratora wykorzystanie środków pseudonimizacyjnych, niewykluczających ogólnej analizy, o ile tylko ten administrator użył środków technicznych i organizacyjnych niezbędnych do tego, aby niniejsze Rozporządzenie zostało wdrożone w zakresie danego przetwarzania, oraz aby dodatkowe informacje pozwalające przypisać dane osobowe poszczególnemu podmiotowi były przechowywane oddzielnie. Na administratora przetwarzającego dane osobowe nałożony jest obowiązek wskazania osób upoważnionych do dokonywania takiej czynności[845].

Pseudonimizację można często mylnie utożsamić z anonimizacją (ujęcie europejskie)[846] lub kodowaniem (ujęcie amerykańskie)[847]. Przepisy RODO nie zawierają z kolei definicji procesu anonimizacji. Zawiera ją norma ISO 29100:2011[848].

Pomimo licznych wątpliwości co do skuteczności anonimizacji w pozbawieniu danych identyfikowalności podmiotów, narzędzie te, obok szyfrowania, jest nadal preferowane przez ustawodawców jako środek służący zmniejszeniu zagrożeń związanych z procesem przetwarzania danych. Zbiory stanowiące przedmiot analizy *Big Data* i niewyposażone bezpośrednio w dane osobowe, poddane wcześniej anonimizacji, zgodnie z definicjami przyjętymi w unijnym Rozporządzeniu, powinny być przetwarzane jak dane pseudonimiczne. Prowadzi to do wniosku, że duże zbiory danych, publicznie dostępne[849], które nie zawierają danych pozwalających wprost na identyfikację, powinny być przetwarzane zgodnie z europejskimi przepisami o ochronie danych, bowiem spełniają definicję danych

[845] J. Żołyński, *RODO. Prawo do zapomnienia…,* s. 241-242.
[846] Zespół LexDigital, *Co to jest anonimizacja i pseudonimizacja,* [dostęp: 10.05.2018] https://lexdigital.pl/co-to-jest-anonimizacja-i-pseudonimizacja.
[847] B. Elger, *Consent and anonymization in research involving biobanks,* "EMBO reports" 2007, nr 7, s. 661-666.
[848] https://www.iso.org/standard/85938.html.
[849] Np. wpisy z mediów społecznościowych, tj. Facebook, Twitter, LinkedIn.

pseudonimicznych oraz zawierają informacje na temat mieszkańców Unii Europejskiej[850].

Należy wskazać, że pomimo podobieństwa tych pojęć, diametralnie się od siebie różnią. Anonimizacja staje się dobrym rozwiązaniem wyłącznie wtedy, gdy administrator chciałby zapewnić całkowity i nieodwracalny brak dostępu do danych. Z kolei w praktyce realnej ochrony przetwarzanych danych, lepszym rozwiązaniem zdaje się być pseudonimizacja. Istotna cecha pseudonimizacji polega na tym, że jest to proces całkowicie odwracalny. Dane osobowe poddane pseudonimizacji należy objąć środkami technicznymi i organizacyjnymi utrudniającymi przypisanie ich zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Administrator danych osobowych, podejmując decyzję o skorzystaniu z pseudonimizacji, powinien od razu zapewnić pełne i sprawne odwrócenie tego procesu[851]. Anonimizacja to proces polegający na usunięciu przez administratora danych lub osobę trzecią wszystkich informacji, które w jakikolwiek sposób umożliwiają identyfikację określonej osoby[852]. Zanonimizowane dane nie są już wówczas danymi osobowymi, ponieważ utrudnione jest zidentyfikowanie osoby, której dane zostały poddane temu procesowi[853].

Do innych metod pseudoanimizujących zalicza się stosowanie skrótów poprzez używanie funkcji *hash.* Technika ta jest popularna i polega na tym, że dane są kodowane w zunifikowany sposób, np. Jan Nowak, Anna Nowakowska, Adam Kowalski zostaną zastąpione „01", „02", „03". Metoda ta okazała się nieskuteczna. W 2006 roku wyszukiwarka internetowa America On Line opublikowała historię wyszukiwań 650 tysięcy użytkowników. Usunięto numery IP oraz zanonimizowano dane. Nazwy użytkowników zakodowano przy użyciu funkcji haszującej. Okazało się, że poprzez historię wyszukiwania można zdobyć dane osobowe użytkownika[854].

Jeszcze innym narzędziem służącym do ochrony danych jest ich szyfrowanie. Stosowane jest do powstrzymywania nieupoważnionych osób przed dostępem do poufnych

[850] W związku z tym wypełniona zostaje przesłanka związana z zakresem terytorialnym stosowania przepisów z art. 2 ust. 2 Rozporządzenia.
[851] Proces pseudonimizacji powinien wiązać się np. z wygenerowaniem numerów identyfikacyjnych.
[852] Do takich danych można zaliczyć imię i nazwisko, adres, numer telefonu.
[853] Anonimizacja może być stosowana na nośnikach papierowych, czyli dokumentach, na przykład poprzez zamazanie w tekście dokumentu wszelkich informacji pozwalających na dokonanie identyfikacji podmiotu danych. Proces ten może ponadto polegać na usunięciu z danego systemu informatycznego danych zezwalających na identyfikację, a pozostawienie jedynie danych statystycznych. Brak możliwości identyfikacji osoby fizycznej powinien mieć charakter obiektywny. Zob. B. Zygmanowski, *Pseudonimizacja a anonimizacja danych. Praktyczne zastosowanie w przedsiębiorstwie,* [dostęp: 27.08.2018] https://gdpr.pl/pseudonimizacja-a-anonimizacja-danych-praktyczne-zastosowanie-w-przedsiebiorstwie.
[854] M. Barbaro, T. Zeller, *A Face Is Exposed for AOL Searcher No. 4417749,* [dostęp: 09.08.2006] https://www.nytimes.com/2006/08/09/technology/09aol.html.

informacji[855]. Istotą tego procesu jest kodowanie wiadomości lub plików, dzięki czemu mogą je odczytać jedynie uprawnione do tego osoby. Zwykły tekst przekształcany jest na tekst szyfrowany. Algorytm szyfrowania używa czytelnych danych i zmienia je w taki sposób, aby przypominały losowy zbiór symboli. Zaszyfrowane dane wyglądają jak losowe znaki, niemniej jednak cała ta procedura przebiega w logiczny sposób, tak aby osoba odbierająca zaszyfrowane dane i posiadająca prawidłowy klucz, wykorzystany do ich szyfrowania, była zdolna odszyfrować dane i dokonać z powrotem ich przekształcenia w zwykły tekst[856].

Powszechne sposoby szyfrowania mogą być tak proste, jak zamiana liter. Rozwój technik kryptograficznych sprawił jednak, że algorytmy szyfrujące są coraz bardziej rozbudowane, a proces deszyfrowania coraz trudniejszy. Procedury szyfrowania są na tyle skomplikowane, że raczej nie jest prawdopodobne, by jakakolwiek obca osoba, bądź algorytm, były w stanie zdekodować tekst metodą *brute force attack*[857].

Atak siłowy jest popularny w sieci internetowej. Stanowi rodzaj ataku cybernetycznego, który wykorzystuje metodę prób i błędów, aby rozpoznać dane logowania, kluczy bezpieczeństwa lub innych poufnych informacji. W tym celu używa się specjalistycznego oprogramowania. W *brute force attack,* metodą prób i błędów, wprowadzane są popularne frazy słownikowe, często używane hasła, bądź określone kombinacje liter i cyfr, dopóki nie uzyska się dopasowania. Atak typu *credential stuffing* jest jedną z najskuteczniejszych metod siłowych. Opiera się na powtarzających się hasłach. Wystarczy jeden zestaw poświadczeń, aby włamać się na większość kont internetowych. Pozwala to na uzyskanie dostępu do wielu kont jednocześnie (np. kont bankowych, kont biznesowych, portali społecznościowych). Cyberprzestępcy stosują m.in. BotNets, aby przeprowadzić ataki na wielu różnych urządzeniach. Konsekwencją tego działania jest kradzież pieniędzy, czy kradzież tożsamości[858].

Ataki siłowe są metodą efektywną, biorąc pod uwagę fakt, że około 65% osób używa

---

[855] Szyfrowanie chroni wiele codziennych czynności, do których zalicza się korzystanie z bankowości internetowej, poczty e-mail, robienie zakupów on-line, a także przeglądanie stron www oraz wyszukiwanie informacji. Zob. Netia, *Szyfrowanie danych. Po co i jak to robić?,* [dostęp: 03.06.2020] https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/szyfrowanie-danych-jak-to-robic.

[856] Do przykładowych sytuacji, w których powinno rozważyć się zastosowanie metody szyfrowania zaliczają się: posługiwanie się przenośnymi komputerami, korzystanie z laptopów z zapisanymi danymi osobowymi z publicznych sieci WIFI, przesyłanie plików o charakterze wrażliwym za pośrednictwem Internetu, przekazywanie danych osobowych na przenośnych nośnikach. Zob. I. Kalisz, *Szyfrowanie danych osobowych,* [dostęp:] https://przetwarzanie-danych-osobowych.pl/szyfrowanie-danych-osobowych/.

[857] Z ang. „zgadując"; „odkodowanie zaszyfrowanych plików bez klucza szyfrowania jest możliwe, jednak złamanie dobrze opracowanego schematu szyfrowania wymagałoby bardzo dużej mocy obliczeniowej". Zob. *Na czym polega szyfrowanie danych?,* [dostęp:] https://experience.dropbox.com/pl-pl/resources/what-is-encryption.

[858] *Czym jest atak typu „credential stuffing"?,* [dostęp:] https://www.keepersecurity.com/pl_PL/threats/credential-stuffing-attacks.html.

ponownie tych samych haseł. Ataki siłowe są coraz to bardziej powszechną formą. Średni koszt skutecznego cyberataku wynosi miliony dolarów. Wzrost tych ataków uwidocznił się w szczególności podczas pandemii Covid-19[859]. Od stycznia do grudnia 2020 roku, liczba ataków zwiększyła się z około 200 tysięcy do ponad 1,4 miliona na całym świecie. Firmy, wykonujące pracę zdalną, przeprowadzały próbne testy modeli pracy w domu, co stworzyło okazję dla cyberprzestępców do wykorzystania niezabezpieczonych komputerów i nieprawidłowych praktyk zarządzania hasłami[860]. Można zauważyć, że wraz z postępem informatycznym, udoskonalane są środki, które służą przełamywaniu wszelkiego rodzaju zabezpieczeń.

4.4.3. Szacowanie ryzyka dla podstawowych praw i wolności

Rozporządzenie o Ochronie Danych Osobowych opiera się na koncepcji analizy ryzyka przetwarzania danych osobowych. Podmioty przetwarzające dane osobowe podejmują działania mające na celu ustalenie i ocenę tego ryzyka, a wcześniej wykorzystują środki profilaktyczne służące zapobieganiu jego wystąpienia. Czynności powinny być adekwatne do stwierdzonego ryzyka. W treści motywu 75 preambuły RODO wskazano, że ryzyko naruszenia praw lub wolności osób o różnorodnej wadze zagrożenia, może być powiązane z przetwarzaniem danych osobowych prowadzącym do uszczerbku fizycznego albo szkód majątkowych lub niemajątkowych, zwłaszcza gdy proces ten prowadzi do naruszenia dobrego imienia, naruszenia poufności danych osobowych chronionych tajemnicą zawodową czy nieuprawnionego odwrócenia pseudonimizacji. Innymi działaniami, z którymi wiąże się wystąpienie ryzyka jest pozbawienie podmiotu danych kontroli nad swoimi danymi, przetwarzanie danych dotyczących wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa. Ryzyko należy oszacować w oparciu o ocenę o charakterze obiektywnym, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się tylko ryzyko, czy ryzyko wysokiego stopnia.

Ustalenia czy przetwarzanie przez administratora danych osobowych związane jest z wysokim naruszeniem praw i wolności osób fizycznych, należy dokonać przy uwzględnieniu założeń Grupy Roboczej Art. 29 z dnia 4 kwietnia 2017 r. dotyczących oceny skutków dla ochrony danych (DPIA) i ustalenia, czy przetwarzanie „może powodować

[859] K. Dobrzeniecki, B. Przywora, *Wnioski z badań,* [w:] *Ograniczenia praw i wolności w okresie pandemii COVID-19 na tle porównawczym. Pierwsze doświadczenia,* Warszawa 2021, s. 481.
[860] *Czym jest atak typu „brute force”?,* [dostęp:] https://www.keepersecurity.com/pl_PL/threats/brute-force-attack.html.

wysokie ryzyko" do celów Rozporządzenia nr 2016/679 (WP 248)[861].

W zakresie tych rozważań, kluczowy jest również motyw 77 preambuły RODO, stanowiący, że wskazówki na temat wdrażania odpowiednich środków oraz wykazywania przestrzegania prawa przez administratora lub podmiot przetwarzający dane mogą być udostępniane w formie zatwierdzonych kodeksów postępowania, certyfikacji, wytycznych EROD lub za pośrednictwem inspektora ochrony danych. Powinny one uwzględniać praktyki pozwalające zminimalizować to ryzyko. Zgodnie z art. 32 ust. 1 lit. d) RODO, należy regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zagwarantować bezpieczeństwo przetwarzania[862].

W kontekście analizy ryzyka wyróżnia się dwa etapy modelu postępowania. W ramach pierwszej fazy ustala się czynności przetwarzania danych osobowych. Z reguły są one wskazane w rejestrze czynności i posiadają wspólne cechy. Jednolity poziom ryzyka przetwarzania danych osobowych ustala się wówczas z punktu widzenia szkód dla osób fizycznych, których dane osobowe są przetwarzane. W drugiej zaś fazie bierze się pod uwagę to, czy występują szczególne rodzaje ryzyka i czy z tego powodu dla tych czynności przetwarzania powinny zostać zastosowane wyższe wymogi w odniesieniu do środków technicznych i organizacyjnych odnoszących się do przetwarzania danych osobowych. Oprócz tego, ważne jest odpowiednie dobranie techniki oceny ryzyka[863].

Na podstawie art. 32 ust. 2 RODO, oceniając, czy stopień bezpieczeństwa jest odpowiedni, bierze się pod uwagę ryzyko wiążące się z przetwarzaniem, wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych, bądź w inny sposób przetwarzanych. Analiza ryzyka obejmuje ustalenie metodyki opartej na jego jakościowej i ilościowej analizie. Oprócz tego, obejmuje szacowanie ryzyka oraz określenie jego poziomu. Kolejnym etapem szacowania ryzyka jest jego ocena, po której następuje postępowanie z ryzykiem w bezpieczeństwie informacji. Dopiero finalnie dochodzi do akceptacji i przeglądu ryzyka[864].

---

[861] https://archiwum.giodo.gov.pl/pl/1520296/10059.

[862] A. Krasuki, *Ochrona danych osobowych na podstawie RODO,* Warszawa 2018, s. 297-298.

[863] Kryterium to okazuje się być niezbędne do wykazania wykonania obowiązków w zakresie rozliczalności zgodnie z art. 5 ust. 1 lit. f) w zw. z ust. 2 RODO. Zasada rozliczalności polega na tym, że na administratorze spoczywa obowiązek udowodnienia, że dane osobowe są przetwarzane na podstawie prawa, a ponadto w sposób rzetelny i przejrzysty. Dane muszą być prawidłowe, aktualne i służyć celowi zgodnemu z prawem. Zob. M. Zygmunt-Jakuć, *Jak wykazać spełnienie zasady rozliczalności RODO,* [dostęp:] https://bezowijania.com/jak-wykazac-spelnienie-zasady-rozliczalnosci-rodo.

[864] Norma PN-ISO/IEC 27005:2014-1, Technika informatyczna-Techniki bezpieczeństwa-Zarządzanie ryzykiem w bezpieczeństwie informacji, Polski Komitet normalizacyjny, Warszawa 2014.

Dokumentacja dotycząca ochrony danych osobowych powinna spełniać wymogi wynikające z nałożonego obowiązku w postaci uwzględniania ochrony danych osobowych w fazie projektowania oraz w fazie domyślnej ochrony danych. Na tym pierwszym z wymienionych etapów, administrator wdraża stosowne środki techniczne i organizacyjne, m.in. pseudonimizację. Z kolei w fazie domyślnej, podmiot ten podejmuje takie czynności, aby przetwarzane były wyłącznie te dane osobowe, które niezbędne są dla osiągnięcia każdego konkretnego celu przetwarzania[865].

Mając na uwadze wymagania związane z przetwarzaniem danych osobowych, wskazać należy na art. 35 RODO. Przepis ten nakłada na administratora obowiązek dokonania oceny skutków planowanych operacji przetwarzania danych osobowych, jeśli dany rodzaj przetwarzania może prowadzić do wysokiego ryzyka naruszenia praw i wolności osób fizycznych, których dane osobowe są przetwarzane. W ust. 3 wymieniono katalog przykładowych okoliczności, kiedy uzasadnione jest przeprowadzenie oceny skutków planowanych operacji przetwarzania danych osobowych. Obejmują one swym zakresem systematyczną, całościową ocenę czynników osobowych, odnoszących się do osób fizycznych, która polega na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Ponadto odnoszą się do przetwarzania na dużą skalę szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO) lub danych osobowych o wyrokach skazujących i naruszeniach prawa (art. 10 RODO).

Analiza ryzyka pozwala zapobiegawczo wprowadzać takie środki bezpieczeństwa, które albo znacząco obniżą ryzyko wystąpienia jakiegoś zdarzenia, albo chociaż ograniczą negatywne konsekwencje z nim związane. Można to zobrazować na następującym kazusie. Spółka udostępniła laptopy jako podstawowe narzędzia pracy kilku swoim pracownikom. Pracownicy zapisują na dyskach twardych różnego rodzaju dokumenty, które zawierają dane osobowe. Jeden z pracowników zabrał laptopa na zewnętrzne szkolenie. Został okradziony. Sprzęt nie był odpowiednio zabezpieczony przed dostępem osób trzecich. Wysoce prawdopodobnym skutkiem tego zdarzenia jest ryzyko dostępu do danych przez osobę do tego nieuprawnioną, a także ryzyko bezpowrotnej utraty tych danych w przypadku nieposiadania zapisanej kopii. Kolejną kwestią jest zastanowienie się, na ile jest możliwe wystąpienie takiego scenariusza. Można, a nawet powinno się odwołać do doświadczeń związanych z wcześniejszymi kradzieżami laptopów, jeśli takie miały miejsce. Następnie

[865] Wiąże się to z ilością zbieranych danych osobowych, zakresem ich przetwarzania, okresem ich przechowywania oraz z dostępnością. Co do zasady, środki te gwarantują sytuację, aby dane osobowe nie były udostępniane bez ingerencji danej osoby nieokreślonej liczbie osób fizycznych. Zob. A. Krasuki, *Ochrona danych osobowych…,* s. 303.

należy ustalić, jaki negatywny skutek może wywołać zaistniałe zdarzenie (np. kradzież tożsamości) oraz oznaczyć jego intensywność. Jeżeli na utraconym laptopie widniały wyłącznie służbowe adresy e-mail, to uzyskanie dostępu do danych nie będzie poważnie wpływało na prawa i wolności tych osób. Znaczniej szkodliwy skutek mogłaby wywołać sytuacja, gdyby na dysku były zapisane umowy o pracę, czy wypełnione kwestionariusze osobowe. Sama zaś spółka musi liczyć się z ryzykiem nałożenia na nią kary pieniężnej w wyniku stosowania niewystarczających zabezpieczeń. Tego typu zdarzenie wpływa też na dobry wizerunek podmiotu. Kolejną czynnością, jaką należy podjąć jest szacowanie ryzyka. Ostatnim krokiem jest dobór środków bezpieczeństwa, adekwatnych do stwierdzonych zagrożeń. Mogłoby się sprawdzić rozwiązanie polegające na wprowadzeniu szyfrowania dysków twardych, dokonywanie okresowych zmian haseł dostępu do systemów informatycznych zainstalowanych na laptopie, jak też organizowanie szkoleń z wprowadzanych zasad bezpieczeństwa[866].

W przepisach unijnego Rozporządzenia nie narzucono konkretnego szablonu analizy ryzyka. Każdy może opracować indywidualny sposób postępowania lub bazować na dostępnych propozycjach.

