Uniwersytet Wrocławski

Mariusz Jabłoński
Justyna Węgrzyn

Prawo do bycia zapomnianym

Wrocław 2021

Prawo do bycia zapomnianym

Prace Naukowe
Wydziału Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego

Seria: **e-Monografie** Nr 192

Dostęp online:
https://bibliotekacyfrowa.pl/publication/142660
https://repozytorium.uni.wroc.pl/publication/142660
DOI: 10.34616/142660

Mariusz Jabłoński
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
ORCID 0000-0001-8347-1884

Justyna Węgrzyn
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
ORCID 0000-0002-7996-9441

Prawo do bycia zapomnianym

Wrocław 2021

Recenzenci: *dr hab. Sabina Grabowska, prof. UR;*
dr hab. Radosław Grabowski, prof. UR

Korekta: *Anna Noga-Grochola*
Projekt i wykonanie okładki: *Karolina Drozd*
Skład i opracowanie techniczne: *Magdalena Gad eBooki.com.pl*

Druk: *Agencja Reklamowa TOP, Agnieszka Łuczak*

Wydawca
E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa.
Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

ISBN 978-83-66601-69-7 (druk)
ISBN 978-83-66601-70-3 (online)

Spis treści

Wykaz skrótów

Akty prawne

EKPC	Konwencja o ochronie praw człowieka i podstawowych wolności
KPP UE	Karta praw podstawowych Unii Europejskiej
RODO	rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
TFUE	Traktat o funkcjonowaniu Unii Europejskiej
TUE	Traktat o Unii Europejskiej
u.o.d.o.	ustawa o ochronie danych osobowych z 1997 r.
u.o.d.o. 2018	ustawa o ochronie danych osobowych z 2018 r.
u.r.p.	ustawa o radcach prawnych

Organy

EROD	Europejska Rada Ochrony Danych
ETPC	Europejski Trybunał Praw Człowieka
ETS	Europejski Trybunał Sprawiedliwości
GIODO	Generalny Inspektor Ochrony Danych Osobowych
NIK	Najwyższa Izba Kontroli

NSA	Naczelny Sąd Administracyjny
TK	Trybunał Konstytucyjny
TSUE	Trybunał Sprawiedliwości Unii Europejskiej
PUODO	Prezes Urzędu Ochrony Danych Osobowych
WSA	Wojewódzki Sąd Administracyjny

Wstęp

Istotą współczesnych procesów poznawczych i innowacyjnych jest stały i w dużej mierze nielimitowany dostęp do informacji. Informacja – co wiemy od dawien dawna – to z jednej strony swoistego rodzaju dobro, którego posiadanie i odpowiednie wykorzystanie jest fundamentem stabilnego rozwoju państwa, społeczeństwa i samej jednostki, z drugiej jednak strony może być nie tylko zagrożeniem dla poszanowania jej wolności i praw, ale niewłaściwie wykorzystywana, np. upubliczniana, stanowić będzie bezpośrednią i niedozwoloną ingerencję w sferę chronioną zarówno na płaszczyźnie prawodawstwa międzynarodowego, jak i krajowego.

Jedną z przyczyn zachodzących dziś zmian w zakresie funkcjonowania jednostki we współczesnym świecie jest dążenie do coraz szerszego wykorzystywania zdobyczy nowoczesnych technologii. Można nawet stwierdzić, że technologie te powodują przewartościowanie dotychczasowego stylu życia jednostki i – jak pokazuje praktyka – mają wpływ nie tylko na pojmowanie istoty i treści znanych wcześniej wolności i praw, ale również takich, które definiowane są na „bieżąco", tzn. w odniesieniu do pojawiających się zagrożeń. Nie budzi przy tym wątpliwości, że płaszczyzną, na której w stopniu najdalej idącym widoczne staje się definiowanie nowych uprawnień, jest globalne wykorzystanie elektronicznego przekazu, a co za tym idzie do-

stępu do informacji za pośrednictwem Internetu i innych cały czas udoskonalanych platform informacyjnych[1].

Łatwy i stale unowocześniany dostęp do informacji, łączący się z daleko idącą swobodą tworzenia i osobistego zamieszczania każdej w zasadzie informacji, prowadzi i będzie prowadził do powstawania szeregu sporów i wątpliwości interpretacyjnych, w szczególności w odniesieniu do ochrony i poszanowania wolności i praw jednostki. W praktyce bowiem każdy zainteresowany ma możliwość nie tylko pozyskania jakiejkolwiek informacji (funkcja informacyjna), ale również do bezpośredniego wymieniania się informacjami z innymi podmiotami (funkcja komunikacyjna) oraz ich definiowania, a także dalszego przetwarzania (funkcja kreacyjna). Pojęcie komunikacji we współczesnym znaczeniu zapewnia więc konkretnej osobie nie tylko dotarcie do pożądanych danych czy możliwość uzyskania dodatkowych informacji przez dwustronną ich wymianę, ale tworzenie bądź modyfikowanie (już istniejącego) określonego zasobu informacyjnego.

Nie budzi przy tym wątpliwości, że istniejąca swoboda definiowania różnego rodzaju informacji dotyczących nie tylko określonego rodzaju zdarzeń (np. katastrof, klęsk itd.), ale i konkretnych osób przybiera różne postaci. Wiele informacji, które wcześniej podlegały wielopłaszczyznowej weryfikacji opartej np. na zasadzie rzetelności dziennikarskiej, „uzupełniono" w praktyce o bliżej niesprecyzowany katalog działań faktycznych, sprowadzających się do zamieszczania w przestrzeni publicznej różnych danych, które nie tylko dotyczą faktów czy wynikają z ustawowo (normatywnie) zdefiniowanych obowiązków informacyjnych, ale są wynikiem subiektywnie definiowanej chęci upo-

[1] J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 8 i n.; P. Wąglowski, *Internet a dobra osobiste człowieka*, [w:] T. Zasępa, R. Chmura (red.), *Internet – fenomen społeczeństwa informacyjnego*, Częstochowa 2001, s. 317 i n.; E. Woch, *Sfera życia prywatnego i jego ochrona przed naruszeniami w Cyberprzestrzeni,* [w:] R. Skubisz (red.), *Internet 2000. Prawo – ekonomia – kultura*, Lublin 2000, s. 80 i n.

wszechnienia „wiedzy" na temat konkretnej osoby, zdarzenia czy też okoliczności.

W wielu przypadkach dochodziło i w dalszym ciągu dochodzi do upubliczniania informacji nieprawdziwych, niepełnych, nierzetelnych, co w istotny sposób wpływa na poczucie braku odpowiedniego poszanowania szeregu wolności i praw gwarantowanych jednostce.

Przekaz elektroniczny zmodyfikował klasyczne rozumienie wielu mechanizmów informacyjnych, w tym tego, co można określić jako trwanie informacji. Pod tym pojęciem można rozumieć sytuację stałej dostępności konkretnych danych, w tym dotyczących zindywidualizowanej osoby fizycznej, w zasadzie bez ograniczeń czasowych. Jak podkreśla się to przy wielu okazjach – w Internecie nic nie ginie i nic nie jest zapominane. Informacja po jej stworzeniu i uzewnętrznieniu zaczyna żyć własnym życiem, niekiedy będąc wykorzystywana w zupełnie innych celach, niż pierwotnie uzasadniających jej wytworzenie. Sytuacja taka od dawna budziła wiele wątpliwości, szczególnie z perspektywy odpowiedniego poszanowania uprawnień gwarantowanych jednostce (przede wszystkim prywatności i powiązanej z nią ochrony danych osobowych). Nie tylko przyczyniła się do powstania dyskusji na temat wolności przekazu i dostępu do informacji, ale ostatecznie doprowadziła do wyartykułowania treści prawa do bycia zapomnianym[2].

[2] Zob. szerzej na temat definiowania koncepcji prawa do bycia zapomnianym: J. Żak, *Koncepcja „prawa do bycia zapomnianym"*, [w:] M. Jabłoński, S. Jarosz-Żukowska (red.), *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi*, Wrocław 2014, s. 142-155; na temat zakresu obowiązków administratora związanych z realizacją art. 17 RODO zob. A. Nerka, *Komentarz do art. 17*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 239-244; P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Komentarz*, Warszawa 2018, s. 398-411; P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, s. 261-278; M. Czerniawski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 522-530.

Wskazane powyżej prawo jest dowodem na to, że w związku z rozwojem technologicznym, a w konsekwencji sposobami oraz mechanizmami pozyskiwania, rozpowszechniania i w szczególności wyszukiwania informacji – niezbędne było wypracowanie takiego rozwiązania (gwarancji), które stworzyłoby uprawnionej jednostce skuteczne egzekwowanie prawa do wyeliminowania z obrotu publicznego konkretnych informacji, które z różnych powodów stanowią nielegalną bądź nieuzasadnioną ingerencję w sferę gwarantowanych jej praw.

Modelowo prawo to ma zapewnić jednostce (osobie fizycznej) – i to oczywiście niezależnie od obywatelstwa czy miejsca stałego zamieszkania – poszanowanie jej podstawowych praw i wolności, szczególnie właśnie prawa do prywatności.

Warto już w tym miejscu odwołać się do prekursorskiego w tym zakresie rozstrzygnięcia TSUE, w którym stwierdził on, że uprawnionym jest każda osoba, której dane są w rzeczywistości przetwarzane z jednoczesnym zweryfikowaniem tego, czy ma ona prawo, aby dana 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". Prawo takie może być skutecznie egzekwowane bez względu na to, czy zawarcie na „liście wyników wyszukiwania danej informacji wyrządza szkodę tej osobie"[3].

Obowiązkiem każdego administratora (zobowiązanego) jest w związku z tym nie tylko respektowanie obowiązków, które towarzy-

[3] Wyrok z dnia 13 maja 2014 r. w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González,* C-131/12 – przy wprowadzeniu imienia i nazwiska M. Costejy Gonzáleza do wyszukiwarki grupy Google (zwanej dalej „Google Search") pojawiał się link do dwóch stron dziennika „La Vanguardia", odpowiednio, z dnia 19 stycznia i 9 marca 1998 r., na których znajdowało się zawierające to imię i nazwisko ogłoszenie w przedmiocie licytacji nieruchomości związanej z ich zajęciem wynikającym z niespłaconych należności na rzecz zakładu zabezpieczeń społecznych.

szą procesowi przetwarzania danych osobowych, ale w ogóle respektowanie tych wszystkich przepisów prawa, które definiowane są przez ustawodawcę unijnego oraz krajowego. Dotyczy to nie tylko organów i podmiotów publicznych, ale także każdego przedsiębiorcy niezależnie, czy jest to oddział lub filia (spółka zależna) posiadająca osobowość prawną, który musi zapewnić, w celu uniknięcia obejścia obowiązujących przepisów, że każda z prowadzonych przez niego działalności (podlegająca reżimowi ochrony danych osobowych) spełniać będzie standardy wynikające z obowiązujących regulacji w obszarze ochrony danych osobowych[4].

Jak wiemy, jedną z takich fundamentalnych regulacji jest obecnie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; dalej też jako: RODO)[5].

[4] Polski organ ochrony już w 2015 r. odwoływał się też do ustaleń belgijskiej Komisji prywatności, wskazując: „Motyw 19 preambuły (dyrektywy) potwierdza, że «Prowadzenie działalności gospodarczej na terytorium Państwa Członkowskiego zakłada efektywne i rzeczywiste prowadzenie działań przez stabilne rozwiązania; forma prawna prowadzonej działalności gospodarczej, niezależnie czy jest to oddział, czy filia posiadająca osobowość prawną, nie jest w tym względzie czynnikiem decydującym, w przypadku ustanowienia jednego administratora danych na terytorium kilku Państw Członkowskich, szczególnie w postaci filii, musi on zapewnić, w celu uniknięcia obejścia przepisów krajowych, że każda z prowadzonych działalności gospodarczych będzie spełniać obowiązki wynikające z prawa krajowego»", decyzja Generalnego Inspektora Danych Osobowych (dalej: GIODO), DOLiS/DEC – 50/16 (styczeń 2016 r.). W szerszym zakresie obejmuje również kwestie transferu danych do państw trzecich poza EOG – zob. więcej: M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Ochrona danych w wybranych państwach Azji*, Wrocław 2019, s. 28 i n.

[5] RODO uchyliło i zastąpiło dyrektywę 95/46/WE w obszarze sektorów prywatnego i publicznego w państwach członkowskich. Konieczne staje się jednocześnie podkreślenie, że obok RODO przyjęta została 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 przepły-

W opracowaniu postaramy się zaprezentować podstawowe elementy treści rozwiązań, które pozwolą na zrozumienie charakteru i znaczenia „prawa do bycia zapomnianym”[6]. Z tego też powodu nie tylko konieczne staje się przedstawienie pewnego „otoczenia” sfery chronionej (prywatność jednostki i dane osobowe), ale i przyjętego w polskim porządku prawnym modelu definiującego przesłanki:

– realizacji przedmiotowego prawa;
– jego ograniczeń i wyłączeń;
– odpowiedzialności za jego naruszenie.

Dopiero taka analiza pozwoli na formułowanie ostatecznych ocen w kontekście skuteczności i efektywności realizacji tego prawa, także w praktyce orzeczniczej polskich organów wymiaru sprawiedliwości.

Wydaje się jednak uzasadnione, już w tym miejscu, podkreślenie, że dotychczasowa praktyka potwierdza, że w wielu przypadkach powołującym się na art. 17 RODO trudno jest zrozumieć, że analiza ich konkretnego przypadku wymaga wzięcia pod uwagę szeregu kwestii szczegółowych, w tym zweryfikowania tego, czy wskazane przez ustawodawcę unijnego wyłączenia nie znajdują – w ich właśnie przypadku – pełnego zastosowania. Bardzo często żądanie poszanowania prawa do bycia zapomnianym (usunięcia danych) kierowane jest do instytucji publicznych (realizujących konkretne zadania publiczne) bez jakiejkolwiek faktycznej weryfikacji tego, czy przetwarzanie danych przez administratora jest niezbędne:

– do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa człon-

wu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (tzw. dyrektywa policyjna), Dz. Urz. UE L 119 z 4.05.2016 r.

[6] Na temat rozumienia i identyfikacji zob. P. Fajgielski, *Ogólne rozporządzenie*…, s. 268-269. Celowo nie posługujemy się w dalszej części opatrzeniem prawa do bycia zapomnianym cudzysłowem, uznając, że pojęcie to można identyfikować z pewnym obszarem uprawnień przysługujących osobie, której dane dotyczą, a o czym szerzej w dalszej części pracy.

kowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; […]

– do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
– do ustalenia, dochodzenia lub obrony roszczeń (art. 17 ust. 3 RODO).

Niezależnie od tego, że można odnieść wrażenie, iż w wielu przypadkach realizacja potwierdzonych w RODO uprawnień ma charakter wyłącznie „sprawdzający" znajomość regulacji przez samego administratora, warto kwestiom tym poświęcić nieco więcej uwagi, tak ze względu na różnorodność organizacyjną adresata żądań (administrator, podmiot przetwarzający), jak i specyfikę konkretnej sytuacji faktycznej i formalnoprawnej towarzyszącej realizacji gwarantowanego prawa (osoby, której dane dotyczą)[7]. Jednocześnie często też realizujący swoje prawo nie uwzględnia tego, iż każda z przesłanek legalizujących przetwarzanie danych osobowych przez administratora tych danych ma charakter autonomiczny i niezależny. Oznacza to, iż – co do zasady – są one równoprawne, a wobec tego spełnienie już jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych.

[7] Na temat podstawowych pojęć oraz analiz im poświęconych zob.: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm [dostęp: 5.10.2021].

Rozdział I

Rola i znaczenie prawa do ochrony danych osobowych w Internecie

1. RODO w systemie prawa krajowego

Z punktu widzenia Konstytucji RP[8] regulacje zawarte w rozporządzeniu ogólnym stosowane są bezpośrednio i mają pierwszeństwo w przypadku kolizji z przepisami ustaw (art. 91 ust. 3). Oznacza to, że krajowy organ stosujący prawo (jak i wszyscy inni zobowiązani do ochrony danych osobowych[9]) ma obowiązek traktowania postanowień RODO jako części krajowego porządku prawnego, a w razie kolizji z ustawą obowiązek jego zastosowania z jednoczesnym pominięciem przepisów aktu prawa krajowego[10]. Jak podkreśla się w literaturze

[8] Konstytucja RP z dnia 2 kwietnia 1997 r., Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.

[9] Na temat wcześniejszych problemów zob. A. Szmyt, *W sprawie ochrony danych osobowych,* „Gdańskie Studia Prawnicze. Studia prawnoadministracyjne" 2012, (red.) T. Bąkowski, K. Żukowski, nr XXVIII, s. 337 i n.

[10] Konieczność przeprowadzania prounijnej wykładni przepisów krajowych i honorowania związanej z tym zasady pierwszeństwa spoczywa nie tylko na sądach, ale na wszystkich organach administracji, które „wyposażone są w kompetencje do wydawania aktów administracyjnych lub podejmowania innych działań normowanych w całości lub części prawem europejskim" – wyrok NSA z dnia 1 grudnia 2011 r., I FSK 1565/11; zob. też: uchwałę SN z dnia 2 czerwca 2010 r., III CZP 37/10; postanowienie SN z dnia 28 listopada 2013 r., I KZP 15/13; wyrok SN z dnia 23 stycznia 2014 r., II CSK 188/13. Wszystkie orzeczenia sądów i Trybunału Konstytucyjnego znajdują się w systemie elektronicznym: sądów administracyjnych pod adresem http://orzeczenia.nsa.gov.pl; na stro-

przedmiotu „[…] normy zawarte w prawie wtórnym – RODO – mogą być bezpośrednio skuteczne, zarówno w układzie wertykalnym, jak i horyzontalnym, co wynika z […] art. 288 TFUE”[11].