4.4.4. Obowiązek oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych

Ocena skutków dla ochrony danych jest nową instytucją w zakresie przepisów dotyczących ochrony danych osobowych[867]. Instytucja ta uległa zmianom podczas prac nad RODO. Zgodnie z pierwotną propozycją Komisji Europejskiej, organ ten miał być uprawniony do przyjmowania aktów delegowanych w celu doprecyzowania kryteriów i warunków operacji przetwarzania, dla których przeprowadzenie oceny miało być obowiązkowe. Komisja UE miała również posiadać prawo do określania wymogów w zakresie oceny skutków, jak też procedur przeprowadzania, weryfikowania i kontroli oceny. Dopiero na końcowym etapie prac nad Rozporządzeniem, Parlament Europejski zadecydował, aby usunąć delegację dla Komisji UE. Wobec tego, aktualnie ocena skutków jest instytucją, gdzie zakazane jest doprecyzowanie w akcie delegowanym lub wykonawczym Komisji Europejskiej.

---

[866] J. Wezgraj, *Prowadzenie analizy ryzyka RODO-przykład,* [dostęp: 01.03.2019] https://www.pps.edu.pl/blog/prowadzenie-analizy-ryzyka-zgodnie-z-wymaganiami-rodo.

[867] N. Kalinowska, P. Litwiński, *Ocena skutków dla ochrony danych i uprzednie konsultacje-nowe obowiązki podmiotów przetwarzających dane osobowe,* „Monitor Prawniczy" 2017, nr 13, s. 694.

Nie sposób nie zauważyć pewnej istotnej kwestii terminologicznej. Przed rozpoczęciem prac nad RODO, używano pojęcia „ocena skutków dla ochrony prywatności”[868]. Z tego wynika, że zakres oceny skutków dla ochrony danych jest węższy niż zakres oceny skutków dla ochrony prywatności[869]. Skoro ochrona prywatności informacyjnej stanowi jeden z aspektów prawa do prywatności, to ocena mająca za punkt odniesienia dane osobowe będzie przeprowadzona w węższym zakresie, w porównaniu z prawem do prywatności. Przeprowadzenie oceny, biorąc pod uwagę nie tylko samą ochronę danych osobowych, ale także prywatność, nie powinno być uznane za błąd, lecz powinno być traktowane w kategoriach dobrej praktyki[870].

Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych nie posiada swojej definicji legalnej[871]. Na podstawie analizy przepisów RODO, można wywnioskować, że składa się na to trzyczęściowy proces, w trakcie którego następuje określenie przetwarzania danych mających wpływ na naruszenie praw lub wolności osób fizycznych, wybór sposobu oceny tego wpływu, jak też dobranie adekwatnych środków do minimalizacji negatywnego oddziaływania. Ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych należy odróżnić od wcześniej wspomnianej ogólnej analizy ryzyka, której przeprowadzenie jest obowiązkiem każdego podmiotu, bez względu na wielkość i ilość przetwarzanych danych. Natomiast DPIA jest konieczne jedynie w sytuacjach określonych w art. 35 RODO. Instytucję tę należy wdrożyć zgodnie z treścią ust. 1, jeśli istnieje przesłanka wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Założenie, że takie ryzyko występuje, może wynikać z charakteru, celu lub kontekstu przetwarzanych danych, w szczególności, jeżeli proces przetwarzania danych odbywa się przy użyciu nowych technologii. W ust. 3 wskazano, że ocena skutków jest wymagana, jeśli dane osobowe przetwarzane są w sposób zautomatyzowany bez udziału człowieka, a rezultatem takiego działania jest podjęcie decyzji wywołujących skutki prawne w stosunku do osoby fizycznej lub w znaczny sposób na nią wpływających[872], a ponadto, jeżeli dane osobowe pochodzą z systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie. Wymienia się także przesłankę przetwarzania danych wrażliwych na

[868] *Tamże,* s. 695.
[869] D. Wright, P. De Hert, *Enforcing Privacy. Regulatory, Legal and Technological Approaches,* [w:] *Springer International Publishing,* Cham 2016, s. 162.
[870] N. Kalinowska, P. Litwiński, *Ocena skutków dla ochrony danych…,* s. 695.
[871] *Ang. Data Protection Impact Assessment,* dalej: DPIA.
[872] Np. automatyczna kwalifikacja do badań klinicznych.

dużą skalę lub dane o wyrokach skazujących i naruszeniach prawa[873].

Ostatnia z wymienionych przesłanek ma swoje zastosowanie w organizacjach pozarządowych, które często gromadzą dane o stanie zdrowia, czy na temat bezdomności. Z kolei informacje o naruszeniach prawa będą miały istotne znaczenie dla organizacji zajmujących się pomocą dla ofiar przestępstw lub dla pomocy postpenitencjarnej. Unijne Rozporządzenie nie wyjaśnia, co oznacza termin „duża skala"[874]. Badając to zjawisko, trzeba wziąć pod uwagę liczbę osób, których dane dotyczą[875], zakres przetwarzanych danych[876], zasięg geograficzny[877] oraz czas przetwarzania danych[878].

Wytyczne Grupy Art. 29 wskazują na przesłanki, których wystąpienie może powodować konieczność dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Przeprowadzenie DPIA jest wymagane w przypadku działań mających na celu prognozowanie zachowań lub tworzenie profili, łączenia zbiorów danych lub operacji nastawionych na porównanie danych w co najmniej dwóch zbiorach, przetwarzania danych osób deprecjonowanych z jakiegoś powodu[879], transferu danych poza terytorium Unii Europejskiej, przetwarzania danych, którego efektem jest niemożność skorzystania przez zainteresowaną osobę z usługi lub z umowy. Wytyczne formułują postulat, który wyraża się w stwierdzeniu, że im większa ilość spełnionych przesłanek, tym większe istnieje ryzyko, że proces będzie wymagał oceny skutków działań. Podmiot ten za bezpieczną granicę przyjął spełnianie dwóch przesłanek – wówczas zaistnieje niskie ryzyko naruszenia praw i wolności osób, których dane są przetwarzane[880].

Oprócz powyższego, wymieniono też warunki, których spełnienie powoduje brak konieczności przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Można wyróżnić kilka sytuacji, zwalniających z wymogu przeprowadzenia DPIA. Pierwszą z nich jest brak ryzyka naruszenia praw lub wolności osób,

---

[873] J. Greser, *RODO. Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych,* [dostęp: 26.06.2018] https://publicystyka.ngo.pl/rodo-ocena-skutkow-planowanych-operacji-przetwarzania-dla-ochrony-danych-osobowych.

[874] Pomocne w interpretacji okazały się być wytyczne Grupy Roboczej Art. 29, tj. *Wytyczne dotyczące inspektorów ochrony danych,* przyjęte w dniu 13 grudnia 2016 r., WP 243 oraz *Wytyczne dotyczące oceny skutków dla ochrony danych oraz określania, czy przetwarzanie danych może powodować wysokie ryzyko,* przyjęte w dniu 13 października 2017 r., WP 248.

[875] Chodzi zarówno o samą ilość, jak i relację do całej populacji z określoną cechą; np. organizacja przetwarza dane osobowe wszystkich osób w Polsce z rzadką chorobą genetyczną (ich liczba może być niewielka, jednak obejmuje całość albo znaczny procent populacji tych osób).

[876] Im więcej szczegółowych danych, tym większe istnieje ryzyko ich naruszenia.

[877] Motyw 91 preambuły RODO wskazuje na zasięg regionalny, krajowy lub ponadnarodowy.

[878] Im dłużej są przechowywane dane, tym większe jest ryzyko naruszenia praw.

[879] Np. dzieci z uwagi na ograniczoną możliwość świadomego podejmowania decyzji.

[880] Z tego wynika, że jeżeli przetwarzane są dane wrażliwe, np. o rodzaju konkretnej dysfunkcji (dane wrażliwe) i dotyczą one osób defaworyzowanych, to spełnione zostały łącznie dwie przesłanki. Nie ma więc potrzeby przeprowadzenia oceny skutków działań ze względu na niskie ryzyko.

których dane dotyczą[881]. Obowiązek oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych nie jest także konieczny, gdy proces przetwarzania jest podobny do takiego, w stosunku, do którego DPIA zostało wcześniej przeprowadzone[882] albo gdy istnieje przepis prawa krajowego lub przepis prawa Unii Europejskiej, który reguluje daną operację przetwarzania, a oceny skutków dokonano na etapie legislacyjnym. Niekiedy organ nadzoru wydaje wykaz operacji przetwarzania, które nie podlegają wymogowi dokonania takiej oceny[883]. Zwolnione z tego jest również przetwarzanie danych osobowych swoich klientów przez prawnika[884].

Rozporządzenie unijne nie podaje gotowego rozwiązania odnoszącego się do zakresu oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jedynie w art. 35 ust. 7 RODO wskazuje się na minimalny zakres takiej oceny[885]. Zgodnie z treścią tego przepisu powinna ona zawierać systematyczny opis planowanych operacji przetwarzania i celów przetwarzania (np. przetwarzanie danych przy procesie rekrutacji w celu zatrudnienia nowych pracowników; zakres danych to imię, nazwisko, adres, wykształcenie, przebieg zatrudnienia)[886], w tym prawnie uzasadnionych interesów realizowanych przez administratora. Ponadto ocenę czy operacje przetwarzania charakteryzują się niezbędnością oraz proporcjonalnością w stosunku do celów (kserowanie dokumentów tożsamości nie jest ani niezbędne do realizacji celu przetwarzania, np. identyfikacji danej osoby, ani nie posiada podstaw prawnych, z wyjątkiem prawa bankowego), jak też ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą (tj. jakie naruszenie może wystąpić, jaka jest waga zagrożenia)[887]. Powinny być także planowane takie mechanizmy, aby zaradzić ryzyku (np. na etapie rozmów kwalifikacyjnych kandydaci proszeni są o pokazanie swoich dyplomów/certyfikatów), w tym zabezpieczenia i środki bezpieczeństwa mające zagwarantować ochronę danych osobowych[888]. Pomocne przy prowadzeniu oceny skutków

[881] Przesłanka ta wynika z art. 35 ust. 1 RODO, natomiast sprawdzenie istnienia ryzyka odbywa się na podstawie ogólnej analizy ryzyka.
[882] Ma to na celu uniknięcie powtarzania już raz przeprowadzonej czynności. Zgodnie z zasadą rozliczalności, odpowiedzialność za udowodnienie tego faktu spoczywa na administratorze danych osobowych.
[883] Wykaz operacji, których prowadzenie powoduje obowiązek dokonania DPIA można znaleźć w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, [dostęp: 08.07.2019] https://monitorpolski.gov.pl/MP/2019/666.
[884] Motyw 91 RODO.
[885] K. Witkowska-Nowakowska, *Ocena skutków dla ochrony danych. Kiedy należy przeprowadzić DPIA i na czym ona polega?,* [dostęp: 13.03.2020] https://portalodo.com/ocena-skutkow-dla-ochrony-danych-kiedy-nalezy-przeprowadzic-dpia-i-na-czym-ona-polega/.
[886] *Ocena skutków dla ochrony danych (DPIA)-wzór formularza,* [dostęp: 08.08.2021] https://odo24.pl/blog-post.ocena-skutkow-dla-ochrony-danych-dpia-bezplatny-formularz.
[887] J. Greser, *RODO. Ocena skutków planowanych operacji…*
[888] Jest to jednak niezbędne minimum, a zatem pełen zakres oceny może być nieco szerszy.

działań są następujące źródła – Wytyczne Grupy 29[889], normy ISO/IEC[890], narzędzie udostępnione przez CNIL (francuski odpowiednik Urzędu Ochrony Danych Osobowych)[891].

4.5. Podsumowanie

Do momentu wejścia w życie przepisów Rozporządzenia unijnego, czyli do dnia 25 maja 2018 roku najważniejszym aktem prawnym obejmującym obszar ochrony danych osobowych była ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku. Wprowadzenie RODO na terenie całej Unii Europejskiej wywarło wpływ na uchwalenie w Polsce nowej ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku. Zastosowanie tej regulacji prawnej miało w szczególności na celu dostosowanie przepisów do RODO[892]. Przyjęty przez rząd projekt ustawy był wynikiem pracy zarówno po stronie Ministerstwa Cyfryzacji, jak i przedstawicieli środowisk związanych z danymi osobowymi, którzy brali udział przy tworzeniu projektu na etapie konsultacji społecznych.

Mając na uwadze swobodę krajów podlegających przepisom Rozporządzenia, odnoszącą się do możliwości ograniczenia działania RODO w zakresie wynikającym z art. 23 ust. 1 oraz ust. 2, spodziewano się podjęcia działań legislacyjnych realizujących tę możliwość. Wyrażając chęć wprowadzenia zmian w związku z prawami osób, których dane dotyczą z rozdziału III RODO, prawodawca powinien tworzyć przepisy realizujące dyspozycję z ustępu 2. wyżej wymienionego przepisu. Określono w nim zobowiązanie, aby wskazać w akcie normatywnym, ograniczającym stosowanie norm dotyczących obowiązków

[889] Wytyczne są nieodpłatne. Ukierunkowane są na dokumentowanie oceny skutków oraz stałe monitorowanie i okresowy przegląd. Zalecają publikowanie chociaż streszczenia z oceny (obowiązek ten nie wynika z przepisów RODO). Zob. Wersja Wytycznych z dnia 4 października 2017 r. w j. polskim, [dostęp:] https://ec.europa.eu/newsroom/article29/items/611236.

[890] Nadzwyczaj istotna jest Norma ISO/IEC 29134, która zawiera wytyczne w kontekście przeprowadzenia analizy ryzyka ukierunkowanej na problematykę ochrony prywatności osób, których dane są przetwarzane. Postuluje, w jaki sposób uwzględnić problem oceny konsekwencji naruszenia prywatności i prawdopodobieństw pojawienia się zdarzeń prowadzących do takich deliktów. Pozwala zidentyfikować działania mogące zmniejszyć ryzyko do akceptowalnego poziomu, a następnie zastosować je zgodnie z opracowanym planem postępowania, [dostęp: 14.03.2018] https://odoserwis.pl/a/1179/ocena-wplywu-na-prywatnosc-zgodnie-z-norma-isoiec-29134-metodyka-prowadzenia-dpia. Przydatna może się okazać również Norma PN-ISO/IEC 29100:2017-07, która dotyczy określania ram prywatności, czyli podstawowych wymogów, jakie powinno spełniać postępowanie administratora, aby realizowało ono warunki ochrony prywatności jednostki. Normy ISO objęte są prawem autorskim, a korzystanie z nich wymaga uzyskania odpłatnej licencji, [dostęp:] https://ikmj.com/pn-iso-iec-291002017-technika-informatyczna-techniki-bezpieczenstwa-ramy-prywatnosci/.

[891] Oprogramowanie jest darmowe, dostępne jako *open source.* Służy ono przygotowaniu pomocy w przeprowadzeniu DPIA. Program ten jest dostępny pod adresem strony internetowej: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

[892] N. Dzieciuchowicz, *Nowelizacja aktów prawnych w związku z obowiązywaniem RODO. Ustawa o ochronie danych osobowych z 10 maja 2018 jako akt wprowadzony w celu dostosowania polskiego prawa do przepisów unijnych,* [dostęp: 08.03.2023] https://lexdigital.pl/nowelizacja-aktow-prawnych-w-zwiazku-z-obowiazywaniem-rodo-ustawa.

i praw nałożonych przez przepisy RODO, szczegółowych uregulowań zawierających informacje o celach przetwarzania lub kategorii przetwarzania, grupach danych osobowych podlegających przetwarzaniu, zakresie wprowadzonych ograniczeń, podjętych działaniach zmierzających do zapobiegnięcia nadużyciom lub niezgodnemu z prawem dostępowi albo przekazywaniu danych podlegających przetwarzaniu wyłączonemu z bezpośredniego działania przepisów RODO, administratorze lub kategorii administratorów tych danych, okresach przechowywania, ryzyku naruszenia praw lub wolności osoby, której dane dotyczą, uprawnieniach podmiotów danych do uzyskania informacji o ograniczeniach, pod warunkiem, że nie narusza to ich celu. Taka regulacja nie może się ograniczyć tylko do wskazania, których przepisów nie powinno się stosować, lecz musi zawierać też szereg innych postanowień[893]. Treść nowej ustawy o ochronie danych osobowych zawiera część regulacji, które wcześniej znajdowały się w ustawie o ochronie danych osobowych z 1997 roku. Większość istotnych zagadnień regulowanych jest w RODO. Tam też przedsiębiorca powinien szukać w pierwszej kolejności informacji dotyczących wymogów na temat przetwarzania danych osobowych[894].

W ustawie z dnia 10 maja 2018 r. wprowadzono nowy organ nadzorczy – Prezesa Urzędu Ochrony Danych Osobowych. Pozostawienie nazwy Generalnego Inspektora Ochrony Danych Osobowych mogłoby okazać się błędne w kontekście pozycji ustrojowej. Uregulowano przepisy dotyczące certyfikacji. Korzyścią uzyskaną z posiadania certyfikatu jest wzrost zaufania do administratora lub podmiotu przetwarzającego. Zlikwidowano obowiązek dotyczący rejestracji zbiorów danych. Powodem podjęcia takiej decyzji było niezgłaszanie tych zbiorów, nieinformowanie o wprowadzanych zmianach. Zamiast tego utworzono wewnętrzny rejestr czynności przetwarzania.

Obowiązująca ustawa o ochronie danych osobowych nie była jednak wystarczająca, aby zapewnić skuteczne stosowanie Rozporządzenia. Stało się potrzebne dokonanie zmian przepisów sektorowych, efektem czego było wprowadzenie nowelizacji w 162 aktach normatywnych, regulujących różne branże i obszary gospodarki. Zmianę przepisów spowodowało też inne podejście do przesłanek legalizujących proces przetwarzania danych wynikających z treści art. 6 ust. 1 lit. c) oraz e) RODO. Zastosowanie formuł, opierających się na założeniu, że przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze oraz do wykonania zadania realizowanego w interesie

[893] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie…,* s. 136-138.
[894] D. Echaust-Przybytniak, *Najnowsza ustawa o ochronie danych osobowych-2023 r.,* [dostęp: 26.03.2023] https://rkrodo.pl/najnowsza-ustawa-o-ochronie-danych-osobowych/.

publicznym, bądź w ramach sprawowania władzy publicznej powierzonej administratorowi wskazało na konieczność podjęcia działań o charakterze lobbingowym przez administratorów, co spowodowało zmianę dotychczasowego brzmienia przepisów sektorowych w postaci bezpośredniego wyartykułowania obowiązku przetwarzania przy założeniu, iż pierwsze z wymienionych zobowiązań daje większą pewność działań administratora danych osobowych, dookreślając chociażby główny cel przetwarzania danych oraz zalicza się do konstrukcji zbliżonej znaczeniowo do przesłanki z art. 9 ust. 2 lit. b[7]) RODO, legalizującej przetwarzanie szczególnych kategorii danych osobowych[895].

Samo wdrożenie w organizacji wymogów wynikających z Ogólnego Rozporządzenia o Ochronie Danych Osobowych nie zapewnia jeszcze zgodności w zakresie przetwarzania danych osobowych. Firmy muszą dostosowywać zasady prowadzenia działalności do szeregu aktów prawnych uzupełniających RODO. W przedsiębiorstwach coraz częściej zwraca się uwagę na sposób prowadzenia dokumentacji obejmującej obszar ochrony danych osobowych, na rolę, jaką pełni inspektor ochrony danych osobowych, czy na prawa podmiotów danych. Świadomie podejmuje się działania dostosowujące funkcjonowanie przedsiębiorstwa do Rozporządzenia i przepisów sektorowych.

Zagwarantowanie adekwatnego do ryzyka poziomu bezpieczeństwa danych osobowych sprowadza się do zastosowania przez administratora odpowiednich środków technicznych i organizacyjnych. Należy przy tym uwzględnić stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst, cele przetwarzania i ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze. Te rozwiązanie jest potwierdzeniem przyjętego w unijnym Rozporządzeniu podejścia opartego na ryzyku[896]. Innymi słowy, administratorzy danych osobowych zobowiązani są do samodzielnego dokonania analizy ryzyka związanego z przetwarzaniem danych, tak aby dobrać należyte do zagrożeń środki techniczne i organizacyjne, zapewniające bezpieczeństwo danych osobowych. Przykłady takich środków, bez podawania konkretnych technik, unijny prawodawca wskazuje w art. 32 ust. 1 RODO, co świadczy o zachowaniu elastyczności technicznej przyjętych regulacji prawnych. Wydaje się to być spowodowane pojawianiem się coraz to nowszych niebezpieczeństw, które wymagają od administratora dokonywania bieżących przeglądów i aktualizacji przyjętych zabezpieczeń.