Mając na względzie powyższe, trzeba sobie uświadomić, że w odróżnieniu od sytuacji, która miała miejsce do 25 maja 2018 r., obecnie istnieje możliwość bezpośredniego odwoływania się do aktu prawa unijnego w zakresie zdefiniowanej w nim istoty ochrony danych osobowych, wiążącej się bezpośrednio z ochroną podstawowych praw i wolności osób fizycznych, w szczególności zaś prawa do prywatności, a w konsekwencji i do poszanowania m.in. prawa do bycia zapomnianym (art. 17 RODO).

Nie może być inaczej, dlatego że podstawowym celem przyjęcia RODO było wzmocnienie i zharmonizowanie ochrony podstawowych wolności i praw osób fizycznych w związku z czynnościami przetwarzania oraz zapewnienia swobodnego przepływu danych osobowych między państwami członkowskimi (motyw 3 preambuły rozporządzenia ogólnego). Ochrona ta w istocie nie ogranicza się wyłącznie do stworzenia gwarancji służących zdefiniowaniu prawidłowości procesów przetwarzania i przepływu danych osobowych[12]. Musi być rozumiana o wiele szerzej – jako ochrona danych i procesu ich przetwarza-

nie Sądu Najwyższego – http://www.sn.pl/orzecznictwo/index.html oraz Trybunału Konstytucyjnego – www.trybunal.gov.pl [dostęp: 15.09.2021].

[11] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017, s. 32-33, 106-119.

[12] Podkreślić trzeba szerokie znaczenie pojęcia przetwarzania danych osobowych. Oznacza ono: operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie – art. 4 pkt 2 RODO. Udostępnienie danych przez administratora na podstawie przepisów prawa krajowego jest więc przetwarzaniem w rozumieniu RODO.

nia w kontekście kompleksowego poszanowania wszystkich wolności i praw definiujących szeroko rozumianą autonomię informacyjną jednostki. W takim ujęciu konieczne jest więc uwzględnienie nie tylko formalnego, ale i materialnego aspektu takiej ochrony.

Obok RODO, co często jest nieco pomijane, doszło do przyjęcia dyrektywy 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 uchylającej decyzję ramową Rady 2008/977/WSiSW[13] (dalej: DODO)[14]. Jej postanowienia zostały implementowane do polskiego porządku prawnego, co nastąpiło w drodze uchwalenia ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[15].

[13] Dz. Urz. UE L 119 z 4.05.2016, s. 89.

[14] Zgodnie z motywem 19 preambuły w związku z art. 2 ust. 2 lit. d) RODO ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy w ramach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, lub wykonywania kar, w tym w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz swobodny przepływ takich danych podlegają szczególnemu aktowi prawnemu Unii, jakim jest 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. Na temat stosowania postanowień dyrektywy jej implementacji w polskim porządku prawnym i relacji RODO-DODO zob. szerzej: *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, A. Grzelak (red.), Warszawa 2019, s. 29 i n.; *Ochrona danych osobowych w sądach i prokuraturze*, A. Grzelak (red.), Warszawa 2019, s. 50 i n.

[15] Dz. U. z 2019 r., poz. 125. W uzasadnieniu projektu ustawy zauważano, że: „Projekt ustawy określa również prawa osób, których dane osobowe są przetwarzane przez właściwe organy oraz środki ochrony prawnej przysługujące tym osobom; spo-

Nie ulega jednak wątpliwości, że dominująca rola, jaką w RODO odgrywa zasada celowości przetwarzania, implikuje podległość jego regulacjom nawet wtedy, gdy, co do zasady, konkretny podmiot jest wyłączony ze stosowania tego rozporządzenia unijnego. Z zasady tej wynika, że w określonym zakresie swej działalności, właśnie z uwagi na cel przez siebie realizowany, administrator będzie podlegał regulacjom rozporządzenia ogólnego (tak będzie np. w przypadku działań policji wiążących się z przetwarzaniem danych osobowych pracowników i funkcjonariuszy czy np. sądów w analogicznej sytuacji). Motyw 20 RODO wskazuje, że ma ono „zastosowanie między innymi do działań sądów i innych organów wymiaru sprawiedliwości, niemniej prawo Unii lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości – tak by chronić niezawisłość sprawowania wymiaru sprawiedliwości. Powinna istnieć możliwość powierzenia nadzoru nad takimi operacjami przetwarzania danych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego, organy te powinny w szczególności zapewnić przestrzeganie przepisów niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikają-

sób prowadzenia nadzoru nad ochroną danych osobowych, z wyłączeniem danych osobowych przetwarzanych przez prokuraturę i sądy; zadania organu nadzorczego oraz formy i sposób ich wykonania; obowiązki administratora i podmiotu przetwarzającego oraz inspektora ochrony danych i tryb jego wyznaczania; sposób zabezpieczenia danych osobowych; tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej oraz odpowiedzialność karną za naruszenie przepisów niniejszej ustawy. Jednocześnie, kierując się wyjaśnieniem zawartym w motywie (80) dyrektywy 2016/680, z zakresu nadzoru określonego w projektowanych przepisach, wyłączono dane osobowe przetwarzane przez prokuraturę i sądy w toku sprawowania przez nie wymiaru sprawiedliwości", uzasadnienie do projektu ustawy, s. 7, www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2989 [dostęp: 15.09.2021].

cych z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takim operacjami przetwarzania danych".

Konieczność stosowania reguł RODO będzie istnieć w przypadku podejmowania przez inny niż sąd organ wymiaru sprawiedliwości zadań obejmujących przetwarzanie danych osobowych niemieszczących się w zakresie celowościowym objętym wyłączeniem stosowania rozporządzenia, czyli zawsze wtedy, gdy jego cel nie będzie wiązał się ze wskazaną w art. 2 ust. 2 lit. d RODO grupą celów wyłączonych.

Wśród rozwiązań przyjętych w rozdziale III RODO zatytułowanym Prawa osoby, której dane dotyczą, prawodawca unijny w art. 23 odniósł się do kwestii ograniczeń. Zgodnie z tym przepisem: prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym realizacji wskazanym w tym przepisie celom[16].

[16] Chodzi tu środek służący:
a) bezpieczeństwu narodowemu;
b) obronie;
c) bezpieczeństwu publicznemu;
d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;
f) ochronie niezależności sądów i postępowania sądowego;
g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;

Jak wynika z treści wskazanego wyżej przepisu, zakres możliwych ograniczeń obowiązków i praw jest szeroki. Obejmuje on bowiem: przejrzyste informowanie i przejrzystą komunikację oraz tryb wykonywania praw przez osobę, której dane dotyczą (art. 12); obowiązki informacyjne (art. 13–14); prawo dostępu do danych (art. 15); prawo do sprostowania danych (art. 16); prawo do usunięcia danych (art. 17); prawo do ograniczenia przetwarzania (art. 18); obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19); prawo do przenoszenia danych (art. 20); prawo do sprzeciwu (art. 21); prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu (art. 22); zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34), a także zasady dotyczące przetwarzania danych osobowych (art. 5). Ograniczenia te – patrząc przez pryzmat postanowień Konstytucji RP – muszą wynikać z ustawy, która zgodnie z art. 23 ust. 2 RODO musi zawierać szczegółowe przepisy przynajmniej o:

a) celach przetwarzania lub kategorii przetwarzania;
b) kategoriach danych osobowych;
c) zakresie wprowadzonych ograniczeń;
d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;
e) określeniu administratora lub kategorii administratorów;
f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;

h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)-e) oraz g);
i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
j) egzekucji roszczeń cywilnoprawnych.

g) ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz

h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Mając powyższe na względzie, należy podkreślić, że wprowadzone przez ustawodawcę polskiego ograniczenia na podstawie art. 23 RODO znalazły swoje odzwierciedlenie w art. 3-5 ustawy o ochronie danych osobowych[17]. Na tle tych przepisów doszło do wyłączenia stosowania art. 13 ust. 3, art. 14 ust. 1, 2 i 4, art. 15 ust. 1-3 RODO przez administratorów wykonujących zadania publiczne w sytuacji, gdy:

1) zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 13 ust. 3 lub art. 14 ust. 1, 2 i 4, lub art. 15 ust. 1-3, jest niezbędne do realizacji celów określonych w art. 23 ust. 1 RODO oraz
2) przekazanie tych informacji:
   a) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z tego zadania publicznego lub
   b) naruszy ochronę informacji niejawnych.