Pseudonimizacja danych różni się od anonimizacji tym, że jest odwracalna. Proces ten polega na zamianie na pseudonim jednego identyfikatora osobistego lub kilku (imienia,

[895] Inaczej mówiąc, są to dane sensytywne (szczególnie wrażliwe).
[896] M. Jabłoński, J. Węgrzyn, *Prawo do bycia…,* s. 220.

adresu poczty elektronicznej, numeru PESEL). Anonimizację warto wykorzystać wtedy, kiedy administrator wyrażałby zamiar całkowitego i nieodwracalnego braku dostępu do danych.

Dokonując oceny stopnia bezpieczeństwa, administrator musi pamiętać o uwzględnieniu ryzyka wiążącego się z procesem przetwarzania, mogącego wynikać na podstawie art. 32 ust. 2 RODO z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Co istotne, przy realizacji obowiązku zapewnienia bezpieczeństwa przetwarzania, nie jest wymagane sporządzanie specjalnej dokumentacji. Wykazaniu tego obowiązku służy prowadzony przez administratorów rejestr czynności przetwarzania, w którym powinien znajdować się ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Rozwiązania nie przewidują ponadto powinności prowadzenia dokumentacji przetwarzania w postaci polityk ochrony danych. W praktyce, polityki są wdrażane przez administratorów danych osobowych, pomimo ich fakultatywnego charakteru. Ma to ułatwić nie tylko realizację obowiązku polegającego na prowadzeniu rejestru czynności przetwarzania, ale i sam proces przetwarzania danych. Polityki ochrony danych są stosowane także z uwagi na treść art. 5 ust. 2 RODO, gdzie administrator jest zobligowany do wykazania przestrzegania przepisów Rozporządzenia.

Przetwarzanie danych osobowych i ich bezpieczeństwo to niebagatelny problem. Podmiot danych ma świadomość swoich praw oraz możliwych do podjęcia działań w sytuacji naruszenia jego danych. Uprawniony do realizacji przysługujących mu praw, w tym „prawa do bycia zapomnianym", może inicjować postępowania nie tylko na podstawie wniesienia skargi do organu nadzorczego, ale także wykorzystując środki ochrony prawnej z art. 79 RODO, jakimi są powództwo cywilne, administracyjne kary pieniężne lub inne sankcje. Narzędzia te mają znaczenie dla ochrony danych osobowych.

Korzystając z uprawnienia wniesienia skargi do organu nadzorczego, należy wywieść, że podmiotem skarżącym może być zarówno obywatel państwa członkowskiego, jak i państwa trzeciego. Nie może być jednak reprezentowany przez osobę fizyczną, ponieważ umocowanym do wykonania tej czynności jest podmiot, organizacja lub zrzeszenie, niemające charakteru zarobkowego. Skargę można wnieść do organu nadzorczego każdego kraju członkowskiego – ze względu na miejsce zwykłego pobytu, miejsce pracy, czy miejsce popełnienia naruszenia. Na dowolność w wyborze organu nadzorczego, do którego można skierować skargę świadczy przede wszystkim termin „w szczególności".

Środek prawny z art. 79 RODO, polegający na dochodzeniu ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu uznawany jest za

niezależny od innych, gdyż nie wymaga uzyskania innych orzeczeń o charakterze administracyjnym lub sądowo-administracyjnym. Można go porównać w polskim porządku prawnym do zainicjowania postępowania przed sądem powszechnym. Za ukształtowaniem tego środka w trybie procesu przemawia sformułowanie z art. 79 RODO, świadczące o tym, że środek ten ma zostać wykorzystany przeciwko administratorowi lub podmiotowi przetwarzającemu. Ciężar dowodu z art. 6 k.c. spoczywa na osobie fizycznej, która dochodzi ochrony prawnej. Ograniczono go do wykazania sprzeczności postępowania strony przeciwnej z systemem prawnym krajowym i europejskim. Strona pozwana musi z kolei udowodnić, że proces przetwarzania danych osobowych trzeba uznać za zgodny z prawem, ponieważ jest on niezbędny dla ochrony interesu osoby, której dane dotyczą.

Dochodząc odpowiedzialności odszkodowawczej, zauważa się, że odpowiedzialność podmiotu przetwarzającego została zawężona w stosunku do odpowiedzialności administratora danych osobowych. Wynika to z tego, że każdy administrator ponosi odpowiedzialność za szkody spowodowane przetwarzaniem naruszającym przepisy Rozporządzenia, zaś podmiot przetwarzający jedynie wtedy, gdy nie dopełnił nałożonych na niego obowiązków lub gdy działał poza legalnymi instrukcjami administratora albo przeciwko nim. Z tego też można wywnioskować, że nie może powodować odpowiedzialności podmiotu przetwarzającego odpowiednie przez niego wykonywanie instrukcji administratora, nawet jeśli pozostają w sprzeczności z przepisami prawa.

Najwięcej obaw wywołują kary pieniężne, które powinny być stosowane w odpowiednich okolicznościach. Zachęca się organy nadzorcze do wykorzystywania „rozważnego i wyważonego podejścia w zakresie stosowania środków naprawczych, tak aby reakcja na dane naruszenie była zarówno skuteczna i odstraszająca, jak również proporcjonalna. Celem nie jest tu traktowanie kar pieniężnych jako ostateczności, czy też powstrzymywanie się od ich stosowania, lecz nakładanie ich w sposób uniemożliwiający podważanie ich skuteczności jako narzędzia”[897]. Podmioty danych, dzięki rozwiązaniom przyjętym w unijnym Rozporządzeniu, posiadają większe poczucie pewności prawa i jego stosowania w praktyce.

Istnieją też przepisy krajowe, których przestrzeganie wymaga przetwarzania danych osobowych. Zazwyczaj stanowią one elementy składowe norm kompetencyjnych czy proceduralnych i nie zostały przyjęte, aby wykonywać zadania z obszaru ochrony danych osobowych, ale by służyć realizacji innych celów. Czasem sprowadzają się one do

[897] Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych…*

szczegółowych norm określających kategorie danych, jakie należy zgromadzić w określonym celu wyrażone zazwyczaj w postaci załączników do rozporządzeń, a innym razem ograniczają się jedynie do wskazania tych celów. Pierwsze rozwiązanie, choć początkowo wydawało się być przemyślane, nasunęło z drugiej strony pewne wątpliwości, przynajmniej w kontekście tych przepisów, które były wydawane dotychczas i będą wydawane w przyszłości przed jeszcze głębszym poznaniem unijnego Rozporządzenia. Fundamentalne reguły, na których opiera się ten akt prawny nie stanowią żadnej nowości (mając na myśli zasadę celowości, adekwatności, czy zasadę ograniczenia czasowego), to jednak prawie każda jednostka spotkała się z koniecznością wypełniania różnych druków czy formularzy, których treści nie powinno uznawać się za dane osobowe. Niejednokrotnie miało to swoje uzasadnienie w braku rzeczywistej potrzeby przetwarzania tak pojemnego zakresu danych, w szczególności, gdy odbywało się to w sposób niedookreślony czy nietransparentny dla osoby, do której te dane się odnoszą. Przypadki takie będą miały miejsce, kiedy ustawodawca ustanawiając normy dotyczące zakresu przetwarzania danych, całkowicie lub częściowo pominie doprecyzowanie innych elementów, ważnych z punktu widzenia reguł ochrony danych[898].

O ile kiedyś, przytoczone wątpliwości można było niemalże lekceważyć, powołując się chociażby na regułę *lex specialis derogat legi generali,* to po dniu 25 maja 2018 roku normy RODO zaczęły być bezpośrednio stosowane przed ustawą czy zwykłym rozporządzeniem. Prowadzenie procesu legislacyjnego uwzględniającego dla ochrony danych etap oceny pozwala na uniknięcie najpoważniejszych uchybień, jednakże wyeliminowanie z systemu prawa norm wątpliwych z pewnością potrwa jeszcze przez wiele lat. Z punktu widzenia zagwarantowania należytego stosowania przepisów RODO bezpieczniejsze jest rozwiązanie sprowadzające się do tego, że to sam administrator danych osobowych ma ponosić odpowiedzialność za określenie rodzajów i zakresu zbieranych informacji, a co z tego wynika – powinien stosować się do reguł ogólnych, a więc ściśle przestrzegać reguł ustanowionych przez Unię Europejską.

[898] Powszechnym przykładem są oświadczenia majątkowe publikowane w Biuletynie Informacji Publicznej, gdzie brakuje terminów, czy chociażby reguł ustanawiających okres udostępniania informacji w tej formie.

Zakończenie

W dobie powszechnego dostępu do Internetu i rozwoju nowoczesnych technologii, informacje ze sfery prywatnej jednostki, w tym także jej dane osobowe, stały się nieocenione. Jednym z fundamentalnych aspektów życia każdego człowieka jest prywatność, ponieważ oprócz tego, że człowiek jest istotą społeczną, to posiada również wrodzoną potrzebę odrębności. Z uwagi jednak na dynamiczny rozwój cyfrowej rzeczywistości, prywatność trzeba rozumieć w dwojaki sposób – jako możliwość „bycia pozostawionym w spokoju" oraz jako prawo jednostki do samodzielnego decydowania o zakresie dostępu osób trzecich do informacji na jej temat. „Prawo do bycia zapomnianym" jawiło się jako odpowiedź na zmiany zachodzące w przestrzeni cyfrowej, zwłaszcza na te związane z rosnącą rolą wyszukiwarek internetowych, mediów społecznościowych oraz globalnej wymiany informacji on-line. Informacje, które niegdyś w przestrzeni analogowej podlegały naturalnemu zapomnieniu, w Internecie zyskały charakter trwały i dostępny, co prowadziło do nieśmiertelności danych osobowych.

W ocenie Autorki, przeprowadzone badania pozwoliły na osiągnięcie celów sformułowanych we wstępie pracy.

Po pierwsze, Autorka poddała szczegółowej analizie relacje między tzw. triadą praw. Analiza aksjologiczna potwierdziła, iż celem „prawa do bycia zapomnianym" jest ochrona godności, autonomii i prywatności podmiotów danych we współczesnym społeczeństwie informacyjnym.

Po drugie, Autorce udało się ukazać ewolucję „prawa do bycia zapomnianym" od czasów obwiązywania Dyrektywy 95/46/WE, poprzez przełomowe dla tej tematyki orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie *Google Spain* (C-131/12), aż po ujęcie tego prawa w art. 17 RODO. Autorka zbadała, jaki wpływ na polskie ustawodawstwo, mają regulacje unijne.

Po trzecie, Autorka w niniejszej pracy doprecyzowała zakres podmiotowy „prawa do bycia zapomnianym" oraz granice korzystania z tego prawa. Scharakteryzowała przesłanki umożliwiające podmiotom danych wysuwanie żądania usunięcia ich danych osobowych, jak również wyjątki od tego uprawnienia przewidziane w ust. 3 art. 17 RODO. W dysertacji podkreślono, że realizacja omawianego prawa napotyka liczne ograniczenia, zwłaszcza w kontekście konfliktu z wolnością słowa i prawem dostępu do informacji.

Po czwarte, Autorka zidentyfikowała istotne problemy teoretyczne i praktyczne związane z realizacją „prawa do bycia zapomnianym". Zwróciła uwagę m.in. na trudności

związane z technicznym usuwaniem danych z sieci internetowej, skuteczność procedur informowania o usunięciu danych, a także wyzwania, przed którymi stoją administratorzy danych oraz organy odpowiedzialne za egzekwowanie przepisów o ochronie danych osobowych.

Ukończenie pracy skłania Autorkę do wysnucia uogólniających wniosków – poniżej przedstawionych.

Na gruncie prawa krajowego, prawo do prywatności z art. 47 Konstytucji RP może być uznane za konglomerat wartości chronionych, w którego obrębie wyróżnia się charakterystyczne postaci prywatności i prawne gwarancje ich ochrony, do których należy ochrona danych osobowych z art. 51 Konstytucji RP. Prywatność pojmowana jako dobro osobiste nie została skodyfikowana w kodeksie cywilnym, jednak biorąc pod uwagę otwarty katalog wynikający *explicite* z art. 23, zarówno w nauce prawa, jak i w judykaturze, dopuszczono ochronę prywatności na mocy tego przepisu[899].

Prawo do ochrony danych osobowych jest bezpośrednio powiązane z prawem do prywatności. Postrzegane jest jako jego część lub rozwinięcie. Oba te prawa można zaliczyć do praw kolektywnych, choć można dyskutować, czy ochrona danych osobowych stanowi odrębne prawo. Łączy je wspólny cel, tj. ochrona prywatności.

Ochronie prywatności jednostki ma sprzyjać „prawo do bycia zapomnianym", które najpierw pojawiło się w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej, a następnie w art. 17 unijnego Rozporządzenia. Celem wejścia w życie Ogólnego Rozporządzenia o Ochronie Danych Osobowych było dostosowanie regulacji poświęconych ochronie danych osobowych do potrzeb społeczeństwa informacyjnego oraz realiów technologicznych. Reforma poprawiła wymiar ochrony danych osobowych powiązany z rynkiem wewnętrznym poprzez ograniczenie rozdrobnienia, wzmocnienie spójności i uproszczenie otoczenia regulacyjnego, a tym samym zlikwidowanie niepotrzebnych kosztów i ograniczenie ciężaru administracyjnego. Wpływ Rozporządzenia na polski porządek prawny był znaczący. Choć Rozporządzenie jest bezpośrednio stosowane, to wymagało przyjęcia odpowiednich przepisów krajowych w zakresie uzupełnienia i dostosowania polskiego prawa, zwłaszcza w obszarach, gdzie RODO pozostawia krajom członkowskim pewien zakres swobody regulacyjnej. W tym celu uchwalono ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych, która weszła w życie wraz z rozpoczęciem stosowania RODO. Ustawa ta m.in. określiła zasady funkcjonowania organu nadzorczego, czyli PUODO. Ponadto,

[899] Wyrok SA w Warszawie z dnia 3 kwietnia 2017 r., sygn. akt: I ACa 2462/15, Legalis 1720163.

doprecyzowała kwestie przetwarzania danych w kontekście zatrudnienia, bezpieczeństwa narodowego, czy działalności dziennikarskiej oraz wskazała sankcje administracyjne i procedury ich nakładania. W związku z wdrożeniem RODO, przeprowadzono szeroką nowelizację ponad 160 polskich aktów prawnych.

„Prawo do bycia zapomnianym" można zaliczyć do jednego z podstawowych elementów reformy europejskich przepisów ochrony danych osobowych. Od dłuższego czasu pozostawało pojęciem teoretycznym. Sama koncepcja znalazła zastosowanie w odniesieniu do instytucji zatarcia skazania w postępowaniu karnym. Z praktycznego punktu widzenia, stwierdzono jednak, że nie jest możliwe zagwarantowanie całkowitej skuteczności prawa, gdyż informacja przekazana do Internetu, może zostać utrwalona[900].

W obecnym kształcie „prawo do bycia zapomnianym" wprowadzono wprost do porządku prawnego w art. 17 Rozporządzenia nr 2016/679. Od 25 maja 2018 r., tj. od dnia, w którym przepisy RODO zaczęły być stosowane, każda osoba, której dane dotyczą jest uprawniona do żądania usunięcia danych osobowych jej dotyczących. Konstrukcja prawna uregulowana w art. 17 RODO wywodzi się z art. 12 lit. b) Dyrektywy 95/46/WE, w którym przewidziano uprawnienie do żądania usunięcia swoich danych. Niniejsze Rozporządzenie rozszerza jednak to uprawnienie, nadając mu miano „prawa do bycia zapomnianym". Prawo te nie jest instytucją całkowicie nową. Należy je traktować jako rozwinięcie i doprecyzowanie dotychczasowego porządku prawnego[901].

Jak wynika z powyższego, przed wprowadzeniem Rozporządzenia, obowiązującą regulacją była Dyrektywa 95/46/WE, której zamierzeniem było wprowadzenie jednolitego systemu ochrony danych osobowych, bowiem rozbieżności w stopniu ochrony praw i wolności jednostki mogły odnosić negatywny skutek dla przepływu danych pomiędzy państwami członkowskimi, co w rezultacie mogłoby doprowadzić do niezrealizowania wielu przedsięwzięć, jakich wykonanie zapewnia ustanowienie rynku wewnętrznego. W przeciwieństwie do przepisów RODO, kraje członkowskie miały pozostawiony margines swobody w podejmowanych działaniach. Dyrektywa jest o tyle istotna w świetle podjętych rozważań, ponieważ na jej podstawie Trybunał Sprawiedliwości Unii Europejskiej konstytuował „prawo do bycia zapomnianym". Zgodnie z art. 12 lit. b) Dyrektywy, państwa członkowskie były obowiązane zapewnić jednostce możliwość dochodzenia od administratora

[900] J. Rosen, *Free speech, privacy, and the Web that never forgets,* "Journal on Telecommunications&High Technology Law" 2011, nr 9, no. 2, s. 345.
[901] C. Pachnik, *Ewolucja „prawa do bycia zapomnianym" w prawie UE a korzystanie z prawa do wypowiedzi i informacji z uwzględnieniem dorobku ETPCz,* [w:] *Nowe standardy w ochronie danych osobowych,* Warszawa 2018, s. 224.

danych sprostowania, usunięcia lub zablokowania danych. Dyrektywa 95/46/WE jako akt prawa pochodnego była skierowana do państw, w związku z czym temu przepisowi nie można było nadać przymiotu posiadania skutku bezpośredniego w relacji horyzontalnej jednostki z jednostką[902]. Istniał obowiązek wydania aktu prawa krajowego, który dopiero wtedy stanowiłby źródło roszczenia w relacji prywatnoprawnej[903]. To doprowadziło do wniosku, że rzeczywista skuteczność ochrony prywatności jednostki nie była zapewniona jednakowo.

Brak jasności uregulowania na poziomie prawa unijnego oraz różnice w ustawodawstwach krajowych stały się powodem wystąpienia do Trybunału Sprawiedliwości Unii Europejskiej z pytaniami prawnymi. Wykreowane „prawo do bycia zapomnianym" w wyniku wydania wyroku TSUE w sprawie o sygn. akt: C-131/12 miało charakter wtórny, ponieważ odnosiło się nie tyle do usunięcia informacji, co do uniemożliwienia znalezienia informacji o jednostce poprzez wpisanie jej imienia i nazwiska w wyszukiwarce internetowej[904].

Zasięg tego prawa był ograniczony jedynie do żądania usunięcia przez operatora wyszukiwarki internetowej linków z listy wyników wyszukiwania mającego za punkt odniesienia imię i nazwisko. To wiązało się z tym, iż dotarcie do informacji było możliwe po wpisaniu w wyszukiwarce innego niż imię i nazwisko sformułowania. W doktrynie pojawiły się głosy przeciwne, m.in. takie, że przez podanie imienia i nazwiska można pozyskać informacje na temat więcej niż jednej osoby, niemniej jednak argument ten można potraktować jako zastrzeżenie do tezy, a nie jako jej obalenie.

Pozytywnie można ocenić uznanie przez Trybunał Sprawiedliwości Unii Europejskiej, że operatorzy wyszukiwarek internetowych nie tylko przetwarzają dane osobowe, ale także są ich administratorami, co umożliwia zobowiązanie ich do usunięcia z wyników wyszukiwania linków do stron internetowych zawierających informacje dotyczące danej osoby.

„Prawo do bycia zapomnianym" ma szerszy zakres zastosowania. Obejmuje nie tylko operatorów wyszukiwarek internetowych, ale też inne podmioty, którym można nadać status administratora. Rozszerzenie katalogu administratorów danych o dalsze podmioty, tj. Google czy Facebook odgrywa ogromną rolę w zwiększeniu ochrony danych osobowych, w tym

[902] Wyrok TSUE z dnia 4 grudnia 1974 r. w sprawie *Yvonne Van Duyn przeciwko Home Office,* sygn. akt: 41/74, [dostęp:] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:61974CJ0041.

[903] W orzeczeniach TSUE są wyrażane także odmienne stanowiska. Należą one do mniejszości. Tytułem przykładu można podać: wyrok TSUE z dnia 22 listopada 2005 r. w sprawie *W. Mangold przeciwko R. Helmowi,* sygn. akt: C-144/04, [w:] *European Court Reports ECR I 9981.*

[904] A. López-Tarruella, *Introduction: Google Pushing the Boundaries of Law, Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models,* red. A. López-Tarruella, Haga 2012, s. 1-8, pkt 2.

prywatności użytkowników.

W sytuacji, gdy podmiot danych wystąpi z żądaniem ich usunięcia, administrator jest zobligowany do usunięcia danych nie tylko z systemu, ale i z innych miejsc, gdzie je przetwarzał, np. z chmury czy dysków zewnętrznych, pod warunkiem ziszczenia się jednej przesłanki z art. 17 ust. 1 RODO, co świadczy też o szerszym zasięgu działania tego prawa. Co istotne, w przypadku upublicznienia danych osoby, której one dotyczą, administrator zgodnie z ust. 2 powinien poinformować administratorów przetwarzających te dane, że osoba ta żąda, aby usunęli wszelkie informacje na jej temat, co należy ocenić *in plus*.

Swoiste „prawo do bycia zapomnianym" ma swoje źródło w art. 7 i 8 Karty Praw Podstawowych. Trybunał Sprawiedliwości UE podkreślił, że w niektórych przypadkach, ze względu na rolę odgrywaną przez daną osobę w życiu publicznym, ingerencja w prawa podstawowe tego podmiotu jest umotywowana nadrzędnym interesem kręgu osób używających wyszukiwarek internetowych, sprowadzającym się do posiadania dostępu do danej informacji dzięki działaniu wyszukiwarki. Ponadto, TSUE w sprawie C-131/12[905] uznał, że „usunięcie linków z listy wyników może, w zależności od rodzaju wyszukiwanej informacji, oddziaływać na uzasadniony interes internautów potencjalnie zainteresowanych uzyskaniem dostępu do tej informacji, (…) należy dążyć do znalezienia punktu równowagi pomiędzy tym interesem a prawami podstawowymi, które przysługują tej osobie na podstawie art. 7 i 8 KPP. Choć niewątpliwie chronione na mocy tych postanowień prawa osoby, której dotyczą dane, są również co do zasady nadrzędne wobec tego interesu internautów, to jednak równowaga ta może, w szczególnych przypadkach, zależeć od charakteru rozpatrywanych informacji i od tego, jak istotne są one dla prywatności osoby, której dane dotyczą, oraz dla publicznego interesu w dysponowaniu tą informacją, który to z kolei interes może być uzależniony w szczególności od roli odgrywanej przez tę osobę w życiu publicznym". Konieczne jest zatem wzajemne wyważenie prawa do ochrony danych osobowych oraz prawa do wolności wypowiedzi i informacji. W konsekwencji wydania ww. wyroku zostały uznane prymat prawa do prywatności oraz potrzeba oceniania przepisów Dyrektywy z punktu widzenia praw podstawowych.

Trybunał Sprawiedliwości Unii Europejskiej zajął stanowisko, że źródłem uprawnienia nie jest samoistnie Dyrektywa, ale prawo podstawowe wynikające z ogólnych zasad prawa, którego treść Dyrektywa jedynie konkretyzuje. Choć nie zostało to wyrażone *explicite* w uzasadnieniu orzeczenia, to wynika z wykładni przyjętej w sprawie *Mangold*.

[905] Wyrok TSUE z dnia 13 maja 2014 r., sygn. akt: C-131/12 w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protecciön de Datos (AEPD) i Mariowi Costeja Gonzàlezowi*…

Analogiczne twierdzenia zawiera opinia Rzecznika Generalnego N. Jääskinena, gdzie posiłkując się orzeczeniem w sprawie *Volkerund Markus Schecke i Eifert*[906] podniósł, że każde przetworzenie danych osobowych w Internecie, bez względu na cel, w którym zostało dokonane, stanowi naruszenie prawa podstawowego wymagającego uzasadnienia[907]. Nie można jednak do końca się z tym zgodzić, ponieważ przekazanie informacji na swój temat oznacza nie tyle ingerencję w prawo podstawowe, co rezygnację z jego korzystania.

Analiza tezy orzeczenia TSUE doprowadziła też do wniosku, że „prawo do bycia zapomnianym" nie ma charakteru bezwzględnego. W art. 17 ust. 3 Rozporządzenia prawodawca unijny wymienił zamknięty katalog przesłanek wyłączających to prawo. Może ono zostać ograniczone też w prawie unijnym lub krajowym zgodnie z art. 23 RODO.

„Prawo do bycia zapomnianym" było przedmiotem dalszych rozstrzygnięć. W wyroku z dnia 8 grudnia 2022 roku[908] TSUE przypomniał, że prawo to nie zalicza się do praw bezwzględnych. Należy je postrzegać w kontekście jego funkcji społecznej i zgodnie z zasadą proporcjonalności dokonać jego wyważenia względem innych praw fundamentalnych.

Mimo że dążenie do wysokiej jakości ochrony danych zdaje się być w dzisiejszym świecie standardem międzynarodowym, to pewne elementy w zestawieniu z rozwojem nowych technologii są wciąż kontrowersyjne. W art. 17 Rozporządzenia uwidaczniają się luki prawne, które pozostawiają te uprawnienie niedookreślone. Nie zostały oznaczone procedury usuwania danych i informowania osób trzecich o skorzystaniu z „prawa do bycia zapomnianym". Jednakże, Rozporządzenie uprościło procedurę żądania „prawa do bycia zapomnianym", nie wymagając tym samym pisemnego wniosku osoby fizycznej. Pojawiają się również problemy techniczne, nasuwające pytanie, z jakiego źródła administrator danych osobowych powinien czerpać wiedzę na temat tego, że dane przez niego udostępnione zostały skopiowane przez inny podmiot. Z uwagi na szerokie spektrum powielania, jak też kopiowania różnorakich treści, kontrola nad rozprzestrzenianiem i rozpowszechnieniem informacji zdaje się być utrudniona, a wręcz niemożliwa.

„Prawo do bycia zapomnianym" stanowi ważny aspekt w ochronie danych osobowych i ochronie prywatności. Niemniej jednak, nawet jeśli może być uznane za skuteczne, ale nie będzie we właściwy sposób przestrzegane, to stanie się po prostu bezużyteczne. Koniecznym wymogiem dla ochrony prywatności jednostki w Internecie jest nadanie przedmiotowemu

[906] Wyrok TSUE z dnia 9 listopada 2010 r. w sprawie *W.M. Schecke i H. Eifert przeciwko L. Hessen,* sygn. akt: C-92/09, [w:] *European Court Reports ECR I-11063.*
[907] Opinia Rzecznika Generalnego Nila Jääskinena przedstawiona 25 czerwca 2013 roku…, pkt 119.
[908] Wyrok TSUE z dnia 8 grudnia 2022 r. w sprawie *TU i RE przeciwko Google LLC,* sygn. akt: C-460/20, [dostęp:] https://www.inforlex.pl/dok/tresc,FOB0000000000006365815,Wyrok-Trybunalu-wielka-izba-z-dnia-8-grudnia-2022-r-TU-i-RE-przeciwko-Google-LLC-sygn-C-460-20.html.

prawu wymiaru globalnego, ponieważ jurysdykcja, biorąc pod uwagę wirtualną rzeczywistość, staje się pojęciem abstrakcyjnym.

„Prawo do bycia zapomnianym", pomimo tego, że zostało ugruntowane w unijnym porządku prawnym, to nie doczekało się jednolitej implementacji we wszystkich państwach członkowskich, co prowadzi do poważnych skutków dla równości ochrony danych osobowych w środowisku cyfrowym. Różnice te zapewne mają swoje źródło w odmiennych tradycjach konstytucyjnych, jak i w zróżnicowanym podejściu do równoważenia prawa do prywatności z wolnością słowa, czy dostępem do informacji. Dla przykładu, w Niemczech i we Francji praktyka egzekwowania prawa do usunięcia danych jest rygorystyczna. Jeszcze większe dysproporcje występują pomiędzy porządkami prawnymi państw członkowskich UE a krajami trzecimi, w tym Stanami Zjednoczonymi, gdzie dominująca pozostaje wolność słowa i ochrona interesu publicznego, a nie prawo do prywatności.

W systemach prawnych, w których brak jest silnych instytucjonalnych mechanizmów kontroli, możliwość usuwania informacji z przestrzeni cyfrowej może stać się narzędziem cenzury. Osoby publiczne, funkcjonariusze państwowi mogą nadużywać prawa do usunięcia danych celem zacierania śladów swojej przeszłości. Z tego względu pojawiają się głosy postulujące wzmocnienie gwarancji proceduralnych, w tym obowiązku przeprowadzania testu proporcjonalności i oceny zasadności wniosków o usunięcie danych osobowych.

„Prawo do bycia zapomnianym" może być postrzegane nie tylko jako narzędzie ochrony danych, ale także jako punkt wyjścia do szerszej debaty o granicach prywatności i odpowiedzialności za przetwarzanie danych w społeczeństwie opartym na informacji.

Konstatując, przeprowadzone w pracy doktorskiej rozważania dotyczące prawa do prywatności, ochrony danych osobowych i „prawa do bycia zapomnianym" determinują stwierdzenie, iż rozwój społeczeństwa informacyjnego, a w tym globalny przepływ informacji, stawiają przed ustawodawcą jeszcze wiele wyzwań. Obecne regulacje nie są wolne od luk prawnych i problemów praktycznych.

W związku z powyższym, można sformułować następujące postulaty *de lege ferenda*:

1. Obowiązujące przepisy dotyczące „prawa do bycia zapomnianym" jawią się jako niedookreślone. Brak precyzyjnych wytycznych skutkuje różnicami w zakresie interpretacji zarówno na poziomie sądów krajowych, jak i w praktyce stosowania prawa przez administratorów danych osobowych.
2. W aktualnym stanie prawnym nie zostały w pełni wytłumaczone obowiązki administratorów danych w przedmiocie efektywnego usuwania danych oraz

informowania osób trzecich o skorzystaniu przez podmiot danych z „prawa do bycia zapomnianym", co stwarza ryzyko nieskutecznej realizacji tego prawa.

3. Należy rozważyć stworzenie takich narzędzi technologicznych, które będą wspierać użytkowników i administratorów danych osobowych przy wykonywaniu „prawa do bycia zapomnianym", przykładowo za pomocą automatycznych systemów informujących o usunięciu danych osobowych albo o ich kopiowaniu i powielaniu przez inne podmioty, co doprowadzi do zahamowania multiplikacji danych.
4. Zaleca się wprowadzenie dodatkowych obowiązków sprawozdawczych dla administratorów danych osobowych, które miałyby polegać na informowaniu osób, których dane dotyczą, o działaniach podjętych w związku z realizacją „prawa do bycia zapomnianym", co pozwoliłoby zwiększyć przejrzystość i zaufanie użytkowników.

Wnioski *de lege ferenda* zaprezentowane w niniejszym zakończeniu mogą okazać się pomocne we wskazaniu ewentualnych kierunków zmian legislacyjnych, które mogłyby zapewnić lepsze funkcjonowanie „prawa do bycia zapomnianym" w realiach cyfrowej przestrzeni.

Bibliografia

I. Akty normatywne

1. Akty konstytucyjne

Ustawa z dnia 17 marca 1921 r.-Konstytucja Rzeczypospolitej Polskiej (Dz. U. 1921 nr 44, poz. 267).

Ustawa Konstytucyjna z dnia 23 kwietnia 1935 r. (Dz. U. 1935 nr 30, poz. 227).

Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dniu 22 lipca 1952 r. (Dz. U. 1952 nr 33, poz. 232).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 nr 78, poz. 483).

2. Umowy międzynarodowe

Powszechna Deklaracja Praw Człowieka z dnia 10 grudnia 1948 r., [dostęp:] https://amnesty.org.pl/wp-content/uploads/2016/04/Powszechna_Deklaracja_Praw_Czlowieka.pdf.

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 roku (Dz. U. 1993 nr 61, poz. 284).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966 r. (Dz. U. 1977 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. Urz. UE 2003 nr 3, poz. 25).

3. Traktaty międzynarodowe

Statut Rady Europy z dnia 5 maja 1949 r. (Dz. U. 1994 nr 118, poz. 565). Traktat o Funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. (Dz. Urz. UE 2016 C 202).

Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz. Urz. UE 2016 C 202).

Traktat ustanawiający Konstytucję dla Europy z dnia 29 października 2004 r. (Dz. Urz. UE 2004 C 310).

Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z dnia 29 grudnia 2006 r. (Dz. Urz. UE C 2006 nr 321E).

Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską z dnia 13 grudnia 2007 r. (Dz. Urz. UE 2009 nr 203, poz. 1569).

4. Akty ustawodawcze

Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, Bundesgesetzblatt nr I.

Ustawa z dnia 14 czerwca 1960 r.-Kodeks postępowania administracyjnego (Dz. U. 2024, poz. 572).

Ustawa z dnia 23 kwietnia 1964 r.-Kodeks cywilny (Dz. U. 2024, poz. 1061).

Ustawa z dnia 17 listopada 1964 r.-Kodeks postępowania cywilnego (Dz. U. 2025, poz. 620).

Ustawa z dnia 26 stycznia 1984 r.-Prawo prasowe (Dz. U. 2018, poz. 1914).

Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. 2019, poz. 730).

Ustawa z dnia 19 grudnia 1989 r. o zmianie Konstytucji Rzeczypospolitej Ludowej (Dz. U. 1989 nr 75, poz. 444).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 nr 133, poz. 883 ze zm.).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2018, poz. 1669).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2024, poz. 1513).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019, poz. 1781).

5. Dyrektywy

Dyrektywa 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 (Dz. Urz. UE L 281, 23/11/1995 P. 0031-0050).

Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003).

Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, [dostęp:] https://eur-lex.europa.eu/eli/dir/2015/1535/oj.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, oraz w sprawie swobodnego przepływu takich danych, uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016).

6. Rozporządzenia

Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r.-Kodeks karny (Dz. U. 1932 nr 60, poz. 571).

Rozporządzenie (WE) Nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz. Urz. UE L 145, 31/05/2001, P. 0043-0048).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz. Urz. UE L 351 z 20.12.2012).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1).

7. Rezolucje i deklaracje

Deklaracja Parlamentu Europejskiego, Rady i Komisji z dnia 5 kwietnia 1977 r., [dostęp:] https://www.europarl.europa.eu/charter/docs/pdf/jointdecl_04_77_en_en.pdf.

Rezolucja o tworzeniu norm międzynarodowych w dziedzinie praw człowieka (rez. 41/120) przyjęta przez Zgromadzenie Ogólne NZ 4 grudnia 1986 r.

Rezolucja PE z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (2011/2025(INI)), [dostęp: 06.07.2011]

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL.

The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 29.06.2012, A/HRC/20/L.30.

General Assembly Resolution 68/167 on the right to privacy in the digital age, 18.12.2013.

The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 20.06.2014, A/HRC/26/L.24.

General Assembly Resolution 69/166 on the right to privacy in the digital age, 18.12.2014.

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 14 kwietnia 2016 r. w sprawie stanowiska Rady przyjętego w pierwszym czytaniu w celu przyjęcia RODO (Dz. Urz. UE 2018 C 58/252).

The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 27.06.2016, A/HRC/32/L.20.

General Assembly Resolution 71/199 on the right to privacy in the digital age, 16.11.2016.

II. Orzecznictwo

1. Europejski Trybunał Praw Człowieka (ETPCz)

Wyrok ETPCz z dnia 6 listopada 1980 r. w sprawie *Van Oosterwijck przeciwko Belgii*, sygn. akt: 7654/76, § 34, LEX nr 80814.

Wyrok ETPCz z dnia 26 marca 1987 r. w sprawie *Leander przeciwko Szwecji*, sygn. akt: 9248/81.

Wyrok ETPCz z dnia 14 września 1987 r. w sprawie *Gillow przeciwko Wielkiej Brytanii*, sygn. akt: 9063/80, § 55.

Wyrok ETPCz z dnia 24 kwietnia 1990 r. w sprawie *Kruslin przeciwko Francji*, sygn. akt: 11801/85.

Wyrok ETPCz z dnia 24 lutego 1998 r. w sprawie *Botta przeciwko Włochom*, sygn. akt: 21439/93, § 33.

Wyrok ETPCz z dnia 4 maja 2000 r. w sprawie *Rotaru przeciwko Rumunii*, sygn. akt: 28341/95, § 46.

Wyrok ETPCz z dnia 16 kwietnia 2002 r. w sprawie *Set Colas Est and Others przeciwko Francji*, sygn. akt: 37971/97, § 4.

Wyrok ETPCz z dnia 6 czerwca 2006 r. w sprawie *Segerstedt-Wiberg i inni przeciwko Szwecji*, sygn. akt: 62332/00.

Postanowienie ETPCz z dnia 29 czerwca 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*, sygn. akt: 54934/00, § 92-94.

Wyrok ETPCz z dnia 3 kwietnia 2007 r. w sprawie *Copland przeciwko Wielkiej Brytanii*, sygn. akt: 62617/00, § 44, [w:] M.A. Nowicki, *Europejski Trybunał Praw Człowieka. Wybór Orzeczeń 2007*.

Wyrok ETPCz z dnia 4 grudnia 2008 r. w sprawie *S. i Marper przeciwko Wielkiej Brytanii*, sygn. akt: 30562/04, 30566/04.

Wyrok ETPCz z dnia 30 lipca 2009 r. w sprawie *VgT przeciwko Szwajcarii*, sygn. akt: 32772/02, § 61.

Wyrok ETPCz z dnia 2 września 2010 r. w sprawie *Uzun przeciwko Niemcom*, sygn. akt: 35623/05, § 43.

Wyrok ETPCz z dnia 7 lutego 2012 r. w sprawie *von Hannover przeciwko Niemcom*, sygn. akt: 40660/08 oraz 60641/08, § 95.

Wyrok ETPCz z dnia 24 lipca 2012 r. w sprawie *Đorđević przeciwko Chorwacji*, sygn. akt: 41526/10, § 152.

Wyrok ETPCz z dnia 16 lipca 2013 r. w sprawie *Węgrzynowski i Smolczewski przeciwko Polsce*, sygn. akt: 33846/07, [dostęp:] https://etpcz.ms.gov.pl/etpccontent/$N/990000000000001_I_ETPC_033846_2007_Wy_2013-07-16_001.

2. Trybunał Sprawiedliwości Unii Europejskiej (TSUE)

Wyrok TSUE z dnia 12 listopada 1969 r. w sprawie *Stauder przeciwko Ulm*, sygn. akt: 29/69, EU:C:1969:57.

Wyrok TSUE z dnia 17 grudnia 1970 r. w sprawie *Internationale Handelsgesellschaft*, sygn. akt: 11/70.

Wyrok TSUE z dnia 4 grudnia 1974 r. w sprawie *Yvonne Van Duyn przeciwko Home Office,* sygn. akt: 41/74, [dostęp:] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:61974CJ0041.

Wyrok TSUE z dnia 10 kwietnia 1984 r. w sprawie *Sabine von Colson and Elisabeth Kamann przeciwko Land Nordrhein-Westfalen*, sygn. akt: C-14/83, EU:C:1984:153.

Wyrok TSUE z dnia 24 września 1985 r. w sprawie *The Queen, ex parte E.D.&F. Man (Sugar) Ltd przeciwko Intervention Board for Agricultural Produce (IBAP)*, sygn. akt: 181/84, EU:C:1985:359.

Wyrok TSUE z dnia 15 czerwca 2005 r. w sprawie *Dokter i inni*, sygn. akt: C-28/05.

Wyrok TSUE z dnia 22 listopada 2005 r. w sprawie *W. Mangold przeciwko R. Helmowi,* sygn. akt: C-144/04, [w:] *European Court Reports ECR I 9981.*

Wyrok TSUE z dnia 9 listopada 2010 r. w sprawie *W.M. Schecke i H. Eifert przeciwko L. Hessen,* sygn. akt: C-92/09, [w:] *European Court Reports ECR I-11063.*

Wyrok TSUE z dnia 21 grudnia 2011 r. w sprawach połączonych *C-411/10 i C-493/10* (Dz. Urz. UE C.2012.49.8).

Wyrok TSUE z dnia 13 maja 2014 r. w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, sygn. akt: C-131/12, [dostęp:] http://curia.europa.eu/juris/liste.jsf?language=pl&num=C-131/12.

Wyrok TSUE z dnia 6 października 2015 r. w sprawie *Schrems*, sygn. akt: C-362/14, [dostęp:] http://curia.europa.eu/juris/liste.jsf?td=ALL&language=pl&jur=C,T,F&num=C-362/14.