Wskazana powyżej ustawa o ochronie danych osobowych nie jest jedynym aktem prawnym wprowadzającym tego typu ograniczenia. Odnosząc się bowiem do kwestii, o których mowa w art. 23 RODO, nie można pominąć ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (ogólne rozporządzenie o ochro-

[17] Ustawa z dnia 10 maja 2018 r., Dz. U. z 2018 r., poz. 1669 ze zm.

nie danych)[18]. To właśnie na mocy tej ustawy dodano do ustawy o ochronie danych osobowych art. 5a[19] oraz wprowadzono w innych ustawach[20] ograniczenia w zakresie niezbędnym do prawidłowej realizacji zadań administratorów. Ograniczenia zakresu obowiązków i praw związane są z działalnością administratorów zarówno ze sfery publicznej, jak i prywatnej i obejmują najczęściej obowiązki informacyjne (art. 13), prawo dostępu do danych (art. 15), prawo do ograniczenia przetwarzania (art. 18), obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19), prawo do sprzeciwu (art. 21). Poza obszarem ograniczeń ustawodawca pozo-

[18] Dz. U. z 2019 r., poz. 730, tzw. ustawa wdrażająca RODO.

[19] Art. 5a. ust. 1. Administrator, który otrzymał dane osobowe od podmiotu realizującego zadanie publiczne, nie wykonuje obowiązków, o których mowa w art. 15 ust. 1-3 rozporządzenia 2016/679, w przypadku gdy podmiot przekazujący dane osobowe wystąpił z żądaniem w tym zakresie ze względu na konieczność prawidłowego wykonania zadania publicznego mającego na celu:

1) zapobieganie przestępczości, wykrywanie lub ściganie czynów zabronionych lub wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom;
2) ochronę interesów gospodarczych i finansowych państwa obejmującą w szczególności:
   a) realizację i dochodzenie dochodów z podatków, opłat, niepodatkowych należności budżetowych oraz innych należności,
   b) wykonywanie egzekucji administracyjnej należności pieniężnych i niepieniężnych oraz wykonywanie zabezpieczenia należności pieniężnych i niepieniężnych,
   c) przeciwdziałanie wykorzystywaniu działalności banków i instytucji finansowych do celów mających związek z wyłudzeniami skarbowymi,
   d) ujawnianie i odzyskiwanie mienia zagrożonego przepadkiem w związku z przestępstwami,
   e) prowadzenie kontroli, w tym kontroli celno-skarbowych.

Ust. 2. W przypadku, o którym mowa w ust. 1, administrator udziela odpowiedzi na żądanie wniesione na podstawie art. 15 rozporządzenia 2016/679 w sposób, który uniemożliwia ustalenie, że administrator przetwarza dane osobowe otrzymane od podmiotu wykonującego zadanie publiczne.

[20] Zob. np.: art. 6, art. 7, art. 12, art. 19, art. 31, art. 35, art. 46, art. 142 ustawy z 21 lutego 2019 r.

stawił natomiast prawo do bycia zapomnianym (art. 17), co wydaje się efektem treści art. 17 ust. 3 RODO.

Odnosząc się do rozwiązań przyjętych w ustawie wdrażającej RODO, dostrzeżmy, że wprowadzony zakres ograniczeń obowiązków i praw określonych w art. 23 RODO uzależniony jest od specyfiki danej regulacji ustawowej. Widać to wyraźnie chociażby na przykładzie rozwiązań wprowadzonych ustawą wdrażającą RODO do ustawy o radcach prawnych (dalej: u.r.p.). W tym przypadku, ograniczenie stosowania niektórych przepisów RODO jest konieczne z uwagi na obowiązek zachowania przez radców prawnych tajemnicy zawodowej. W związku z tym, w dodanym na mocy ustawy wdrażającej RODO do u.r.p. art. 5a ust. 1 wprowadzono ograniczenia art. 15 ust. 1 i 3, art. 18 i art. 19 RODO polegające na tym, że przepisy te stosuje się w zakresie, w jakim nie naruszają one obowiązku zachowania przez radców prawnych wiążącej ich tajemnicy zawodowej. Należy mieć na uwadze, że radcowie prawni przetwarzają dane osobowe osób trzecich, które są im przekazywane przez klientów w związku z prowadzoną sprawą. Dane te objęte są tajemnicą zawodową, która nie ma ograniczeń czasowych. Brak wskazanych wyżej ograniczeń doprowadziłby do naruszenia tajemnicy, a więc interesów klienta, bowiem – jak zauważył Trybunał Konstytucyjny – „obowiązek zachowania tajemnicy ustanowiono […] w interesie klientów, a nie radców. Nie jest on wyrazem uprzywilejowania grupy zawodowej, lecz właśnie obowiązkiem związanym z wykonywaniem zawodu”[21].

O tym, jak istotne znaczenie przypisuje się tajemnicy zawodowej, świadczy także przyjęte na mocy ustawy wdrażającej RODO w art. 5b u.r.p. rozwiązanie. W przepisie tym wyraźnie wskazano, że „obowiązek zachowania tajemnicy, o której mowa w art. 3 ust. 4-6 (u.r.p. – przyp. M.J. i J.W.) nie ustaje, w przypadku, gdy z żądaniem

[21] Wyrok TK z dnia 22 listopada 2004 r., SK 64/03.

ujawnienia informacji uzyskanych przez radcę prawnego w związku z udzieleniem pomocy prawnej występuje Prezes Urzędu Ochrony Danych Osobowych".

Wprowadzone do u.r.p. ograniczenia dotyczą także prawa sprzeciwu. Zgodnie bowiem z treścią dodanego na podstawie ustawy wdrażającej RODO do u.r.p. art. 5a ust. 2, przepisu art. 21 ust. 1 RODO nie stosuje się w przypadku danych osobowych pozyskanych przez radcę prawnego w związku z udzielaniem pomocy prawnej. Ustawodawca krajowy zauważył, że wynikające z art. 21 ust. 1 RODO przesłanki, od których uwarunkowane jest prawo do wniesienia sprzeciwu, mogą mieć zastosowanie do radców prawnych. Nie można bowiem wykluczyć, że wniesiony przez osobę, której dane dotyczą, sprzeciw uniemożliwi radcy prawnemu przetwarzanie danych osobowych, „a w konsekwencji zablokuje możliwość dochodzenia roszczeń na rzecz klienta, czy uniemożliwi dalsze prowadzenie tego postępowania sądowego, prowadząc do jego przewlekłości. Spektakularnym przykładem ukazującym niezbędność wyłączenia jest także zastosowanie prawa do sprzeciwu wobec przetwarzania danych osobowych, które paraliżowałoby wykonywanie funkcji pełnomocników procesowych i uniemożliwiałoby wykonywanie jakichkolwiek czynności przedprocesowych na rzecz klientów, tym samym rażąco naruszając ich prawa konstytucyjne"[22].

2. Zakres ochrony danych osobowych

Aktem wtórnym UE, który w sposób najbardziej kompleksowy odnosił się dotychczas do problematyki ochrony danych osobowych była dyrektywa 95/46/WE[23]. Definiowała ona dane osobowe jako

[22] Uzasadnienie do projektu ustawy o zamianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, druk nr 3050, s. 30.

[23] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobo-

„wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej («osoby, której dane dotyczą»); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość”[24].

wych i swobodnego przepływu tych danych, OJ L 281, 23.11.1995 r. Por. M. Sakowska-Baryła, *Prawo do ochrony…*, s. 58.

[24] Art. 2 lit. a). W celu wywiązania się z realizacji wymogów określonych w art. 23 RODO, ustawodawca krajowy w dodanym na mocy ustawy wdrażającej RODO do u.r.p. art. 5c ustalił okres przechowywania danych osobowych, który wynosi:

1) 5 lat od końca roku, w którym zakończyło się postępowanie, w którym dane osobowe zostały zgromadzone – w przypadku danych osobowych przetwarzanych przez organy samorządu radców prawnych w zakresie niezbędnym do prawidłowej realizacji zadań publicznych określonych w ustawie oraz danych osobowych przetwarzanych w ramach nadzoru nad działalnością samorządu radców prawnych;
2) 10 lat od końca roku, w którym zakończyło się postępowanie, w którym dane osobowe zostały zgromadzone – w przypadku danych osobowych przetwarzanych:
   a) w toku prowadzonych przez organy samorządu radców prawnych postępowań:
      – administracyjnych,
      – w zakresie skarg i wniosków,
      – innych przewidzianych przez ustawę lub wydane na podstawie ustawy akty prawne organów samorządu radców prawnych dotyczących radców prawnych, aplikantów radcowskich lub osób ubiegających się o wpis na listę radców prawnych lub listę aplikantów radcowskich, a także osób przystępujących do egzaminu wstępnego na aplikację radcowską i egzaminu radcowskiego,
   b) w ramach nadzoru nad tymi postępowaniami, o których mowa w lit. a),
   c) przez radców prawnych w ramach wykonywania zawodu;
3) 15 lat od końca roku, w którym zakończyło się postępowanie, w którym dane osobowe zostały zgromadzone – w przypadku danych osobowych przetwarzanych w toku prowadzonych przez organy samorządu radców prawnych postępowań dyscyplinarnych wobec radców prawnych i aplikantów radcowskich oraz podczas wykonywania przewidzianych przez ustawę kompetencji nadzorczych nad postępowaniami dyscyplinarnymi w sprawach radców prawnych i aplikantów radcowskich.