Wyrok TSUE z dnia 19 października 2016 r. w sprawie *Breyer*, sygn. akt: C-582/14, [dostęp:] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=PL.

Wyrok TSUE z dnia 21 grudnia 2016 r. w sprawach połączonych *Tele2 Sverige AB i Secretary of State for the Home Department*, sygn. akt: C-203/15 i C-698/15, [dostęp:] http://curia.europa.eu/juris/document/document.jsf;jsessionid=CDD148747DDB91158709E5CD59F825C6?text=&docid=186492&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=10671937.

Wyrok TSUE z dnia 5 czerwca 2018 r. w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, sygn. akt: C-210/16, [dostęp:] https://curia.europa.eu/juris/liste.jsf?language=pl&td=ALL&num=C-210/16.

Wyrok TSUE z dnia 24 września 2019 r. w sprawie *GC i in. przeciwko CNIL,* sygn. akt: C-136/17 (Dz. Urz. UE Seria C, 2019/C 399/02).

Wyrok TSUE z dnia 24 września 2019 r. w sprawie *Google LLC przeciwko Commission Nationale de l'Informatique et des Libertés (CNIL)*, sygn. akt: C-507/17, [dostęp:] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CC0507.

Wyrok TSUE z dnia 8 grudnia 2022 r. w sprawie *TU i RE przeciwko Google LLC,* sygn. akt: C-460/20, [dostęp:] https://www.inforlex.pl/dok/tresc,FOB0000000000006365815,Wyrok-Trybunalu-wielka-izba-z-dnia-8-grudnia-2022-r-TU-i-RE-przeciwko-Google-LLC-sygn-C-460-20.html.

3. Trybunał Konstytucyjny (TK)

Wyrok TK z dnia 19 czerwca 1992 r., sygn. akt: U 6/92, OTK 1992, nr 1, poz. 13.

Wyrok TK z dnia 21 listopada 1995 r., sygn. akt: K 12/95, OTK 1995, nr 1, poz. 15.

Uchwała TK z dnia 16 stycznia 1996 r., sygn. akt: W 12/94, OTK 1996, nr 1, poz. 4.

Wyrok TK z dnia 24 czerwca 1997 r., sygn. akt: K 21/96, OTK 1997, nr 2, poz. 23.

Wyrok TK z dnia 19 maja 1998 r., sygn. akt: U 5/97, OTK ZU 1998, nr 4, poz. 46.

Wyrok TK z dnia 21 października 1998 r., sygn. akt: K 24/98, OTK 1998, nr 6.

Wyrok TK z dnia 26 września 2000 r., sygn. akt: P 11/99, OTK 2000, nr 6, poz. 187.

Wyrok TK z dnia 13 lutego 2001 r., sygn. akt: K 19/99, OTK 2001, nr 2, poz. 30.

Wyrok TK z dnia 29 czerwca 2001 r., sygn. akt: K 23/00, OTK ZU 2001, nr 5, poz. 124.

Wyrok TK z dnia 19 lutego 2002 r., sygn. akt: U 3/01, OTK-A 2002, nr 1, poz. 3.

Wyrok TK z dnia 12 listopada 2002 r., sygn. akt: SK 40/01, OTK-A 2002, nr 6, poz. 81.

Wyrok TK z dnia 20 listopada 2002 r., sygn. akt: K 41/02, OTK-A 2002, nr 6, poz. 83.

Wyrok TK z dnia 11 maja 2005 r., sygn. akt: K 18/04, OTK-A 2005, nr 5, poz. 49.

Wyrok TK z dnia 20 czerwca 2005 r., sygn. akt: K 4/04, OTK-A 2005, nr 6, poz. 64.

Wyrok TK z dnia 12 września 2005 r., sygn. akt: SK 13/05 (Dz. U. 2005 nr 186, poz. 1566).

Wyrok TK z dnia 13 września 2005 r., sygn. akt: K 38/04 (Dz. U. 2005 nr 186, poz. 1567).

Wyrok TK z dnia 26 października 2005 r., sygn. akt: K 31/04, OTK ZU 2005, nr 9, poz. 103.

Wyrok TK z dnia 12 grudnia 2005 r., sygn. akt: K 32/04 (Dz. U. 2005 nr 250, poz. 2116); OTK-A 2005, nr 11, poz. 132.

Wyrok TK z dnia 20 marca 2006 r., sygn. akt: K 17/05, OTK-A 2006, nr 3, poz. 30.

Wyrok TK z dnia 30 października 2006 r., sygn. akt: P 10/06 (Dz. U. 2006 nr 202, poz. 1492).

Wyrok TK z dnia 11 maja 2007 r., sygn. akt: K 2/07 (Dz. U. 2007 nr 85, poz. 571).

Wyrok TK z dnia 17 czerwca 2008 r., sygn. akt: K 8/04, OTK-A 2008, nr 5, poz. 81.

Wyrok TK z dnia 17 lipca 2008 r., sygn. akt: SK 25/07, OTK-A 2008, nr 6, poz. 119.

Wyrok TK z dnia 29 września 2008 r., sygn. akt: SK 52/05 (Dz. U. 2008 nr 178, poz. 1103).

Wyrok TK z dnia 23 czerwca 2009 r., sygn. akt: K 54/07, OTK-A 2009, nr 6, poz. 86.

Wyrok TK z dnia 23 lutego 2010 r., sygn. akt: K 1/08, OTK-A 2010, nr 2, poz. 14.

Wyrok TK z dnia 18 lipca 2011 r., sygn. akt: K 25/09, OTK-A 2011, nr 6, poz. 57.

Wyrok TK z dnia 11 października 2011 r., sygn. akt: K 16/10 (Dz. U. 2011 nr 240, poz. 1436).

Wyrok TK z dnia 5 marca 2013 r., sygn. akt: U 2/11, OTK-A 2013, nr 3, poz. 24.

Wyrok TK z dnia 30 lipca 2014 r., sygn. akt: K 23/11 (Dz. U. 2014, poz. 1055).

Wyrok TK z dnia 20 stycznia 2015 r., sygn. akt: K 39/12, OTK-A 2015, nr 1, poz. 2.

Wyrok TK z dnia 14 lipca 2015 r., sygn. akt: K 2/13, OTK-A 2015, nr 7, poz. 100.

Wyrok TK z dnia 11 października 2016 r., sygn. akt: SK 28/15 (Dz. U. 2016, poz. 2200).

Wyrok TK z dnia 19 czerwca 2018 r., sygn. akt: SK 19/17, OTK-A 2018, poz. 42.

4. Naczelny Sąd Administracyjny (NSA)

Wyrok NSA z dnia 29 grudnia 1999 r., sygn. akt: I SA/Po 3057/98, ONSA 2001, nr 1, poz. 34.

Wyrok NSA z dnia 3 lipca 2009 r., sygn. akt: I OSK 633/08, [dostęp:] https://www.inforlex.pl/dok/tresc%2CNSA.2009.001.300207296%2CWyrok-NSA-z-dnia-3-lipca-2009-r-sygn-I-OSK-633-08.html?utm_source=chatgpt.com.

Wyrok NSA z dnia 19 maja 2011 r., sygn. akt: I OSK 1079/10, [dostęp:] http://orzeczenia.nsa.gov.pl/doc/42DC7AE3F0.

Postanowienie NSA z dnia 21 marca 2017 r., sygn. akt: I OSK 2500/16.

Wyrok NSA z dnia 11 kwietnia 2017 r., sygn. akt: I OSK 2170/15, LEX nr 2296415.

Wyrok NSA z dnia 9 lutego 2023 r., sygn. akt: III OSK 6781/21, [dostęp:] https://orzeczenia.nsa.gov.pl/doc/6C317F6401.

5. Sąd Najwyższy (SN)

Wyrok SN z dnia 19 stycznia 1982 r., sygn. akt: IV CR 500/01, OSNCP 1982, nr 8-9, poz. 123.

Wyrok SN z dnia 14 listopada 1986 r., sygn. akt: II CR 295/86, OSNCP 1988, nr 2-3, poz. 40.

Uchwała SN z dnia 20 września 1988 r., sygn. akt: III CZP 37/88, OSNCP 1989, nr 3, poz. 40.

Wyrok SN z dnia 8 kwietnia 1994 r., sygn. akt: III ARN 18/94, OSNP 1994, nr 4, poz. 550.

Wyrok SN z dnia 9 października 2002 r., sygn. akt: IV CKN 1402/00, Legalis nr 59130.

Wyrok SN z dnia 10 listopada 2005 r., sygn. akt: V CK 314/05, Legalis nr 181192.

Postanowienie SN z dnia 17 kwietnia 2007 r., sygn. akt: I PZ 5/07, OSNAPiUS 2008, nr 13-14, poz. 196.

Wyrok SN z dnia 17 lipca 2008 r., sygn. akt: II CSK 111/08, Legalis nr 133166.

Uchwała SN z dnia 2 czerwca 2010 r., sygn. akt: III CZP 37/10, [dostęp:] https://www.saos.org.pl/judgments/92394.

Wyrok SN z dnia 19 maja 2011 r., sygn. akt: I CSK 497/10, LEX nr 936483.

Wyrok SN z dnia 14 stycznia 2015 r., sygn. akt: II CSK 747/13, OSNC 2016, nr 1, poz. 9.

Wyrok SN z dnia 11 lutego 2015 r., sygn. akt: I CSK 868/1426, LEX nr 1677121.

6. Sądy powszechne (apelacyjne i okręgowe)

Wyrok SA w Gdańsku z dnia 25 kwietnia 2006 r., sygn. akt: I ACa 1877/05, LEX 466363.

Wyrok SA w Rzeszowie z dnia 10 grudnia 2010 r., sygn. akt: I ACa 376/09, Legalis 526614.

Wyrok SA w Warszawie z dnia 30 listopada 2012 r., sygn. akt: VI ACa 728/12, Legalis 739296.

Wyrok SA w Białymstoku z dnia 13 września 2013 r., sygn. akt: I ACa 374/13, Legalis 743003.

Wyrok SA w Warszawie z dnia 3 kwietnia 2017 r., sygn. akt: I ACa 2462/15, Legalis 1720163.

Wyrok SA w Warszawie z dnia 29 marca 2018 r., sygn. akt: I ACa 2267/15, LEX nr 2466241.

Wyrok SO w Warszawie z dnia 5 grudnia 2022 r., sygn. akt: XXV C 559/22, [dostęp:] https://orzeczenia.ms.gov.pl/content/$N/154505000007503_XXV_C_000559_2022_Uz_2022-12-05_002.

Wyrok SO w Warszawie z dnia 7 lutego 2023 r., sygn. akt: III C 280/22, [dostęp: 29.03.2023] https://orzeczenia.warszawa.so.gov.pl/details/$N/154505000000903_III_C_000280_2022_Uz_2023-02-28_001.

7. Wojewódzki Sąd Administracyjny (WSA)

Wyrok WSA w Warszawie z dnia 26 lutego 2009 r., sygn. akt: II SA/Wa 1685/08, LEX nr 519827.

8. Sądy zagraniczne

Griswold vs. Connecticut, U.S. 1965, nr 381.

Wyrok SPI (Sąd Pierwszej Instancji UE) z dnia 30 listopada 2004 r., sygn. akt: T-168/02, *IFAW Internationale Tierschutz-Fonds GmbH i in. przeciwko Komisji Wspólnot Europejskich*, Zbiór Orzeczeń 2004, pkt 58-59.

Wyrok SPI z dnia 8 listopada 2007 r., sygn. akt: T-194/04, *The Bavarian Lager Co Ltd przeciwko Komisji Wspólnot Europejskich*, Zbiór Orzeczeń 2007.

III. Literatura

1. Wydawnictwa zwarte

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne*, Warszawa 2020.

Adamski A., *Prawo karne komputerowe,* Warszawa 2000.

Alexy R., *Teoria praw podstawowych*, Warszawa 2010.

Balcerzak M., Gronowska B., Jasudowicz T., Lubiszewski M., Mizerski R., *Prawa człowieka i ich ochrona*, Toruń 2010.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Warszawa 2012.

Banaszak B., *Prawo konstytucyjne*, Warszawa 2001.

Banaszak B., *Prawo konstytucyjne*, Warszawa 2004.

Banaszak B., *Prawo konstytucyjne*, Warszawa 2008.

Banaszak B., *Prawo konstytucyjne*, Warszawa 2010.

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2007.

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013.

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016.

Benoit-Rohmer F., Klebes H., *Prawo Rady Europy. W stronę europejskiej przestrzeni prawnej,* przekł. M.A. Nowicki, Warszawa 2006.

Bernaczyk M., *Obowiązek bezwnioskowego udostępniania informacji publicznej*, Warszawa 2008.

Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne,* Warszawa 2003.

Boć J., *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, red. J. Boć, Wrocław 1998.

Boć J., *Prawo administracyjne*, Wrocław 2007.

Burczyński T., *Elektroniczna wymiana informacji w administracji publicznej,* Wrocław 2011.

Czubik A., *Prawo do prywatności: Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe,* Kraków 2013.

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy,* Warszawa 2008.

Fajgielski P., *Informacja w administracji publicznej-prawne aspekty gromadzenia, udostępniania i ochrony*, Warszawa 2007.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Fellner R., *The Right to be Forgotten in the European Human Rights Regime,* Műnchen 2014.

Freeman M., *Prawa człowieka,* Warszawa 2007.

Gałaj-Emiliańczyk K., *Tworzenie systemu ochrony danych osobowych krok po kroku,* Warszawa 2016.

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2014.

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu,* Warszawa 2011.

Garlicki L., Sarnecki P., *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* t. 3, Warszawa 2003.

Garlicki L., Zubik M., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. II, wyd. II, Warszawa 2016.

Gawroński M., Kunda K., *RODO. Przewodnik ze wzorami,* red. M. Gawroński, Warszawa 2018.

Goban-Klas T., *Media i komunikowanie masowe. Teorie i analizy prasy, radia, telewizji i Internetu,* Warszawa-Kraków 1999.

Górzyńska T., *Prawo do informacji i zasada jawności administracyjnej*. *Orzecznictwo Sądu Najwyższego, Naczelnego Sądu Administracyjnego i Trybunału Konstytucyjnego,* Kraków 1999.

Grabowski R., Grabowska S., Młynarska-Sobaczewska A., Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, Warszawa 2009.

Grzybowski K., *Autonomia informacyjna jednostki a zgoda na przetwarzanie przez pracodawcę danych osobowych*, Warszawa 2020.

Gudowski J., *Komentarz do kodeksu cywilnego. Księga trzecia. Zobowiązania,* red. G. Bieniek, t. 2, Warszawa 2011.

Hołda J., Hołda Z., Ostrowska D., Rybczyńska J.A., *Prawa człowieka. Zarys wykładu,* Warszawa 2008.

Izdebski H., *Doktryny polityczno-prawne. Fundamenty współczesnych państw,* Warszawa 2015.

Izdebski H., *Fundamenty współczesnych państw,* Warszawa 2007.

Jabłoński M., Jarosz-Żukowska S., *Prawa człowieka i systemy ich ochrony. Zarys wykładu,* Wrocław 2004.

Jabłoński M., Kornobis-Romanowska D., Wygoda K., *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym,* Wrocław 2017.

Jabłoński M., Węgrzyn J., *Prawo do bycia zapomnianym,* Wrocław 2021.

Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice: wolność informacji, prawo dostępu do informacji publicznej, ochrona danych osobowych,* Wrocław 2002.

Jabłoński M., Wygoda K., *Praktyczne znaczenie podstawowych pojęć RODO-wybrane zagadnienia,* Wrocław 2019.

Janowski J., *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniach administracji,* Warszawa 2009.

Jasiński F., *Karta Praw Podstawowych,* Warszawa 2003.

Jasudowicz T., *Administracja wobec praw człowieka,* Toruń 1996.

Kamiński I.C., *Słuszność i prawo. Szkic prawnoporównawczy,* Kraków 2003.

Knysiak-Molczyk H., *Granice prawa do informacji w postępowaniu administracyjnym i sądowoadministracyjnym*, Warszawa 2013.

Kordasiewicz B., *Jednostka wobec środków masowego przekazu,* Wrocław 1991.

Kornobis-Romanowska D., Łacny J., Wróbel A., *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz,* t. 3, Warszawa 2012.

Krasińska M., Mizerek S., *ABC wybranych zagadnień ustawy o ochronie danych osobowych,* Warszawa 2007.

Krasuki A., *Ochrona danych osobowych na podstawie RODO,* Warszawa 2018.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016.

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.

Leszczyński L., Liżewski B., *Ochrona praw człowieka w Europie-szkic zagadnień podstawowych,* Lublin 2008.

Lipowicz I., *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku,* red. J. Boć, Wrocław 1998.

Lipowicz I., *Uwagi do strategii poprawy skuteczności unijnych przepisów dotyczących ochrony danych osobowych przedstawionej przez Komisję Europejską,* przygotowane przez Stowarzyszenie „Naukowe Centrum Prawno-Informatyczne", Warszawa 2011.

Liszcz T., *Prawo pracy,* Warszawa 2011.

Litwiński P., Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* red. P. Litwiński, Warszawa 2018.

Lubasz D., *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Warszawa 2018.

López-Tarruella A., *Introduction: Google Pushing the Boundaries of Law, Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models,* red. A. López-Tarruella, Haga 2012.

Makowski P., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017.

Marcisz P., *Koncepcja tworzenia prawa przez Trybunał Sprawiedliwości Unii Europejskiej,* Warszawa 2015.

Mednis A., *Prawo do prywatności a interes publiczny,* Warszawa 2006.

Mednis A., *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 1999.

Michalski B., *Prawo dziennikarza do informacji,* Kraków 1974.

Milczarek E., *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w Internecie,* Warszawa 2020.

Morawska E.H., Gałka K., *Standardy ochrony praw człowieka w prawie europejskiej konwencji praw człowieka,* Ministerstwo Sprawiedliwości, Warszawa 2011.

Mucha M., *Obowiązki administracji publicznej w sferze dostępu do informacji,* Wrocław 2002.

Nowicki M.A., *Europejski Trybunał Praw Człowieka. Wybór orzeczeń 2007*, Kraków 2008.

Nowicki M.A., *Wokół Konstytucji i Europejskiej Konwencji Praw Człowieka*, Kraków 2001.

Orwell G., *Rok 1984,* Warszawa 2013.

Petrażycki L., *Wstęp do nauki polityki prawa,* Warszawa 1968.

Piechowiak M., *Filozofia praw człowieka. Prawa człowieka w świetle ich międzynarodowej ochrony,* Lublin 1999.

Podręcznik europejskiego prawa o ochronie danych, Urząd Publikacji Unii Europejskiej 2014.

Radwański Z., Olejniczak A., *Prawo cywilne-część ogólna,* wyd. 11, Warszawa 2005.

Rozmaryn S., *Konstytucja jako ustawa zasadnicza PRL,* Warszawa 1967.

Sadurski W., *Prawo przed sądem. Studium sądownictwa konstytucyjnego w postkomunistycznych państwach Europy Środkowej i Wschodniej,* Warszawa 2008.

Sakowicz A., *Prawnokarne gwarancje prywatności,* Kraków 2006.

Sakowska-Baryła M., *Prawo do ochrony danych osobowych,* Wrocław 2015.

Salwa Z., *Prawo pracy,* Olsztyn 1994.

Sarnecki P., *Konstytucja Rzeczypospolitej Polskiej. Komentarz do Art. 51,* III, red. L. Garlicki, Warszawa 2003.

Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Warszawa 2013.

Sobczak J., *Prawo prasowe. Podręcznik akademicki,* Warszawa 2000.

Stefanowicz B., *Informacja,* Warszawa 2004.

Stępień-Załucka B., *Wolności i prawa człowieka oraz obywatela w Konstytucji RP z dnia 2 kwietnia 1997 r. Zagadnienia wybrane,* Rzeszów 2021.

Szewczyk H., *Ochrona dóbr osobistych w zatrudnieniu,* Kraków 2007.

Szmulik B., Szymanek J., *Introduction to the Constitution of the Republic of Poland,* Warszawa 2019.

Taczkowska-Olszewska J., *Dostęp do informacji publicznej w polskim systemie prawnym,* Warszawa 2014.

Walczak K., *Prawo pracy i ubezpieczeń społecznych,* red. K.W. Baran, Warszawa 2017.

Wierzbołowski J., *Informacja i technologie informacyjne jako element przekształceń strukturalnych i systemowych w gospodarce światowej,* tom 46, Warszawa 1997.

Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.,* Warszawa 2000.