Jak wynika ze wskazanej wyżej definicji, prawodawca unijny za dane osobowe uznał nie tylko informacje, na podstawie których mamy ustaloną tożsamość osoby fizycznej, ale także i takie informacje, które umożliwiają dopiero jej identyfikację, np. PESEL, numer dowodu osobistego, wygląd zewnętrzny, grupę krwi, status majątkowy, poglądy polityczne[25] itp. Ponadto odniósł się on do szczególnych kategorii danych, do których zgodnie z art. 8 zaliczył: zarówno dane ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak i dane dotyczące zdrowia i życia seksualnego.

Mając powyższe na względzie, można więc przyjąć, że dyrektywa wyróżniała dwie kategorie danych, a mianowicie: dane zwykłe niebędące danymi szczególnej kategorii (np. imię i nazwisko, adres zamieszkania, data urodzenia, seria i numer dowodu osobistego) oraz dane szczególnej kategorii (tzw. dane wrażliwe). Podział ten pozostaje bez zmian także w rozporządzeniu ogólnym 2016/679 o ochronie danych[26], które uchyliło dyrektywę 95/46/WE.

Sięgając do rozwiązań przyjętych na gruncie RODO, dostrzeżemy, że prawodawca unijny nieco zmodyfikował definicję danych osobowych. Terminem tym objął on bowiem „wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej («osobie, której dane dotyczą»); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię

Po upływie wskazanych wyżej okresów, w przypadku danych osobowych przetwarzanych przez radców prawnych w ramach wykonywania zawodu, dane osobowe ulegają usunięciu.

[25] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 346.

[26] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), OJ L 119, 4.05.2016 r.

i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”[27].

Z przyjętej w RODO definicji danych osobowych wynika, że jej treść została wzbogacona o identyfikator, taki jak imię i nazwisko, dane o lokalizacji (uzyskane np. z monitoringu czy GPS-u), identyfikator internetowy (np. adres IP komputera, nick, identyfikator plików *cookie*) oraz szczególny czynnik określający genetyczną tożsamość (np. DNA[28], RNA[29]).

Poza wskazaną wyżej definicją prawodawca unijny wyodrębnił także „dane genetyczne”, „dane biometryczne” oraz „dane dotyczące zdrowia”. Danymi genetycznymi są dane osobowe „dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej”[30]. W prezentowanym ujęciu do tej kategorii danych zalicza się np. kolor skóry, oczu, włosów, rysy twarzy (cechy dziedziczne), odporność organizmu (cecha nabyta). Z kolei dane biometryczne to dane osobowe, które „wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek lub dane

[27] Sprostowanie do 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 (ogólne rozporządzenie o ochronie danych), OJ L 127/2, 23.05.2018, (art. 4 pkt 1).

[28] Kwas dezoksyrybonukleinowy.

[29] Kwas rybonukleinowy.

[30] Art. 4 pkt 13 rozporządzenia 2016/679.

daktyloskopijne”[31]. Zalicza się do nich m.in. odciski palców, geometrię rąk, wzór siatkówki oka, brzmienie głosu, szczególny sposób mówienia, szczególny chód. Dane dotyczące zdrowia to „dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia”[32]. „Do danych takich należą informacje o danej osobie fizycznej zbierane podczas rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej […]; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby […] do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpitala, urządzenie medyczne lub badanie diagnostyczne *in vitro*”[33].

„Szczególne kategorie danych osobowych” to kolejny termin, który wyodrębniono w RODO. Zalicza się do nich pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne (w celu jednoznacznego zidentyfikowania osoby fizycznej) lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej. W porównaniu z dyrektywą 95/46 można dostrzec, że zakres tego terminu został rozszerzony o dane genetyczne, dane biometryczne, seksualność oraz orientację seksualną[34].

[31] Art. 4 pkt 14, *ibidem.* Por. A. Buczyńska-Borowy, *Alfabet ODO*, „ABI Expert” 2017, nr 2, s. 6.

[32] Art. 4 pkt 15, *ibidem.*

[33] Motyw 35, *ibidem.*

[34] Zob. szerzej: M. Jabłoński, K. Wygoda, *Legalność pozyskiwania*…, s. 87 i n.

W piśmiennictwie przyjmuje się, że „seksualność jest podstawowym elementem bycia człowiekiem przez całe życie, obejmującym seks, płciową identyfikację i role, orientację seksualną, erotyzm, pożądanie, intymność i reprodukcję. Seksualność jest doświadczana i wyrażana w myślach, fantazjach, przeżyciach, przekonaniach, wartościach, zachowaniach rolach i związkach. Seksualność powstaje na skutek interakcji czynników biologicznych, psychologicznych, społecznych, ekonomicznych, politycznych, kulturowych, etycznych, prawnych, historycznych, religijnych i duchowych”[35]. W zaprezentowanym ujęciu na seksualność składa się wiele elementów, w tym także orientacja seksualna, która w rozporządzeniu 2016/679 została wymieniona odrębnie, co może świadczyć o odmiennym znaczeniu tych terminów lub celowym zabiegu prawodawcy unijnego, z uwagi na możliwość różnego definiowania seksualności, tj. w sposób szeroki lub wąski. Jedno pozostaje pewne, a mianowicie to, że bez względu na zakres rozumienia seksualności, orientacja seksualna stanowić będzie zawsze szczególną kategorię danych osobowych.

Jak wskazaliśmy powyżej, do szczególnych kategorii danych zaliczono m.in. dane biometryczne. Należy jednak zaznaczyć, że „przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją «danych biometrycznych» tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości”[36]. To z kolei oznacza, że posiadanie np. przez pracodawcę zdjęcia swojego pracownika w aktach osobowych – nie stanowi jeszcze przetwarzania danych biometrycznych[37]. „Wizerunek osoby fi-

[35] Z. Lew-Starowicz, *Psychospołeczne podstawy seksualności,* [w:] Z. Lew-Starowicz, V. Skrzypulec (red.), *Podstawy seksuologii,* Warszawa 2010, s. 25.

[36] Motyw 51 rozporządzenia 2016/679.

[37] https://www.linkedin.com/pulse/dane-biometryczne-w-rodo-pawel-litwinski [dostęp: 15.09.2021].

zycznej będzie jej daną biometryczną tylko wtedy, gdy dzięki specjalnym technikom przetwarzania będzie umożliwiał identyfikację tej osoby lub potwierdzenie jej tożsamości. Nie wystarczy więc, że pracodawca będzie wiedział, do kogo należy konkretny wizerunek (bo zna swoich pracowników, bo akta osobowe są podpisane itp.) – żeby wizerunek został uznany za dane biometryczne, taka możliwość identyfikacji musi wynikać z technologii przetwarzania wizerunku"[38].

Poza zakresem szczególnych kategorii danych (tzw. danych wrażliwych) pozostają dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych (np. mandaty karne) lub powiązanych środków bezpieczeństwa[39]. Przetwarzanie tych danych osobowych jest możliwe „wyłączne pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych"[40].

Z przedstawionych powyżej definicji przyjętych w RODO wynika, że prawodawca unijny wprowadził kilka istotnych zmian w porównaniu do dyrektywy 95/46/WE. Mianowicie, zmodyfikował pojęcie danych osobowych, a także włączył do szczególnych kategorii danych osobowych m.in. dane genetyczne, biometryczne, dotyczące zdrowia, które dodatkowo zdefiniował. Rozszerzenie słownika pojęć o nowe terminy wydaje się być dobrym rozwiązaniem, bowiem zmniejszy bądź wyeliminuje wątpliwości, które mogą pojawić się w praktyce stosowania przepisów RODO.

Jak widać, ustawodawca unijny nie tworzy zamkniętego katalogu identyfikatorów, wskazując jedynie przykładowo na te, które mają cha-

[38] *Ibidem.*

[39] Por. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016, s. 114.

[40] Art. 10 rozporządzenia 2016/679.

rakter najczęstszy i najbardziej oczywisty. Świadczy o tym nie tylko użycie w treści wskazanego przepisu zwrotu „w szczególności", ale dotychczasowa praktyka ich definiowania. Konsekwencją takiego stanu rzeczy jest wyodrębnienie w literaturze przedmiotu dwóch płaszczyzn identyfikacji konkretnej osoby fizycznej: bezpośredniej i pośredniej, obejmujących szereg konkretnych identyfikatorów, takich jak:

- „imię i nazwisko,
- adres zamieszkania,
- numer identyfikacyjny w elektronicznym systemie ewidencji ludności,
- numer identyfikacji podatkowej,
- seria i numer dokumentu tożsamości,
- fotografia (wizerunek twarzy to również jedna z danych biometrycznych),
- nazwisko rodowe,
- imiona i nazwiska rodowe rodziców,
- imię i nazwisko małżonka oraz jego nazwisko rodowe,
- numer telefonu,
- adres e-mail,
- numer rejestracyjny samochodu[41],

[41] W niedawnym orzeczeniu sąd administracyjny uznał, że „Tradycyjny numer rejestracyjny pojazdu, składający się z liter i cyfr, nie jest daną osobową, gdyż określenie tożsamości osoby parkującej (właściciela, posiadacza) wymagałoby nadmiernych kosztów, czasu lub działań. Z tych samych pojazdów korzystają bowiem często różne osoby, w różnych miejscach, są one niejednokrotnie rejestrowane na więcej niż jeden podmiot. W takich sytuacjach nie da się powiązać pojazdu z określoną osobą w sposób łatwy i niewymagający nadzwyczajnych nakładów. Numer rejestracyjny identyfikuje pojazd, a nie osobę. Istnieje jednak możliwość oznaczenia pojazdu tzw. tablicami rejestracyjnymi indywidualnymi, na których litera i cyfra stanowią wyróżnik województwa, zaś kolejne litery w liczbie od 3 do 5 stanowią wyróżnik indywidualny pojazdu, w którym nie więcej niż dwie ostatnie litery można zastąpić liczbą. Nie ma żadnych przeszkód, by takie indywidualne oznaczenie w sposób dość łatwy (lub wręcz wprost) pozwalało zidentyfikować właściciela pojazdu, jeśli będzie to określenie dla niego bardzo charakterystyczne i zindywidualizowane, pozwalające się zorientować o jaką osobę chodzi. Są to jednak przypadki marginalne" – wyrok WSA w Gliwicach z dnia

– wzór podpisu,
– numer rachunku bankowego,
– numer karty kredytowej”[42].

Ponadto wskazuje się, że identyfikatorami takimi mogą być również inne wskazane już wyżej.

Zakres i charakter możliwej do przeprowadzenia identyfikacji osoby fizycznej jest więc bardzo szeroki, w praktyce zarówno organy i podmioty publiczne, jak i przedsiębiorcy jako administratorzy (jak i podmioty przetwarzające) zostają zobowiązani do stosowania wszystkich mechanizmów skonkretyzowanych w RODO. Jednym z nich jest dokonywanie oceny zagrożeń na etapie projektowania (*privacy by design*)[43], łączącej się z tzw. domyślną ochroną danych (*privacy by default*)[44]. Przeprowadzenie takiej oceny jest równoznaczne z podjęciem przez każdego z administratorów stosownych działań w zakresie ustalenia prawdopodobieństwa naruszenia konkretnych wolności i praw jednostki (jednostek), a w następstwie dokonanych ustaleń – sprecyzowania istoty potencjalnego ryzyka (chodzi tu więc o ustalenie zakresu i charakteru ewentualnych naruszeń lub ich niebezpieczeństw).

31 października 2018 r., II SA/Gl 593/18. Podobnie: wyrok WSA w Krakowie z dnia 14 grudnia 2016 r., II SA/Kr 1339/16. Odmiennie zaś: wyrok WSA w Warszawie z dnia 9 kwietnia 2013 r., II SA/Wa 211/13; oraz tego samego sądu z dnia 13 kwietnia 2017 r., VII SA/Wa 1069/16.

[42] M. Krzysztofek, *Ochrona danych osobowych…*, s. 43.

[43] Jak wskazuje się w literaturze przedmiotu „Privacy by Design jest podejściem, a właściwie preferowanym sposobem działania, polegającym na zapewnieniu ochrony danych osobowych poprzez włączenie i stosowanie odpowiednich reguł i zasad takiej ochrony już w fazie projektowania systemu informatycznego, aplikacji, działań marketingowych, usług lub produktów, które opierają się na przetwarzaniu danych osobowych”. Podejście to traktowane jest jako jeden ze standardów prywatności, zob. szerzej: A. Kobylańska, Ł. Ślęzak, *Ochrona danych w fazie projektowania – Privacy by Design*, „ABI Expert” 2016, nr 1, http://www.abi-expert.pl/wydania/listopad-2016/art,1426,ochrona-danych-w-fazie-projektowania-privacy-by-design.html [dostęp: 15.09.2021].

[44] W tym zakresie konieczne staje się uwzględnienie treści art. 25 RODO i motywu 78 RODO. Uwzględnianie ochrony danych osobowych ma nastąpić już na etapie projektowania danego rozwiązania, czyli jeszcze przed nadaniem mu warstwy technicznej; wyłącznie na etapie warstwy koncepcyjnej.

Konieczne w tym zakresie staje się podkreślenie, że ocena zagrożeń naruszeń musi być dokonywana względem poszanowania wolności i praw osoby (osób), której te dane dotyczą[45]. W praktyce chodzi tu m.in. o wskazane (i wyeliminowanie) w motywie 75 RODO zagrożenia, prowadzące do powstania:

- uszczerbku fizycznego;
- szkód majątkowych i szkód niemajątkowych, „w szczególności: jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą".

Ocena ryzyka, której efektem będzie wprowadzenie konkretnych rozwiązań, może, a w wielu konkretnych przypadkach musi mieć wpływ na postrzeganie żądań udostępniania informacji – w szczegól-

[45] Por. A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych osobowych,* „Monitor Prawniczy" 2016, nr 20, s. 29.

ności publicznych – których składową będą dane osobowe. Potencjalna odpowiedzialność administratora (zarówno cywilna, administracyjna, jak i karna) powinna determinować ocenę tego, czy i w jakim zakresie konkretne informacje bezpośrednio lub pośrednio identyfikujące osobę fizyczną będą mogły być udostępniane osobie lub podmiotom trzecim.

3. Prawo do prywatności

3.1. Pojęcie prywatności

Z przejawem prywatności jednostki i ochrony jej aspektów mamy do czynienia od dawna. Początki tej ochrony sięgają Starego Testamentu, prawa „starożytnego Babilonu, Egiptu, Grecji czy Rzymu”[46]. Prywatność nie pozostała obojętna także koncepcjom filozoficzno-prawnym, które w różny sposób odnoszą się do tego zagadnienia[47]. Pomijając jednak wątki filozoficzne, należy podkreślić, że dopiero w XIX w. po raz pierwszy doszło do zdefiniowania prawa do prywatności. „Pierwszą i zarazem najkrótszą definicję sformułował amerykański profesor Thomas McIntyre Cooley w 1888 r., który ujął prywatność jako prawo do pozostawienia w spokoju *(a right to be let alone),* powtórzoną dwa lata później przez amerykańskich prawników Samuela Warrena i Lusia Brandeisa w słynnym artykule *The Right*

[46] J. Sieńczyło-Chlabicz, *Geneza i rozwój prawa do prywatności,* [w:] *O prawie i jego dziejach. Księgi dwie. Studia ofiarowane Profesorowi Adamowi Lityńskiemu w czterdziestopięciolecie pracy naukowej i siedemdziesięciolecie urodzin, Księga II,* Białystok–Katowice 2010, s. 1149 i cytowana tam literatura. Zob. P. Sut, M. Wojciechowski, *Co zamiast prywatności? Czy prawo do intymności jest prawem człowieka?,* [w:] J. Jaskiernia (red. nauk.), *Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania tom 1,* Warszawa 2014.

[47] Zob. J. Baszkiewicz, F. Ryszka, *Historia doktryn politycznych i prawnych,* Warszawa 1973; H. Olszewski, *Historia doktryn politycznych i prawnych,* Warszawa 1986.

to Privacy"[48], który uznany został „za przełomowy nie tylko ze względu na to, że szczególnie mocno akcentowano w nim pojęcie prywatności *(right to privacy)*"[49], ale przede wszystkim z uwagi na zaprezentowane „w nim nowe spojrzenie na prawa obywatelskie, z jednoczesnym poszerzeniem ich zakresu o samoistne prawo, którego celem była ochrona sfery życia prywatnego"[50].