Wiśniewski L., *Prawo a wolność człowieka-pojęcie i konstrukcja prawna,* Warszawa 1997.

Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP,* Kraków 1999.

Wronkowska S., *Podstawowe pojęcia prawa i prawoznawstwa,* Poznań 2005.

Wronkowska S., Ziembiński Z., *Zarys teorii prawa,* Poznań 2001.

Wróblewski J., *Teoria racjonalnego tworzenia prawa,* Wrocław-Warszawa-Kraków-Gdańsk-Łódź 1985.

Wyrzykowski M., *Ochrona danych osobowych,* Warszawa 1999.

Young J.B., *Privacy,* Chichester 1978.

Zawadzka Z., *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną. Problem rozstrzygania konfliktu zasad,* Warszawa 2013.

Zieliński T., *Prawo pracy. Zarys systemu, cz. 2,* Warszawa-Kraków 1986.

Zwara A., Mednis A., Pisz M., *RODO. Przewodnik dla adwokatów i aplikantów adwokackich,* Warszawa 2018.

Żołyński J., *RODO. Prawo do zapomnienia w sferze zatrudnienia,* Warszawa 2018.

2. Artykuły w wydawnictwach zwartych

Banaszak B., *Ogólne wiadomości o prawach człowieka,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2002.

Banaszak B., *Zagadnienia podstawowe. Terminologia,* [w:] *System ochrony praw człowieka*, red. B. Banaszak, A. Bisztyga, K. Complak, M. Jabłoński, R. Wieruszewski, K. Wojtowicz, Kraków 2003.

Banaś M., Krzywonos A., *Prawo do obywatelstwa,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* Warszawa 2002.

Baran K.W., *O funkcjach zbiorowego prawa pracy uwag kilka,* [w:] *Prawo pracy a wyzwania XXI-go wieku. Księga jubileuszowa Profesora Tadeusza Zielińskiego,* red. M. Matey-Tyrowicz, L. Nawacki, B. Wagner, Warszawa 2012.

Błachut M., *Prawnicze interpretacje praw człowieka,* [w:] *Z zagadnień teorii i filozofii prawa. Lokalny a uniwersalny charakter interpretacji prawniczej,* Wrocław 2009.

Błaszczyńska A., *Prawo do odszkodowania i odpowiedzialność,* [w:] *Realizacja praw osób, których dane dotyczą na podstawie rodo,* red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017.

Błaś A., *Rodzaje źródeł prawa administracyjnego,* [w:] *Prawo administracyjne,* red. J. Boć, Wrocław 2010.

Boć J., *Prawo do prywatności i jego ochrona w prawie konstytucyjnym,* [w:] *Przetwarzanie i ochrona danych osobowych,* red. G. Szpor, Katowice 1998.

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,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2004.

Brewin C., *Europe,* [w:] *Foreign Policy and Human Rights. Issues and Responsem,* red. R.J. Vincent, Cambridge 1986.

Brieskorn N., *Ochrona danych osobowych a zagrożenie prywatności,* [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa 1999.

Cisek A., *Komentarz do art. 23-24*, [w:] *Kodeks cywilny. Komentarz do artykułów 1-534*, red. E. Gniewek, t. I, Warszawa 2004.

Davies S., *The Re-Engineering the Right to Privacy,* [w:] *Technology and Privacy: The New Landscape,* red. P.E. Agre, M. Rotenberg, Cambridge 1998.

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

Dobrzeniecki K., Przywora B., *Wnioski z badań,* [w:] *Ograniczenia praw i wolności w okresie pandemii COVID-19 na tle porównawczym. Pierwsze doświadczenia,* Warszawa 2021.

Dörre-Kolasa D., *Wpływ rozporządzenia ogólnego na zakres ochrony danych osobowych przetwarzanych w związku z zatrudnieniem,* [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2017.

Fajgielski P., *Funkcjonowanie portali internetowych-wybrane problemy prawne,* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* red. G. Szpor, W. Wiewiórowski, Warszawa 2012.

Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2018.

Fischer B., *Prawo do usunięcia danych,* [w:] *Realizacja praw osób, których dane dotyczą, na podstawie RODO,* red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017.

Frankiewicz A., *Regulacje wolności wypowiedzi w polskim porządku prawnym,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2002.

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

Garlicki L., *Komentarz do art. 8, Nb. 1,* [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, tom I, Komentarz do artykułów 1-18,* red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010.

Garlicki L., *Uwaga 5 do art. 34 Konstytucji,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, tom 3, Warszawa 2003.

Garlicki L., *Uwagi do wstępu do Konstytucji,* [w:] *Konstytucja RP. Komentarz,* red. L. Garlicki, t. 5, Warszawa 2007.

Gdula M., *Wprowadzenie do prawa do prywatności w prawie polskim,* [w:] *Ochrona prywatności w nowych technologiach. Publikacja Studenckiego Koła Naukowego Blok Prawa Komputerowego,* Wrocław 2015.

Gliszczyńska-Grabias A., Sękowska-Kozłowska K., *Komentarz do art. 17 MPPOiP,* [w:] *Międzynarodowy Pakt Praw Obywatelskich (osobistych) i Politycznych,* red. R. Wieruszewski, Warszawa 2012.

Górzyńska T., *Geneza i rozwój prawa do informacji,* [w:] *Prawo do informacji,* red. W. Góralczyk, Warszawa 2006.

Gronowska B., *Systematyka międzynarodowo chronionych praw człowieka,* [w:] *Prawa człowieka w sytuacjach nadzwyczajnych,* red. T. Jasudowicz, Toruń 1997.

Hliwa R., *Model ochrony praw człowieka w systemie Rady Europy. Mechanizmy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności,* [w:] *Ochrona praw człowieka w świecie,* red. L. Wiśniewski, Poznań 2000.

Jabłoński M., *Klasyfikacja wolności i praw jednostki w Konstytucji RP,* [w:] *Wolności i prawa jednostki w Konstytucji RP. Idee i zasady przewodnie konstytucyjnej regulacji wolności i praw jednostki w RP,* red. M. Jabłoński, tom I, Warszawa 2003.

Jabłoński M., *Zasada różnicowania zakresu realizacji konstytucyjnych wolności i praw jednostki w oparciu o kryterium obywatelstwa polskiego,* [w:] *Wolności i prawa jednostki w Konstytucji RP,* red. M. Jabłoński, tom I, Warszawa 2010.

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

Jarosz-Żukowska S., *Charakter i znaczenie wolności i praw jednostki wyrażonych w Rozdziale I Konstytucji RP,* [w:] *Prawa człowieka i system ich ochrony. Zarys wykładu,* Warszawa 2010.

Kański L., *Prawo do prywatności, nienaruszalność mieszkania i tajemnicy korespondencji,* [w:] *Prawa człowieka. Model prawny,* red. R. Wieruszewski, Wrocław 1991.

Kluska M., *Droga do ogólnego rozporządzenia o ochronie danych osobowych,* [w:] *Vademecum ABI cz. II-Przygotowanie do roli Inspektora Ochrony Danych,* red. T. Izydorczyk, M. Kluska, M. Kołodziej, Warszawa 2017.

Koksanowicz G., *Ochrona danych osobowych w świetle Konstytucji oraz Ustawy o ochronie danych osobowych,* [w:] *Konstytucyjny ustrój państwa. Księga jubileuszowa Profesora Wiesława Skrzydły,* red. T. Bojarski, E. Gdulewicz, J. Szreniawski, Lublin 2000.

Koncewicz T., *Zasada pierwszeństwa prawa wspólnotowego przed prawem krajowym w orzecznictwie Trybunału Sprawiedliwości Wspólnot Europejskich,* [w:] *Węzłowe problemy w orzecznictwie Trybunału Sprawiedliwości Wspólnot Europejskich,* red. B. Banaszkiewicz, Biuro Trybunału Konstytucyjnego 2003.

Kopff A., *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne),* [w:] *Studia Cywilistyczne,* tom XX, Kraków 1972.

Kuberska W., *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu,* [w:] *Realizacja praw osób, których dane dotyczą na podstawie rodo,* red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017.

Kulesza E., *Prawo obywateli do informacji o działalności podmiotów publicznych,* [w:] *Wolności i prawa jednostki oraz ich gwarancje w praktyce,* red. J. Wiśniewski, Warszawa 2006.

Leciak M., *Kultura jawności-Klauzula tajności. Dziennikarskie prawo do informacji a prawnokarna ochrona tajemnicy państwowej. Zarys problematyki,* [w:] *Znaczenie informacji w społeczeństwie obywatelskim. Wybrane aspekty prawne,* red. J. Marszałek-Kawa, B. Chludziński, Toruń 2007.

Lipowicz I., *Konstytucyjne podstawy ochrony danych osobowych,* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia,* red. P. Fajgielski, Lublin 2008.

Litwiński P., *Zasada autonomii informacyjnej w orzecznictwie Trybunału Konstytucyjnego a stosowanie przepisów o ochronie danych osobowych,* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia,* red. P. Fajgielski, Lublin 2008.

Łabno-Jabłońska A., *Zasada bezpośredniego obowiązywania konstytucyjnych praw i wolności jednostki. Analiza prawnoporównawcza,* [w:] *Podstawowe prawa jednostki i ich sądowa ochrona,* red. L. Wiśniewski, Warszawa 1997.

Łopatka A., *System Międzynarodowej Ochrony Praw Człowieka,* [w:] *Ochrona praw człowieka w świecie,* red. L. Wiśniewski, Bydgoszcz-Poznań 2000.

Machnikowski P., *Komentarz do art. 23, Nb. 2,* [w:] *Kodeks cywilny. Komentarz,* red. E. Gniewek, P. Machnikowski, Warszawa 2017.

Maciejewski M., *Prawo informacji-zagadnienia podstawowe,* [w:] *Prawo informacji, prawo do informacji,* red. W. Góralczyk, Warszawa 2006.

Mednis A., *Prawo do wniesienia skargi do organu nadzorczego,* [w:] *Realizacja praw osób, których dane dotyczą, na podstawie rodo,* Wrocław 2017.

Mednis A., *Prywatność od epoki analogowej do cyfrowej-czy potrzebna jest redefinicja?,* [w:] *Prywatność a jawność-bilans 25-lecia i perspektywy na przyszłość,* red. A. Mednis, Warszawa 2016.

Mędrala M., *Ochrona pracowniczych danych osobowych w postępowaniu sądowym w sprawach z zakresu prawa pracy,* [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* red. D. Dörre-Kolasa, Warszawa 2017.

Miąsik D., Wróbel A., *Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności,* [w:] *Europeizacja prawa administracyjnego. System Prawa Administracyjnego,* tom 3, red. R. Hauser, Warszawa 2014.

Mizerski R., *Wolność ekspresji,* [w:] *Prawa człowieka i ich ochrona. Podręcznik dla studentów prawa i administracji,* Toruń 2005.

Oleński J., Jaworski W., *Uwarunkowania patologii informacji i drogi jej zwalczania,* [w:] *Prawo informacji, prawo do informacji,* red. W. Góralczyk, Warszawa 2006.

Pachnik C., *Ewolucja „prawa do bycia zapomnianym" w prawie UE a korzystanie z prawa do wypowiedzi i informacji z uwzględnieniem dorobku ETPCz,* [w:] *Nowe standardy w ochronie danych osobowych,* Warszawa 2018.

Pazdan M., *Dobra osobiste i ich ochrona,* [w:] *Prawo cywilne-część ogólna,* red. M. Safjan, Warszawa 2012.

Piech M., *One stop shop. Mechanizmy podejmowania decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE,* [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych,* red. G. Sibiga, Warszawa 2016.

Piotrowski R., *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne,* [w:] *Prywatność a jawność-bilans 25-lecia i perspektywy na przyszłość,* red. A. Mednis, Warszawa 2016.

Piotrowski R., *Prawo do tożsamości informacyjnej i jego znaczenie w ustroju demokratycznym,* [w:] *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka,* red. J. Jaskiernia, Warszawa 2013.

Pryciak M., *Prawo do prywatności,* [w:] *Prawa człowieka: idea, instytucje, krytyka,* red. M. Sadowski, P. Szymaniec, Wrocław 2010.

Rzucidło 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., *Ochrona danych osobowych-granice autonomii informacyjnej,* [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa 1999.

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 2006.

Sarnecki P., *Komentarz do art. 47 Konstytucji Rzeczypospolitej Polskiej,* [w:] *Konstytucja Rzeczypospolitej Polskiej, Komentarz,* red. L. Garlicki, tom III, Warszawa 2003.

Sarnecki P., *Uwaga 2 do art. 47,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, M. Zubik, tom II, Warszawa 2016.

Siewicz K., *Prywatność w serwisach społecznościowych. Nowe wyzwania dla ruchu wolnego oprogramowania,* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* red. G. Szpor, W. Wiewiórowski, Warszawa 2012.

Skrzydło W., *Konstytucyjny katalog wolności i praw jednostki,* [w:] *Konstytucyjne wolności i prawa w Polsce. Zasady ogólne,* red. M. Chmaj, tom I, Kraków 2002.

Sławiński A.A., *„Prawo do bycia zapomnianym" w świetle ogólnego rozporządzenia o ochronie danych osobowych i orzecznictwa TSUE,* [w:] *Prawo do prywatności-współczesne wyzwania,* Warszawa 2019.

Sobczak J., *Komentarz do art. 7, Nb. 2,* [w:] *Karta Praw Podstawowych Unii Europejskiej,* Warszawa 2013.

Sobczak J., *Prawo do prywatności a wolność słowa i druku,* [w:] *Podstawowe problemy stosowania Konstytucji Rzeczypospolitej Polskiej. Raport wstępny,* red. K. Działocha, Warszawa 2004.

Sokolewicz W., *Komentarz do art. 61 Konstytucji,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, Warszawa 2005.

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

Sokolewicz W., *Wprowadzenie do rozdziału II Konstytucji RP,* [w:] *Konstytucja Rzeczypospolitej Polskiej,* red. L. Garlicki, Warszawa 2005.

Szekely I., *The Right to Forget, The Right to be forgotten,* [w:] *European Data Protection: In Good Health?,* red. S. Gutwirth, R. Leenes, P. De Hert, Y. Poullet, Dordrecht 2012.

Szmulik B., *Ochrona prawna,* [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz Encyklopedyczny,* red. W. Skrzydło, S. Grabowska, R. Grabowski, Warszawa 2009.

Szmulik B., *Prawa człowieka-pojęcie, geneza oraz klasyfikacja,* [w:] *Dylematy praw człowieka,* red. T. Gardocka, J. Sobczak, Toruń 2008.

Szot L., *"Prawo do bycia zapomnianym w sieci",* [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne,* red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017.

Szpor G., *Pojęcie informacji a zakres ochrony danych,* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia,* red. P. Fajgielski, Lublin 2008.

Szwarc-Kuczer M., *Komentarz do art. 42 Karty Praw Podstawowych,* [w:] *Karta Praw Podstawowych. Komentarz,* red. A. Wróbel, Warszawa 2013.

Szymanowska A., Wierzbowski M., *Granice ochrony danych osobowych,* [w:] *Prawne uwarunkowania wymiany informacji-nowe wyzwania,* red. K. Markowski, M. Wierzbowski, Warszawa 2009.

Szymańska L., *Prawo do ochrony życia prywatnego na podstawie art. 47, 49-51 Konstytucji RP-wybrane zagadnienia,* [w:] *Polska wobec europejskich standardów praw człowieka,* red. T. Jasudowicz, Toruń 2001.

Tinnefeld M.-Th., *Jak Internet zmienia prawne ramy prywatności,* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* red. G. Szpor, W. Wiewiórowski, Warszawa 2012.

Tinnefeld M.-Th., *Ochrona danych osobowych-kamień węgielny budowy Europy,* [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa 1999.

Volio F., *Legal Personality, Privacy and the Family,* [w:] *The International Bill of Rights: The Convent of Civil and Political Rights,* red. L. Henkin, New York 1981.

Wach S., *Administracyjno-prawne ograniczenia wolności jednostki w Polsce,* [w:] *Prawne aspekty wolności. Zbiór studiów,* red. E. Cała-Wacinkiewicz, D. Wacinkiewicz, Toruń 2008.

Wąglowski P., *Internet a dobra osobiste człowieka,* [w:] *Internet-fenomen społeczeństwa informacyjnego,* red. T. Zasępa, R. Chmura, Częstochowa 2001.

Wilbrandt-Gotowicz M., *Prywatność osoby fizycznej jako ograniczenie jawności informacji publicznych w świetle orzecznictwa sądów administracyjnych,* [w:] *Jawność i jej ograniczenia. Znaczenie orzecznictwa,* red. M. Jaśkowska, Warszawa 2014.

Wprowadzenie, Nb. 10, [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, tom I. Komentarz do artykułów 1-18,* red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010.

Wright D., De Hert P., *Enforcing Privacy. Regulatory, Legal and Technological Approaches,* [w:] *Springer International Publishing,* Cham 2016.

Wróbel A., *Obywatelstwo polskie a prawa i wolności konstytucyjne,* [w:] *Konstytucyjne wolności i prawa w Polsce. Zasady ogólne,* red. M. Chmaj, tom I, Kraków 2002.

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

Wyrzykowski M., *Status informacyjny obywatela,* [w:] *Prawo i ład społeczny. Księga ku czci profesor Anny Turskiej,* Warszawa 2000.

Żak J., *Koncepcja „prawa do bycia zapomnianym",* [w:] *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi,* red. M. Jabłoński, S. Jarosz-Żukowska, Wrocław 2014.

3. Artykuły w wydawnictwach ciągłych

Abeyrante R., *Attacks on America-Privacy implications of heightened security measures In The United States, Europe and Canada,* "Journal of Air Law and commerce" 2002, nr 67.

Ambrose M.L., Ausloos J., *The right to be forgotten across the pond,* "Journal of Information Policy" 2013, nr 3.

Ambrose M.L., *It's about time: Privacy, Information Life Cycles, and the Right to be Forgotten,* "Stanford Law Review" 2013, nr 2.

Ball C.A., *Communitarianism and Gay Rights,* "Cornell Law Review" 2000, nr 85.

Bałaban A., *Opinia w sprawie interpretacji art. 61 Konstytucji RP z 2 kwietnia 1997 r.,* „Przegląd Sejmowy" 1999, nr 6.

Banaszewska A., *Prawo do prywatności we współczesnym świecie,* „Białostockie Studia Prawnicze" 2013, z. 13.

Baran B., Południak-Gierz K., *Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki,* „Zeszyty Naukowe Towarzystwa Doktorantów UJ" 2017, nr 2.

Barta J., Markiewicz R., *Granice wolności wypowiedzi w Internecie na tle prawa autorskiego i prawa mediów*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2008, z. 2.

Barta J., Markiewicz R., *Prawo do prywatności w społeczeństwie informatycznym,* „Ethos" 1999, nr 45-46.

Bennet S.C., *Right to be forgotten,* "Berkeley Journal of International Law" 2012, nr 30.

Bisztyga A., *Geneza Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz Europejskiego Trybunału Praw Człowieka,* „Prawa Człowieka-Humanistyczne Zeszyty Naukowe" 1994, nr 1(9).

Bjarnadóttir M.R., *Does the Internet Limit Human Rights Protection? The Case of Revenge Porn,* "JIPITEC" 2016, no. 7(3).

Błachnio-Parzych A., *Prawo do prywatności a dobra osobiste-zbieżność czy rozbieżność pojęć?*, „Państwo i Prawo" 2007, nr 10.

Błaszczyk M., *Instytucja zatarcia skazania w polskim prawie karnym,* „Studia Iuridica" 2006, t. XLVI.

Błoński D., Florczak-Wątor M., *Problem horyzontalnej skuteczności prawa do ochrony danych osobowych w świetle przepisów konstytucyjnych Polski i Szwajcarii,* „Przegląd Sejmowy" 2015, nr 1 (126).

Boling P., *Privacy As Autonomy vs. Privacy As Familial Attachment. A conceptual approach to right to privacy cases,* "Policy Studies Review" 1994, nr 13.

Carter E., *Argentina's right to be forgotten,* "Emory International Law Review" 2012, z. 27.

Ciechomska M., *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych,* „Monitor Prawniczy" 2017, nr 16.

Czerniawski M., *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych,* „Europejski Przegląd Sądowy" 2015, nr 5.

Denning B., Reynolds G., *Comfortably Penumbral,* "Boston University Law Review" 1997, vol. 77.

Dobosz I., *Przesłanki cywilnoprawnej ochrony przed podsłuchem,* „Zeszyty Naukowe UJ. Prace z Wynalazczości i Ochrony Własności Intelektualnej" 1992, nr MLXII.