„Prywatność" to termin, którym posługuje się wiele dziedzin nauki, niemniej w żadnej z nich pojęcie to nie zostało zdefiniowane w sposób jednolity. Jedną z takich dziedzin są nauki prawne. Na przykład Andrzej Kopff przez *right of privacy* rozumie „prawo jednostki do życia swym własnym życiem, układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej. […] prawo do ochrony życia prywatnego *(right of privacy)* jest ujmowane jako kategoria nadrzędna, chroniąca wiele jednostkowych dóbr osobistych. […] naruszenia tego prawa dopuszcza się ten, kto: 1) ingeruje w życie prywatne, rodzinne lub domowe, 2) narusza integralność psychofizyczną jednostki, 3) narusza wolność przekonań lub obyczajów człowieka, 4) narusza cześć, honor lub zdobytą opinię, 5) ukazuje inną osobę w niekorzystnym dla niej świetle, 6) ujawnia krępujące lub intymne fakty odnoszące się do życia prywatnego jednostki, 7) przywłaszcza sobie cudze nazwisko, pseudonim lub osiągnięcia, 8) niepo-

[48] J. Braciak, *Prawo do prywatności,* [w:] S. Pajączkowski, A. Preisner (red.), *Zeszyty Luksemburskie 1. Praktyczne i teoretyczne problemy współczesnego państwa. Wybrane zagadnienia,* Lublin 2012, s. 75. Zob. S. Warren, L. Brandeis, *The Right to Privacy,* Harward Law Review, Vol. IV, December 15, 1980, No. 5; W. Sokolewicz, *Prawo do prywatności,* [w:] *Prawa człowieka w Stanach Zjednoczonych,* Warszawa 1985, s. 248 i n.; A. Bierć, P. Zawirska, *Konstytucjonalizacja ochrony prywatności na tle standardów europejskich,* [w:] J. Kuciński (red.), *Piętnaście lat Konstytucji RP z 1997 roku. Inspiracje, uregulowania, trwałość,* Warszawa 2012, s. 118 i n.

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

[50] *Ibidem.* Zob. także K. Łakomiec, *Konstytucyjne gwarancje ochrony prywatności informacyjnej wobec rozwoju nowych technologii,* „Przegląd Legislacyjny" 2015, nr 1 (91), s. 57 i n.; A. Mednis, *Prawo do prywatności a interes publiczny,* Zakamycze 2006, s. 57 i n.

koi drugą osobę przez jej śledzenie, narzucanie swego towarzystwa *(besetting)* lub w jakikolwiek inny sposób, 9) dopuszcza się naruszenia korespondencji oraz rozpowszechnia cudzy wizerunek bez zezwolenia osoby portretowanej, 10) nadużywa informacji uzyskanych prywatnie (ochrona wypowiedzi), 11) ujawnia informacje uzyskane od zainteresowanego lub udzielone mu w warunkach poufności”[51].

Jacek Sobczak odróżnia prywatność w ujęciu szerokim i wąskim. W tym pierwszym „prywatność jest stanem, w którym jednostka podejmuje decyzje jej dotyczące bez ingerencji osób trzecich”[52], natomiast w drugim, prywatność „to stan, w którym jednostka decyduje o zakresie i zasięgu informacji udostępnionych i komunikowanych innym osobom”[53]. Marlena Sakowska-Baryła pojęciu prywatności przypisuje „dwa zasadnicze znaczenia: pierwsze wynika z postawienia go w opozycji do pojęcia «publiczność», które odnosi się do sfery pozostającej zwykle w gestii władzy publicznej; drugie, węższe, odnosi się konkretnego człowieka i zbliża językowo do takich terminów jak «osobiste», «indywidualne», a więc określających osobowość człowieka”[54]. Joanna Braciak uważa, że „prywatność jest ściśle związana z pojęciem interesu własnego jednostki, jej dobra oraz z aktywnością podejmowaną przez jednostkę na rzecz ochrony tego dobra, w przeciwieństwie do aktywności podejmowanej dla dobra wszystkich. Chodzi więc o orientację na dobro własne jednostki jako pierwsze kryterium odróżniające to, co prywatne od tego co prywatnym nie jest. […] prywatność obejmuje sferę aspiracji, dążności oraz tych rodzajów aktywności, które nie podlegają zewnętrznej kontroli. Stąd prywatność bywa definiowa-

[51] A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne),* „Studia Cywilistyczne”, t. XX, Kraków 1972, s. 30.

[52] J. Sobczak, *Komentarz do art. 7 Karty Praw Podstawowych Unii Europejskiej*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2013, s. 221.

[53] *Ibidem*.

[54] M. Sakowska-Baryła, *Prawo do ochrony…*, s. 23.

na jako przestrzeń wolnego poruszania się, bądź też jako domena autonomicznej aktywności, wolnej od kontroli szerszych grup. Prywatność obejmuje przestrzeń fizyczną, przedmioty, budowle, do których inni nie mają dostępu. Prywatność i jej zasięg są określone rodzajem interakcji, stopniem dystansu i izolacji, które w danym systemie kulturowym składają się na tzw. prawo do prywatności, które bez zgody danej osoby lub grupy nie może być przekroczone"[55]. Mariusz Jabłoński definiuje prywatność jako „sumę wielu wartości składających się na rozumienie autonomiczności jednostki żyjącej w określonej rzeczywistości wobec innych jednostek, a także ich wspólnot oraz samego państwa i funkcjonariuszy"[56]. Z kolei Krzysztof Motyka wyróżnia „podstawowe typy definiowania prywatności:

A. Prywatność jako prawo do bycia pozostawionym w spokoju.
B. Prywatność jako prawo do kontroli informacji na swój temat.
C. Prywatność jako kontrola dostępu do osoby.
D. Prywatność jako autonomia jednostki.
E. Podejście redukcjonistyczne do prywatności"[57].

W doktrynie oprócz wielu definicji prywatności zwraca się także uwagę na trzy koncepcje dotyczące relacji zachodzących między prawem do prywatności a prawem do ochrony danych osobowych. Według pierwszej koncepcji „prawo do ochrony danych jest prawem będącym częścią składającą się na prawo do prywatności, elementem prawa do prywatności"[58]. „Konstrukcja ta ma związek z niejednoznacznym zakresem pojęciowym terminu «prywatność». Jeśli przypi-

[55] J. Braciak, *Prawo do prywatności,* [w:] B. Banaszak, A. Preisner (red.), *Prawa i wolności obywatelskie w Konstytucji RP,* Warszawa 2002, s. 278.

[56] M. Jabłoński, *Prywatność jako przesłanka ograniczenia dostępu do informacji publicznej,* „Przegląd Prawa i Administracji" LXXVI, Wrocław 2007, s. 280.

[57] M. Jagielski, *Konstytucjonalizacja ochrony prywatności,* [w:] R.M. Małajny (red.), *Konstytucjonalizm a doktryny polityczno-prawne. Najnowsze kierunki badań,* Katowice 2008, s. 265 i n.

[58] A. Gonschior, *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej,* [w:] D. Kornobis-Romanowska (red.), *Aktualne problemy prawa Unii Eu-*

sze się temu terminowi szerokie rozumienie, nie będzie wątpliwości, że zagadnienie ochrony danych osobowych wchodzi w jego zakres. Stąd naruszenia oraz zagrożenia, które uznajemy za godzące w prawo do ochrony danych, uderzają także w prywatność […]. Argumentem za uznaniem prawa do ochrony danych osobowych za wyspecjalizowane ogniowo prawa do prywatności może być również przywołanie koncepcji, że prawo do ochrony danych osobowych sprowadza się do pozostawania anonimowym. Mieści się to w formule prawa do bycia pozostawionym w spokoju (*my home is my castel*), jako węższym ujęciu gwarancji prywatności"[59].

Druga koncepcja „akcentuje odrębność obu praw"[60] z uwagi na osobne ich uregulowanie w przepisach Konstytucji RP. Trzecia koncepcja natomiast określa wzajemne relacje między prawem do prywatności a prawem do ochrony danych osobowych w kontekście funkcjonalnym[61]. W tym ujęciu „prawo do ochrony danych osobowych służy ochronie prywatności w tej części, która odnosi się do informacji dotyczących danej osoby oraz gwarancji pewnego stanu niezależności, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym informacji o swoim życiu, określanej mianem autonomii informacyjnej. Ma ona również zapewnić pozostawanie anonimowym, jeśli tego sobie życzymy, oraz możliwość samodzielnego decydowania o tym, jakie informacje o nas mogą być udostępniane osobom trzecim"[62]. Nie dziwi więc, że w doktrynie uzna-

ropejskiej i prawa międzynarodowego – aspekty teoretyczne i praktyczne, Wrocław 2017, s. 258.

[59] M. Sakowska-Baryła, *Prawo do ochrony…*, s. 92 i n.

[60] A. Gonschior, *op. cit.*, s. 258. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 151.

[61] M. Sakowska-Baryła, *Prawo do ochrony…*, s. 94.

[62] *Ibidem*, s. 95.

je się, że „bezpośrednią funkcją, jaką […] spełnia ochrona danych osobowych, jest zabezpieczenie samego prawa do prywatności”[63].