Dolgin J.L., *The family in transition. From Griswold to Eisenstadt and Beyond,* "Georgetown Law Journal" 1994, nr 82.

Elger B., *Consent and anonymization in research involving biobanks,* "EMBO reports" 2007, nr 7.

Finnell D., *Invasions of privacy,* "The Laurel Review" 1993, nr 27.

Fleszer D., *Godność i prywatność osoby w świetle Konstytucji Rzeczypospolitej Polskiej,* „Roczniki Administracji i Prawa" 2015, nr 15.

Garlicki L., Zubik M., *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* „Wydawnictwo Sejmowe" 2016, nr 2.

Gavison R., *Privacy and the Limits of Law,* "The Yale Law Journal" 1980, nr 3.

Gerety T., *Redefining Privacy,* „Harvard Civil Rights-Civil Liberties Law Review" 1977, nr 12.

Glancy D., *The Invention of the right to privacy,* "Arizona Law Review" 1979, nr 21.

Gliszczyńska-Grabias A., Sękowska-Kozłowska K., Wieruszewski R., *Koncepcja Światowego Trybunału Praw Człowieka,* „Państwo i Prawo" 2011, nr 5.

Gonera K., Łętowska E., *Artykuł 190 Konstytucji i jego konsekwencje w praktyce sądowej,* „Państwo i Prawo" 2003, nr 53/9.

Goździaszek Ł., *Prawo do bycia zapomnianym w wyszukiwarce internetowej-glosa do wyroku Trybunału Sprawiedliwości z 13.05.2014 r. w sprawie C-131/12 Google Spain SL i Google Inc. przeciwko Agencia de Protección de Datos (AEPD) i Mario Costeja Gonzàlez,* „Europejski Przegląd Sądowy" 2015, nr 2.

Górski M., *Właściciel fanpage'a na portalu społecznościowym jako administrator,* „ABI Expert" 2018, nr 3.

Green L., *The right to privacy,* "Illinois Law Review" 1932, nr 27.

Grzegory T., *Pamięć absolutna czy kontrolowana amnezja-wybrane problemy prawne regulacji „prawa do bycia zapomnianym" w ogólnym rozporządzeniu o ochronie danych,* „Monitor Prawniczy" 2016, nr 20.

Grzelak A., *Prawo do bycia zapomnianym-założenia i kontrowersje*, „Europejski Przegląd Sądowy" 2018, nr 1.

Grzybowski K., *Autonomia informacyjna jednostki a zgoda na przetwarzanie przez pracodawcę danych osobowych,* „Przegląd Sejmowy" 2020, nr 6 (161).

Hornung G., Schnabel Ch., *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination,* "Computer Law&Security Report" 2009, nr 1.

Jakimowicz W., *O publicznych prawach podmiotowych,* „Państwo i Prawo" 1999, nr 1.

Jendrośka J., Stoczkiewicz M., *Ustawa o dostępie do informacji publicznej a regulacje szczególne,* „Państwo i Prawo" 2003, z. 6.

Kalinowska N., Litwiński P., *Ocena skutków dla ochrony danych i uprzednie konsultacje-nowe obowiązki podmiotów przetwarzających dane osobowe,* „Monitor Prawniczy" 2017, nr 13.

Katz A., *Privacy and Pornography: Stanley vs. Georgia,* "Supreme Court Review" 1969.

Kawecki M., *Prawo do bycia zapomnianym jako nowa postać prawa do prywatności w środowisku cyfrowym*, „Monitor Prawniczy" 2016, nr 17.

Kawecki M., *Prawo do bycia zapomnianym w kontekście przetwarzania danych osobowych w Internecie-problem zrównoważonego podejścia*, „Internetowy Przegląd Prawniczy TBSP UJ" 2013, nr 1.

Kawecki M., *Zakres stosowania przepisów ogólnego rozporządzenia o ochronie danych-wybrane problemy praktyczne*, „Europejski Przegląd Sądowy" 2017, nr 11.

Kędzia Z., *Pojęcie „prawa i wolności obywatelskie" (Uwagi na tle ustawy o Rzeczniku Praw Obywatelskich),* „Państwo i Prawo" 1989, z. 3.

Kępiński M., *Ocena stanu przepisów prawa cywilnego ujętych w kodeksie cywilnym po roku 1997,* „Przegląd Legislacyjny" 2001, nr 3.

Klimas D., *Prawo do zapomnienia-postulaty de lege lata i de lege ferenda,* „Prawo Mediów Elektronicznych" 2014, nr 2.

Kondak I., *Kto chce, ten wie,* „Rzeczpospolita" z dnia 10.06.2002 r.

Kondak I., *Prawo do informacji publicznej w świetle standardów Rady Europy,* „Państwo i Prawo" 2007, nr 3.

Kordasiewicz B., *Cywilnoprawna ochrona prawa do prywatności,* „Kwartalnik Prawa Prywatnego" 2000, z. 1.

Kozik P., *Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego,* „Europejski Przegląd Sądowy" 2017, nr 5.

Kozłowski M., *Jak kosmos pomógł Internetowi,* „Rzeczpospolita" z dnia 18.08.2016 r.

Krzysztofek M., *"Prawo do bycia zapomnianym" i inne aspekty prawa prywatności w epoce Internetu w prawie Unii Europejskiej,* „Europejski Przegląd Sądowy" 2012, nr 8.

Krzysztofek M., *Zmiana przepisów o zgodzie na przetwarzanie danych osobowych,* „Przegląd Prawa Handlowego" 2011, nr 4.

Kubiński K.W., *Ochrona życia prywatnego człowieka,* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1993, z. 1.

Kulesza E., *Konstytucyjne prawo do ochrony danych osobowych i jego ustawowa realizacja,* „Human Rights HZN" 2000, nr 7.

Leja P., *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych,* „Prawo Mediów Elektronicznych" 2017, nr 3.

Litwiński P., *Hosting danych osobowych. Zagadnienia podstawowe,* „Monitor Prawniczy" 2008, nr 23.

Łakomiec K., *Konstytucyjne gwarancje ochrony prywatności informacyjnej wobec rozwoju nowych technologii,* „Przegląd Legislacyjny" 2015, nr 1.

Łakomy J., *Prawa człowieka w perspektywie interdyscyplinarnej,* „Wrocławskie Studia Erazmiańskie" 2010, tom IV.

Mączyński A., *Prawo do prywatności wobec zagrożeń wynikających z rozwoju społeczeństwa informacyjnego*, „Przegląd Sejmowy" 2002, nr 2.

Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej,* „Państwo i Prawo" 1997, z. 6.

Michałowska K., *Prawo do życia rodzinnego na tle ogólnie pojmowanej prywatności jednostki,* „Zeszyty Naukowe UEK" 2013, nr 911.

Mielnik Z., *Prawo do prywatności (zagadnienia wybrane),* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, z. 2.

Młynarska-Sobaczewska A., *Konstytucyjne wskazania podmiotów praw człowieka,* „Studia Prawno-Ekonomiczne" 2004, tom 70.

Młynarska-Sobaczewska A., *Prawo do informacji jako element konstytucyjnego statusu jednostki*, „Przegląd Sejmowy" 2002, nr 2.

Motyka K., *Prawo do prywatności,* „Zeszyty naukowe Akademii Podlaskiej w Siedlcach" 2010, nr 85.

Mrózek A., *Prawno-polityczne problemy funkcjonowania banków danych w państwach burżuazyjnych,* „Państwo i Prawo" 1976, nr 8-9.

Musiała A., *Prawo pracy: prawo publiczne czy prawo prywatne,* „Praca i Zabezpieczenie Społeczne" 2017, nr 12.

Nowak K., *Kompetencje głowy państwa w zakresie zwierzchnictwa nad siłami zbrojnymi i bezpieczeństwa państwa w okresie prowizorium konstytucyjnego Polski Ludowej (1944-1952),* „Ius et Administratio" 2013, nr 3.

Osiatyński W., *Prawa człowieka-uniwersalizm i różnorodność,* „Państwo i Prawo" 2013, nr 11.

Piotrowski R., *Demokratyczne państwo prawne a lustracja,* „Państwo i Prawo" 2007, nr 6.

Prosser W., *Privacy,* „California Law Review" 1960, nr 48.

Pryciak M., *Prawo do prywatności,* „Studia Erasmiana Wratislaviensia" 2010, nr 4.

Rojszczak M., *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE,* „Prawo Mediów Elektronicznych" 2017, nr 3.

Rosen J., *Free speech, privacy, and the Web that never forgets,* "Journal on Telecommunications&High Technology Law" 2011, nr 9, no. 2.

Rosen J., *The right to be forgotten,* "Stanford Law Review" 2012, vol. 88.

Rustad M.L., Kulevska S., *Reconceptualizing the right to be forgotten to enable transatlantic data flow,* "Harvard Journal of Law&Technology" 2015, nr 2.

Rutkowska P., *"Prawo do bycia zapomnianym" w cyfrowym świecie. Wybrane zagadnienia,* „Społeczeństwo i Polityka" 2019, nr 1 (58).

Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informacyjnym,* „Państwo i Prawo" 2002, nr 6.

Safjan M., *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych,* „Kwartalnik Prawa Publicznego" 2002, z. 1.

Sakowicz A., *Prywatność jako samoistne dobro prawne (per se),* „Państwo i Prawo" 2006, nr 1.

Sandel M., *Moral Argument and Liberal Toleration: Abortion and Homosexuality,* "California Law Review" 1989, nr 77.

Seidman L.M., *The problems with privacy's problem,* "Michigan Law Review" 1995, nr 93.

Shoor E., *Narrowing the right to be forgotten: why the European Union needs to amend the proposed data protection regulation,* "Brooklyn Journal of International Law" 2014, nr 38.

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych-wybrane zagadnienia,* dodatek do „Monitora Prawniczego" 2016, nr 20.

Siejnik D., *Obowiązek informacyjny w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2018, nr 3.

Sieńczyło-Chlabicz J., *Dozwolona krytyka prasowa osób pełniących funkcje publiczne w orzecznictwie ETPCz,* „Europejski Przegląd Sądowy" 2007, nr 4.

Siostrzonek-Siergiel A., *Prawo do prywatności a bezpieczeństwo publiczne realizowane przez proces karny,* „Kultura bezpieczeństwa. Nauka-Praktyka-Refleksje" 2014, nr 16.

Skrzydło J., *Wolność słowa a ochrona prywatności osób powszechnie znanych w orzecznictwie ETPCz,* „Europejski Przegląd Sądowy" 2009, nr 7.

Sobczyk P., *Ochrona danych osobowych jako element prawa do prywatności,* „Zeszyty Prawnicze" 2009, nr 1.

Stuart A.H., *Google search results: buried if not forgotten,* "North Carolina Journal of Law & Technology" 2014, z. 15.

Symonides J., *Powszechna Deklaracja Praw Człowieka (po 60 latach od jej przyjęcia),* „Państwo i Prawo" 2008, nr 12.

Szmyt A., *W sprawie interpretacji art. 61 Konstytucji RP z 2 kwietnia 1997 roku,* „Przegląd Sejmowy" 1999, nr 6.

Szymielewicz K., Walkowiak A., *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem,* „Monitor Prawniczy" 2014, nr 9.

Świerczyński M., *Prawo do prywatności w prawie polskim i międzynarodowym*, „Państwo i Prawo" 2000, nr 3.

Tarnacka K., *Prawo do informacji w Polsce,* „Państwo i Prawo" 2003, nr 5.

Thomson J.J., *The right to privacy,* „Philosophy and public affairs" 1975, nr 4.

Vries K., *Identity, profiling algorithms and a world of ambient intelligence,* "Ethics and Information Technology" 2010, vol. 12, no. 1.

Wach M., *Prawo do prywatności osób publicznych w Stanach Zjednoczonych,* „Państwo i Prawo" 2004, nr 8.

Warren S.D., Brandeis L.D., *The right to privacy,* "Harvard Law Review" 1890, nr 4.

Weber R.H., *The right to be forgotten: More than a Pandora's Box?,* "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2011, nr 2.

Wiewiórowski W.R., *Nowe ramy ochrony danych osobowych w Unii Europejskiej,* „Monitor Prawniczy" 2012, Nr 7-dodatek specjalny „Ochrona danych osobowych 2012".

Wild M., *Ochrona prywatności w prawie cywilnym. Koncepcja sfer a prawo podmiotowe,* „Państwo i Prawo" 2001, nr 4.

Winczorek P., *Opinia w sprawie dostępu do informacji w Kancelarii Sejmu,* „Przegląd Sejmowy" 2003, nr 1.

Winczorek P., *Prawo obywatela do informacji,* „Rzeczpospolita" z dnia 24.02.2000 r.

Wróblewski M., *Karta Praw Podstawowych Unii Europejskiej w polskim sądownictwie-problemy i wyzwania,* „Kwartalnik Krajowej Rady Sądownictwa" 2015, nr 2.

Zubik M., *Opinia w sprawie dostępu do informacji w Kancelarii Sejmu,* „Przegląd Sejmowy" 2003, nr 1.

Żołyński J., *Glosa do wyroku SN z dnia 4 września 2013 r., sygn. akt: II PK 358/12,* „Praca i Zabezpieczenie Społeczne" 2014, nr 3.

IV. Inne materiały

1. Raporty

Report of the Office of the United Nations High Commissioner for Human Rights on ways to bridge the gender digital divide from a human rights perspective, [dostęp: 09.02.2017] http://www.ohchr.org/EN/Issues/Women/WRGS/Pages/WaystoBridgetheGenderDigital.aspx.

2. Komunikaty

Komunikat Komisji Europejskiej z dnia 13 września 1990 r. na temat ochrony jednostek w związku z przetwarzaniem danych osobowych we Wspólnocie oraz bezpieczeństwa informacji, COM (90) 314 final, CELEX: 51990DC0314.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej,* 4 listopada 2010 r., COM (2010) 609.

Komunikat Komisji do Parlamentu Europejskiego na podstawie art. 294 ust. 6 TFUE dotyczący stanowiska Rady dotyczącego przyjęcia Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylającego Dyrektywę 95/46/WE, Bruksela 11.04.2016, COM(2016)214 final, [dostęp:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52016PC0214.

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, [dostęp: 08.07.2019] https://monitorpolski.gov.pl/MP/2019/666.

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów-Europejski Zielony Ład, Bruksela, COM(2019)640 final, [dostęp: 11.12.2019] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52019DC0640.

Komunikat Komisji do Parlamentu Europejskiego i Rady, *Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej-dwa lata stosowania ogólnego rozporządzenia o ochronie danych,* COM(2020)264 final, [dostęp:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0264.

Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, *A European strategy for data,* Brussels, COM(2020)66 final, [dostęp: 19.02.2020] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

3. Strony internetowe

Barbaro M., Zeller T., *A Face Is Exposed for AOL Searcher No. 4417749,* [dostęp: 09.08.2006] https://www.nytimes.com/2006/08/09/technology/09aol.html.

Bernacka M.A., *Naruszenie ochrony danych osobowych,* [dostęp: 24.06.2022] https://www.parp.gov.pl/component/content/article/81837:naruszenie-ochrony-danych-osobowych.

Co zmienia nowe rozporządzenie o ochronie danych osobowych?, [dostęp: 07.02.2017] https://biznesalert.pl/zmienia-nowe-rozporzadzenie-o-ochronie-danych-osobowych/.

Czerniawski M., *Prawo do bycia zapomnianym w Internecie. Glosa do wyroku TS z dnia 13 maja 2014 r. C-131/12,* [dostęp: 02.03.2023] https://sip.lex.pl/komentarze-i-publikacje/glosy/prawo-do-bycia-zapomnianym-w-internecie-glosa-do-wyroku-ts-z-dnia-13-386107074.

Czym jest atak typu „brute force"?, [dostęp:] https://www.keepersecurity.com/pl_PL/threats/brute-force-attack.html.

Czym jest atak typu „credential stuffing"?, [dostęp:] https://www.keepersecurity.com/pl_PL/threats/credential-stuffing-attacks.html.

Dok. 5455/16, [dostęp: 28.01.2016] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN.

Dok. 9565/15, [dostęp: 11.06.2015] https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/pl/pdf.

Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, [dostęp:] https://rm.coe.int/16806a616c.

Dutch DPA imposes fine of €525,000 on Locatefamily.com, [dostęp: 12.05.2021] https://edpb.europa.eu/news/national-news/2021/dutch-dpa-imposes-fine-eu525000-locatefamilycom_pl.

Dutton W.H., Dopatka A., Law G., Nash V., *Freedom of Connection, Freedom of Expression, UNESCO Series on Internet Freedom,* [dostęp: 13.08.2017] http://unesdoc.unesco.org/images/0019/001915/191594e.pdf.

Dzieciuchowicz N., *Nowelizacja aktów prawnych w związku z obowiązywaniem RODO. Ustawa o ochronie danych osobowych z 10 maja 2018 jako akt wprowadzony w celu dostosowania polskiego prawa do przepisów unijnych,* [dostęp: 08.03.2023] https://lexdigital.pl/nowelizacja-aktow-prawnych-w-zwiazku-z-obowiazywaniem-rodo-ustawa.

Echaust-Przybytniak D., *Najnowsza ustawa o ochronie danych osobowych-2023 r.,* [dostęp: 26.03.2023] https://rkrodo.pl/najnowsza-ustawa-o-ochronie-danych-osobowych/.

Europejska chmura dla otwartej nauki (EOSC), [dostęp: 25.10.2024] https://digital-strategy.ec.europa.eu/pl/policies/open-science-cloud.

Factsheet on the „Right to be Forgotten" ruling (C-131/12), [dostęp: 29.06.2014] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2014/06/factsheet_data_protection_en.pdf.

Fioretti J., *Google sticks to EU only application of "right to be forgotten",* [dostęp: 20.09.2016] http://www.reuters.com/article/2015/01/19/us-google-eu-privacy-idUSKBNOKS21E20150119.

Fleischer P., *Foggy thinking about the right to oblivion,* [dostęp: 22.07.2014] http://peterflesicher.blogspot.com/2011/03/foggy-thinking-about-the-right-to-oblivion.html.

Gibbs S., *Facebook questions use of „right to be forgotten" ruling,* [dostęp: 20.09.2016] http://www.theguardian.com/technology/2015/jul/07/facebook-questions-use-of-right-to-be-forgotten-ruling.

Goodman E.P., *Practical Obscurity and The Right to Be Forgotten*: *"Pretty Much" Privacy is Enough,* [dostęp: 04.02.2015] https://medium.com/@ellgood/practical-obscurity-and-the-right-to-be-forgotten-pretty-much-privacy-is-enough-c321bdaffa08#.rksxmkgp9.

Google Transparency Report, stan na 13.06.2016, [dostęp: 20.09.2016] https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en.

https://www.google.com/transparencyreport/removals/europe-privacy/?hl=pl.

Greser J., *RODO. Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych,* [dostęp: 26.06.2018] https://publicystyka.ngo.pl/rodo-ocena-skutkow-planowanych-operacji-przetwarzania-dla-ochrony-danych-osobowych.

Grupa Robocza Artykułu 29 ds. Ochrony Danych, Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości, *Przyszłość prywatności,* [dostęp:] http://www.giodo.gov.pl/data/filemanager_pl/Dokument%20WP%20168%20wersja%20nieoficjalna.pdf.

Gudfinnsson M., *Obowiązek informacyjny w RODO,* [dostęp: 05.04.2018] https://blog-daneosobowe.pl/obowiazek-informacyjny-rodo/.

Gupta S., *The right to be forgotten,* [dostęp: 29.06.2014] https://www.lexology.com/library/detail.aspx?g=58540b9b-b571-48ed-9aab-4b70c34fb196.

Gutowski M., Kardas P., Pietrzak M., *Inwigilacja w obywateli, czyli wchodzimy w rok 1984,* [dostęp: 04.01.2016] https://prawo.gazetaprawna.pl/artykuly/915811,inwigilacja-w-obywateli-czyli-wchodzimy-w-rok-1984.html.

Gutowski P., *Prawo do bycia zapomnianym-usunięcie danych jako ochrona prywatności,* [dostęp: 22.02.2018] https://itls.pl/1063/prawo-do-bycia-zapomnianym-usuniecie-danych-jako-ochrona-prywatnosci/.

Herma M., *Za prywatność w internecie trzeba płacić,* [dostęp: 28.12.2014] https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1603593,1,za-prywatnosc-w-internecie-trzeba-placic.read.

House of Lords, European Union Committee, *EU Data Protection law: a "right to be forgotten"?,* Evidence, 2nd Report of Session 2014-15, [dostęp: 12.07.2015] https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf.

http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

https://alterweb.pl/-rodo-jak-dziala [dostęp: 07.04.2022].

https://archiwum.giodo.gov.pl/pl/1520296/10059.

https://ec.europa.eu/newsroom/article29/items/611236.

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52012SC0073.

https://gdpr.pl/artykuly/certyfikacja-rodo.

https://geobid.pl/aktualnosci/rodo-co-zmienia-nowe-prawo-o-ochronie-danych-osobowych.

https://giodo.gov.pl/261.

https://niezbednikrodo.pl/pl/blog/rodo-poradnik-dla-sektora-fintech/.

https://omnimodo.com.pl/ogolne-warunki-nakladania-administracyjnych-kar-pienieznych.

https://pl.wikipedia.org/wiki/Suma_kontrolna.

https://rodoradar.pl/motywy-61-75/.

https://websensa.com/pl/2020/05/13/strategiczne-pozyskiwanie-danych-jak-stac-sie-firma-ai-czesc-1/.

https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/.

https://www.iso.org/standard/85938.html.

https://www.pckp.pl/rodo-podstawowe-zalozenia,4,6248.

Jagielska P., *RODO: Jak usunąć dane osobowe z systemu informatycznego?,* [dostęp: 13.05.2018] https://biznes.gazetaprawna.pl/artykuly/1122751,rodo-usuwanie-danych-osobowych-z-systemu-informatycznego.html.

Jaworowska O., *Dane osobowe w kopiach zapasowych,* [dostęp: 03.12.2018] https://www.isecure.pl/blog/dane-osobowe-w-kopiach-zapasowych/.

Jędrzejak M., *RODO-rozporządzenie o ochronie danych: to trzeba wiedzieć,* [dostęp: 01.02.2018] https://business.trustedshops.pl/blog/rodo-co-trzeba-wiedziec/.

Kalisz I., *Szyfrowanie danych osobowych,* [dostęp:] https://przetwarzanie-danych-osobowych.pl/szyfrowanie-danych-osobowych/.

Kamińska-Kasjaniuk J., *Rejestr czynności przetwarzania danych osobowych zastąpi rejestrację zbiorów w GIODO,* [dostęp: 12.03.2018] https://odoserwis.pl/a/1175/rejestr-czynnosci-przetwarzania-danych-osobowych-zastapi-rejestracje-zbiorow-w-giodo.

Kamiński J., *Prawo do usunięcia danych a polityka retencji danych osobowych,* [dostęp:] https://www.roedl.pl/pl/warto-wiedziec/warto-wiedziec/rodo/prawo-do-usuniecia-danych-a-polityka-retencji-danych-osobowych.

Keller D., *The final draft of Europe's "Right to be forgotten law",* "The Center for Internet and Society", [dostęp: 17.12.2015] https://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law.

Klich A., *Boimy się wolności, marzymy o wspólnocie,* [dostęp: 18.01.2013] https://wyborcza.pl/magazyn/7,124059,13259382,boimy-sie-wolnosci-marzymy-o-wspolnocie.html?disableRedirects=true.

Komitet Praw Człowieka, *General comment No. 16: Article 17 (Right to privacy),* [dostęp:] http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx.

Komitet Praw Człowieka, *General comment No. 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant,* [dostęp:] http://www.ohchr.org/EN/HRBBodies/CCPR/Pages/CCPRIndex.aspx.

Kradzież danych osobowych w Internecie, [dostęp: 13.04.2023] https://lexdigital.pl/kradziez-danych-osobowych-w-internecie.

Kradzież tożsamości vs. oszustwo tożsamościowe, [dostęp: 14.05.2019] https://ochronatozsamosci.pl/blog/kradziez-tozsamosci-vs-oszustwo-tozsamosciowe-o35gc3-one.html.

Liddicoat J., *The Right to be Forgotten,* [dostęp:] https://www.privacy.org.nz/assets/Files/Speeches-presentations/Right-to-be-Forgotten-Joy-Liddicoat.pdf.

Marek A., *RODO w praktyce, lekcja 1,* [dostęp:] https://www.podatki.biz/media/File/RODO/RODO_w_praktyce_1.pdf.

Mączyński A., *Konstytucyjne prawa do godności i prawa do prywatności,* [dostęp: 16.04.2014] http://26konferencja.giodo.gov.pl/data/resources/MaczynskiA_paper.pdf.

Ministerstwo Cyfryzacji, *RODO-informator,* [dostęp: 12.01.2018] https://www.gov.pl/cyfryzacja/rodo-informator.

Na czym polega szyfrowanie danych?, [dostęp:] https://experience.dropbox.com/pl-pl/resources/what-is-encryption.

Naughton J., *In the battle of free speech now it's France vs. Google,* [dostęp: 20.09.2016] http://www.theguardian.com/commentisfree/2015/aug/09/battle-free-speech-france-google-right-to-be-forgotten.

Netia, *Szyfrowanie danych. Po co i jak to robić?,* [dostęp: 03.06.2020] https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/szyfrowanie-danych-jak-to-robic.

NETmundial Multistakeholder Statement, Sao Paulo 2014, s. 4, [dostęp: 09.02.2017] http://net-mundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

New Technologies: a challenge to privacy protection?; Data protection and media, [dostęp: 22.07.2014]

http://www.coe.int/t/dghl/standardsetting/dataprotection/reports_and_studies_en.asp?toPrint=yes&.

Norwegian DPA: Company fined for illegal forwarding of e-mail, [dostęp: 13.05.2021] https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-company-fined-illegal-forwarding-e-mail_pl.

Nosowski M., *Czy usunięcie danych dotyczy też kopii zapasowych?,* [dostęp: 05.12.2018] https://www.wsroddanych.pl/post/2018/12/05/czy-usuni%C4%99cie-danych-dotyczy-te%C5%BC-kopii-zapasowych.

Nowa ustawa o ochronie danych osobowych od 25 maja 2018 r., [dostęp: 23.05.2018] https://ksiegowosc.infor.pl/wiadomosci/783642,Nowa-ustawa-o-ochronie-danych-osobowych-od-25-maja-2018-r.html.

NSA: kasowanie danych osobowych możliwe dla archiwów prasowych. Adam Bodnar: de facto fałszowalibyśmy przeszłość, [dostęp: 03.03.2023] https://tvn24.pl/polska/nsa-kasowanie-danych-osobowych-mozliwe-dla-archiwow-prasowych-w-internecie-adam-bodnar-de-facto-falszowalibysmy-przeszlosc-st6793664.

Ocena skutków dla ochrony danych (DPIA)-wzór formularza, [dostęp: 08.08.2021] https://odo24.pl/blog-post.ocena-skutkow-dla-ochrony-danych-dpia-bezplatny-formularz.

Omówienie ustawy o ochronie danych osobowych z 10 maja 2018 roku, [dostęp:] https://gdpr.pl/omowienie-ustawy-o-ochronie-danych-osobowych-z-10-maja-2018-roku.

Polityka bezpieczeństwa danych, [dostęp: 08.11.2018] https://lexdigital.pl/polityka-bezpieczenstwa-danych-osobowych-rodo.

„Prawo do bycia zapomnianym": kontrowersje po wyroku korzystnym dla Google, [dostęp: 26.09.2019] https://cyberdefence24.pl/polityka-i-prawo/prawo-do-bycia-zapomnianym-kontrowersje-po-wyroku-korzystnym-dla-google.

Prawo do bycia zapomnianym-obowiązki administratora danych, [dostęp: 27.01.2021] https://spoldzielniaalbert.pl/2021/01/27/prawo-do-bycia-zapomnianym-obowiazki-administratora-danych/.

„Prawo do bycia zapomnianym" w Internecie, [dostęp: 15.03.2022] https://eur-lex.europa.eu/PL/legal-content/summary/right-to-be-forgotten-on-the-internet.html.

Przemówienie Sekretarza Generalnego ONZ w Senacie Włoch, [dostęp: 18.12.2019] https://press.un.org/en/2019/sgsm19916.doc.htm.

Przetacznik I., *RODO: Polityka Bezpieczeństwa-czy muszę ją mieć?,* [dostęp: 10.05.2018] https://legalnybiznesonline.pl/rodo-polityka-bezpieczenstwa/.

Pseudonimizacja-czym jest, jakie są jej cele i kiedy jest efektywna?, [dostęp: 03.02.2020] https://odo24.pl/blog-post.pseudonimizacja-wytyczne-enisa-rzucaja-nowe-swiatlo-na-jej-uzytecznosc.

Pułło A., *Konstytucja Stanów Zjednoczonych Ameryki,* Warszawa 2002, [dostęp:] libr.sejm.gov.pl.

Rada Europy, *Amendments approved by the Committee of Ministers,* Strasburg, [dostęp: 15.06.1999] http://rm.coe.int/168008c2b8.

Rekordowa kara dla administratora za naruszenie ochrony danych, [dostęp: 28.02.2022] https://uodo.gov.pl/pl/138/2389.

Rostkowska K., *RODO-zmiany w ochronie danych osobowych w 2018 roku. Najważniejsze informacje,* [dostęp: 28.12.2017] https://www.bankier.pl/wiadomosc/RODO-zmiany-w-ochronie-danych-osobowych-w-2018-roku-Najwazniejsze-informacje-7563322.html.

Ryzyko finansowe-dogłębne wyjaśnienie zagadnienia, [dostęp: 28.10.2019] https://academy.binance.com/pl/articles/financial-risk-explained.

Sierzputowski P., *Omówienie wyroku Trybunału Sprawiedliwości UE w sprawie C-136/17,* [dostęp: 30.09.2019] https://gdpr.pl/omowienie-wyroku-trybunalu-sprawiedliwosci-ue-w-sprawie-c-136-17.

Skibińska E., *„Prawo do bycia zapomnianym",* [dostęp: 12.01.2023] https://legalis.pl/prawo-do-bycia-zapomnianym/.

Słownik Języka Polskiego PWN, [dostęp: 20.06.2014] http://sjp.pwn.pl/slownik/2507328/pozyskać; http://sjp.pwn.pl/szukaj/gromadzić; http://sjp.pwn.pl/szukaj/udostępnić.

Specjalna ankieta Eurobarometru (EB) nr 359 „Ochrona danych i tożsamość elektroniczna w UE (2011)", [dostęp: 29.08.2017] https://commission.europa.eu/index_pl.

Szczudlik K., *Granice prawa do bycia zapomnianym,* [dostęp: 29.01.2019] https://newtech.law/pl/granice-prawa-do-bycia-zapomnianym/.

Szkutnik M., *Przepisy o ochronie danych osobowych, czyli nie tylko RODO,* [dostęp: 29.09.2020] https://blog-daneosobowe.pl/przepisy-o-ochronie-danych-osobowych-czyli-nie-tylko-rodo/.

Sztuwe A., *Polityka bezpieczeństwa zgodnie z RODO-czy trzeba ją nadal prowadzić?,* [dostęp: 16.04.2018] https://www.poradyodo.pl/aktualnosci-rodo/polityka-bezpieczenstwa-zgodnie-z-rodo-czy-trzeba-ja-nadal-prowadzic-8491.html#.

Szymielewicz K., *RODO na tacy. Odcinek II: Fair play-czyli o szacunku dla naszych wyborów,* [dostęp: 16.02.2018] https://panoptykon.org/wiadomosc/rodo-na-tacy-odcinek-ii-fair-play-czyli-o-szacunku-dla-naszych-wyborow.

Szymielewicz K., *RODO na tacy. Odcinek IV: O prawie do bycia zapomnianym (sic!) i zabrania danych ze sobą,* [dostęp: 11.04.2018] https://panoptykon.org/wiadomosc/rodo-na-tacy-odcinek-iv-o-prawie-do-bycia-zapomnianym-sic-i-zabrania-danych-ze-soba.

Ustawa o ochronie danych osobowych z 1997 r., [dostęp:] https://odo24.pl/rodo-uodo/ustawa-o-ochronie-danych-osobowych-z-1997-r/,.

Uzasadnienie do projektu Konwencji Rady Europy o dostępie do dokumentów urzędowych (CM/Del/Dec2008) 1025/4.3, [dostęp: 04.04.2008] http://assembly.coe.in.

Uzasadnienie do projektu ustawy o ochronie danych osobowych z dnia 13 września 2017 r., druk sejmowy nr 2410, Sejm VIII kadencji, [dostęp:] https://www.sejm.gov.pl/.

Warecka K., *Strasburg: „prawo do bycia zapomnianym" musi być w równowadze z prawem do informacji. M.L. i W.W. przeciwko Niemcom-wyrok ETPCz z dnia 28 czerwca 2018 r., połączone skargi nr 60798/10 i 65599/10,* [dostęp: 02.07.2018] https://www.prawo.pl/.

Wezgraj J., *Prowadzenie analizy ryzyka RODO-przykład,* [dostęp: 01.03.2019] https://www.pps.edu.pl/blog/prowadzenie-analizy-ryzyka-zgodnie-z-wymaganiami-rodo.

White Paper on Artificial Intelligence: a European approach to excellence and trust, Brussels, COM(2020)65 final, [dostęp: 19.02.2020] https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en?etransnolive=1.

Witkowska-Nowakowska K., *Ocena skutków dla ochrony danych. Kiedy należy przeprowadzić DPIA i na czym ona polega?,* [dostęp: 13.03.2020] https://portalodo.com/ocena-skutkow-dla-ochrony-danych-kiedy-nalezy-przeprowadzic-dpia-i-na-czym-ona-polega/.

Wojciechowski Ł., *Kary RODO nie działają,* [dostęp: 04.09.2022] https://statuo.pl/2022/09/04/kary-rodo-nie-dzialaja/.

www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_du_Droit.pdf.

Wydawcy pod ścianą po wyroku NSA. „Prawo do bycia zapomnianym" działa wstecz, [dostęp: 02.03.2023] https://www.rp.pl/dane-osobowe/art38050021-wydawcy-pod-sciana-po-wyroku-nsa-prawo-do-bycia-zapomnianym-dziala-wstecz.

Your rights matter: Data protection and privacy-Fundamental Rights Survey, [dostęp: 18.06.2020] https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

Zespół LexDigital, *Co to jest anonimizacja i pseudonimizacja,* [dostęp: 10.05.2018] https://lexdigital.pl/co-to-jest-anonimizacja-i-pseudonimizacja.

Zgoda na przetwarzanie danych osobowych według RODO, [dostęp: 19.05.2017] https://blog-daneosobowe.pl/zgoda-przetwarzanie-danych-osobowych-rodo/.

Zygmanowski B., *Pseudonimizacja a anonimizacja danych. Praktyczne zastosowanie w przedsiębiorstwie,* [dostęp: 27.08.2018] https://gdpr.pl/pseudonimizacja-a-anonimizacja-danych-praktyczne-zastosowanie-w-przedsiebiorstwie.

Zygmunt-Jakuć M., *Jak wykazać spełnienie zasady rozliczalności RODO,* [dostęp:] https://bezowijania.com/jak-wykazac-spelnienie-zasady-rozliczalnosci-rodo.

Żaczkiewicz-Zborska K., *Komputer może dyskryminować, a RODO temu zapobiega,* [dostęp: 13.02.2018] https://www.prawo.pl/prawnicy-sady/komputer-moze-dyskryminowac-a-rodo-temu-zapobiega,73866.html.

Żaczkiewicz-Zborska K., *NSA: Prawo do zapomnienia obejmuje internetowe archiwa prasowe,* [dostęp: 28.02.2023] https://www.prawo.pl/prawo/prawo-do-zapomnienia-obejmuje-e-archiwa-prasowe,520093.html.

Żądania usunięcia treści zgodnie z europejskim prawem dotyczącym prywatności, [dostęp:] https://transparencyreport.google.com/eu-privacy/overview.

4. Protokoły

Protokół w sprawie stosowania Karty Praw Podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa (Dz. Urz. UE 2009 nr 203, poz. 1569).

5. Decyzje

Decyzja z dnia 6 lipca 1988 r., w sprawie *Hilton vs. Wielka Brytania,* skarga nr 12175/86, DR 57/108.

Decyzja Komitetu Praw Człowieka z dnia 15 listopada 2004 r. w sprawie *Hulst vs. Holandia,* sygn. akt: 903/1999.

Decyzja CNIL z 10.03.2016 r., nr 2016-054, [dostęp:] https://www.cnil.fr/fr/decision-n-2016-054-du-10-mars-2016.

Decyzja PUODO z dnia 16 października 2019 r., znak sprawy: ZSPR.421.7.2019, [dostęp:] https://uodo.gov.pl/decyzje/ZSPR.421.7.2019.

Decyzja PUODO z dnia 24 sierpnia 2020 r., znak sprawy: DKN.5112.13.2020, [dostęp: 21.02.2021] https://uodo.gov.pl/decyzje/DKN.5112.13.2020.

Decyzja PUODO z dnia 11 lutego 2021 r., znak sprawy: DKN.5130.2024.2020, [dostęp: 19.02.2021] https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020.

6. Opinie i wytyczne

Grupa Robocza Art. 29, Opinia 5/2009 w sprawie portali społecznościowych przyjęta w dniu 12 czerwca 2009 r., WP 163, Bruksela 2009.

Opinia Europejskiego Inspektora Ochrony Danych z dnia 07.03.2012 r. w sprawie pakietu reform w zakresie ochrony danych (Dz. Urz. UE C 192/7 z 30.06.2012).

Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wniosku dotyczącego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, COM(2012)11 final-2012/011 (COD), (Dz. Urz. UE C 229 z 31.07.2012).

Opinia Komisji Przemysłu, Badań Naukowych i Energii dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych z dnia 26 lutego 2013 r. w sprawie wniosku dotyczącego Ogólnego Rozporządzenia o Ochronie Danych Osobowych (COM(2012)0011).

Hoboken van J., *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember. Freedom of Expression Safeguards in a Converging Information Environment,* opinia przygotowana dla Komisji Europejskiej, [dostęp: 01.05.2013] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC86747/lbna26410enn.pdf.

Opinia Rzecznika Generalnego Nila Jääskinena przedstawiona 25 czerwca 2013 r. w sprawie Google Spain SL i Google Inc. przeciwko AEPD i Mario Costeja Gonzàlez, sygn. akt: C-131/12.

Grupa Robocza Art. 29, *Wytyczne w zakresie prawa do przenoszenia danych,* przyjęte w dniu 13 grudnia 2016 r., WP 242.

Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów ochrony danych,* przyjęte w dniu 13 grudnia 2016 r., WP 243.

Grupa Robocza Art. 29, *Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów Rozporządzenia nr 2016/679*, przyjęte w dniu 03 października 2017 r., WP 253.

Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz określania, czy przetwarzanie danych może powodować wysokie ryzyko,* przyjęte w dniu 13 października 2017 r., WP 248.

Opinia Rzecznika Generalnego Macieja Szpunara z dnia 10 stycznia 2019 r., sprawa C-507/17, Google LLC przeciwko CNIL, ECLI:EU:C:2019:15.

7. Wnioski

Wniosek z 25 stycznia 2012 r. dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (Ogólne Rozporządzenie o Ochronie Danych Osobowych), COM(2012)11 final, [dostęp:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52012PC0011.

8. Dokumenty legislacyjne UE

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), [dostęp:] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011.

Projekt Rezolucji Parlamentu Europejskiego z dnia 20 listopada 2008 r., pkt C.

Uzasadnienie Rady: Stanowisko Rady (UE) nr 6/2016 w pierwszym czytaniu w sprawie przyjęcia rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego

przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz. Urz. UE 2016 C 159/02).

9. Normy

Norma PN-ISO/IEC 27005:2014-1, *Technika informatyczna-Techniki bezpieczeństwa-Zarządzanie ryzykiem w bezpieczeństwie informacji,* Polski Komitet normalizacyjny, Warszawa 2014.

Norma PN-ISO/IEC 29100:2017-07, *Technika informatyczna-Techniki bezpieczeństwa-Ramy prywatności,* [dostęp:] https://ikmj.com/pn-iso-iec-291002017-technika-informatyczna-techniki-bezpieczenstwa-ramy-prywatnosci/.

Norma ISO/IEC 29134, *Guidelines for privacy impact assessment,* [dostęp: 14.03.2018] https://odoserwis.pl/a/1179/ocena-wplywu-na-prywatnosc-zgodnie-z-norma-isoiec-29134-metodyka-prowadzenia-dpia.