Mając na względzie wskazane powyższe kwestie, a przede wszystkim przedstawione przykłady definicji prywatności, należy podkreślić, że nie sposób tym definicjom zaprzeczyć, bowiem termin ten jest na tyle szeroki, że daje swobodę w jego definiowaniu. Wobec tego próba określenia tego pojęcia w sposób jednoznaczny z góry skazana jest na niepowodzenie. Zdecydowanie łatwiej wskazać jest więc źródło zagrożeń, które może godzić w prywatne życie jednostki. Niewątpliwie, jednym z takich źródeł jest Internet, który sprawił, że informacje z szeroko pojmowanej sfery prywatności udostępniane są w przestrzeni wirtualnej przez bardzo wiele osób, dla których prywatność przestała mieć jakiekolwiek znaczenie. Zmiana w podejściu do prywatności wydaje się efektem nie tylko darmowego dostępu do serwisów społecznościowych czy innych usług − które z uwagi na olbrzymie zainteresowanie, a także wywoływanie wrażenia, że „każdy to przecież ma”, mają zachęcić do korzystania z nich − ale także brakiem świadomości na temat zagrożeń występujących w świecie wirtualnym. Efektem tego wszystkiego jest utrata kontroli nad obiegiem własnych danych, które mogą być pozyskiwane przez inne podmioty czerpiące z nich korzyści. Wobec tego bezsprzeczne jest, że powszechny dostęp do Internetu i towarzysząca mu rewolucja cyfrowa stanowią obecnie jedno ze szczególnych zagrożeń naszej prywatności.

[63] K. Wygoda, *Ochrona danych osobowych i prawo do informacji o charakterze osobowym,* [w:] B. Banaszak, A. Preisner (red.), *Prawa i wolności obywatelskie w Konstytucji RP,* Warszawa 2002, s. 402.

3.2. Prawo do prywatności w unijnym porządku prawnym i praktyce orzeczniczej Trybunału Sprawiedliwości Unii Europejskiej

Na prawo do prywatności składa się kilka aspektów, do których prawodawca unijny zalicza: życie prywatne, rodzinne, dom i komunikowanie się. Potwierdzeniem tego jest art. 7 KPP UE, który stanowi: „Każdy ma prawo do poszanowania swego życia prywatnego i rodzinnego, domu i komunikowania się".

Próbując wyjaśnić znaczenie wymienionych wyżej elementów, kluczowych dla tych rozważań prawa przez pryzmat orzecznictwa TSUE, dostrzeżemy, że organ ten „ogranicza się do dyskusji na temat prywatności w kontekście problematyki ochrony danych osobowych"[64], co „nie pozostaje bez wpływu na liczbę rozpatrywanych"[65] przez niego spraw. Nie oznacza to jednak, że TS w ogóle nie zajmuje stanowiska „w zakresie treści i przedmiotu ochrony prawa do prywatności"[66]. Co prawda, zdarza się to niezbyt często, ale gdy do tego dojdzie, to Trybunał „konsekwentnie korzysta z dorobku ETPC"[67] ukształtowanego na tle art. 8 EKPC[68], którego zakres jest taki sam, jak art. 7 KPP UE. Traktowanie orzecznictwa strasburskiego jako wyznacznika treści art. 7 Karty, stało się możliwe na mocy art. 6 ust. 2 i 3 traktatu z Lizbony[69],

[64] J. Sieńczyło-Chlabicz, *Ochrona prawa do prywatności w Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, Karcie Praw Podstawowych oraz w prawie krajowym,* [w:] M. Pecyna, J. Pisuliński, M. Podrecka (red.), *Rozprawy cywilistyczne. Księga pamiątkowa dedykowana Profesorowi Edwardowi Drozdowi,* Warszawa 2013, s. 21.

[65] *Ibidem.*

[66] *Ibidem,* s. 25.

[67] *Ibidem.*

[68] Art. 8 ust. 1 EKPC „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji".

[69] Art. 6 ust. 2. „Unia przystępuje do europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Przystąpienie do Konwencji nie narusza kompetencji Unii określonych w Traktatach.

Ust. 3. Prawa podstawowe, zagwarantowane w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz wynikające z tradycji konstytucyj-

który uznał EKPC za część prawa unijnego, a także z uwagi na art. 52 ust. 3 KPP UE, który stanowi: „W zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich znaczenie i zakres są takie same jak praw ustanowionych przez tę Konwencję. Niniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę". Mając powyższe na względzie, w dalszej części pracy, opierając się na wybranym orzecznictwie TSUE i ETPC, odniesiemy się do pojęcia życia prywatnego, rodzinnego, domu i komunikowania się.

W sprawie *Volker und Markus Schecke*[70], która dotyczyła publikacji na stronie internetowej federalnego instytutu rolnictwa i wyżywienia danych osobowych beneficjentów dopłat rolnych pochodzących z Europejskiego Funduszu Rolniczego Gwarancji i Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich, Trybunał Sprawiedliwości stwierdził ingerencję w życie prywatne. Podkreślił bowiem za ETPC, że „termin «życie prywatne» nie może być interpretowany w sposób zawężający oraz że nic nie uzasadnia wyłączenia działalności zawodowej"[71] lub handlowej zarówno osób fizycznych, jak i prawnych[72] z zakresu tego pojęcia. „Rozszerzająca interpretacja «życia prywatnego» ma

nych wspólnych Państwom Członkowskim, stanowią część prawa Unii jako zasady ogólne prawa", Dz. Urz. UE C 306/01 z 17.12.2007 r.

[70] Wyrok TSUE z dnia 9 listopada 2010 r., C-92/09. Zob. wyrok ETPC z dnia 16 lutego 2000 r. w sprawie *Amann przeciwko Szwajcarii*; wyrok ETPC z dnia 4 maja 2000 r. w sprawie *Rotaru przeciwko Rumunii.*

[71] *Ibidem.* Por. wyrok ETS z dnia 20 maja 2003 r. w sprawie *Österreichischer Rundfunk i in.,* C-465/00.

[72] Wyrok ETS z dnia 14 lutego 2008 r. w sprawie *Varec SA,* C-450/06. Zob. wyrok ETPC z dnia 16 grudnia 1992 r. w sprawie *Niemietz przeciwko Niemcom*; wyrok ETPC z dnia 16 kwietnia 2002 r. w sprawie *Société Colas Est i in. przeciwko Francji*; wyrok ETPC z dnia 28 stycznia 2003 r. w sprawie *Peck przeciwko Zjednoczonemu Królestwu.*

jednak granice i nie może prowadzić do obejmowania tym pojęciem działań o charakterze zasadniczo publicznym”[73].

Życie prywatne jest pojęciem bardzo szerokim, które – jak podkreślił ETPC – nie ma „ani możliwości, ani potrzeby, by starać się”[74] wyczerpująco zdefiniować[75]. Wobec tego w praktyce orzeczniczej nie podejmuje się próby ustalenia w sposób jednoznaczny tego terminu, lecz wyodrębnia się jego elementy składowe. Przykładem jest wyrok w sprawie *Ilonka Sayn-Wittgenstein*[76], w którym TSUE wskazał, że „nazwisko osoby jest jednym z elementów składowych jej tożsamości i życia prywatnego, które podlega ochronie na podstawie art. 7 Karty Praw Podstawowych Unii Europejskiej oraz art. 8 Europejskiej Konwencji praw człowieka i podstawowych wolności. Chociaż art. 8 Konwencji nie wymienia w sposób wyraźny nazwiska osoby, odnosi się ono jednak do życia prywatnego i rodzinnego tej osoby, będąc środkiem identyfikacji osobowej i związania z rodziną”[77]. Z kolei w sprawie *Malgožata Runevič-Vardyn* Trybunał Sprawiedliwości rozstrzygał spór w przedmiocie odmowy zmiany przez urząd miasta Wilna „nazwisk i imion skarżących w postępowaniu przed sądem krajowym figurujących w wydanych im aktach stanu cywilnego”[78]. Co do transkrypcji imion i nazwisk Trybunał stwierdził, iż w przypadku wykazania,

[73] L. Garlicki, *Komentarz do art. 8,* [w:] L. Garlicki (red.), *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1-18,* Warszawa 2010, s. 491.

[74] Opinia Rzecznika Generalnego Pedra Cruza Villalóna z dnia 12 grudnia 2013 r. Sprawa C-293/12 *Digital Rights Ireland Ltd* oraz sprawa C-594/12 *Kärntner Landesregierung Michael Seitlinger i in.*

[75] Zob. wyrok ETPC z dnia 16 grudnia 1992 r. w sprawie *Niemietz przeciwko Niemcom*; wyrok ETPC z dnia 19 kwietnia 2002 r. w sprawie *Pretty przeciwko Zjednoczonemu Królestwu.*

[76] Wyrok TSUE z dnia 22 grudnia 2010 r., C-208/09.

[77] *Ibidem.* Zob. wyrok ETPC z dnia 22 lutego 1994 r. w sprawie *Burghartz przeciwko Szwajcarii*; wyrok z dnia 25 listopada 1994 r. w sprawie *Stjerna przeciwko Finlandii.*

[78] Wyrok TSUE z dnia 12 maja 2011 r., C-391/09.

„że odmowa zamiany wspólnego nazwiska pary obywateli Unii, których dotyczy postępowanie przed sądem krajowym, powoduje poważne niedogodności na płaszczyźnie administracyjnej, zawodowej i prywatnej dla nich i dla ich rodziny, do sądu krajowego należeć będzie ustalenie, czy odmowa taka szanuje słuszną równowagę występujących tu interesów, a mianowicie z jednej strony prawo skarżących w postępowaniu przed sądem krajowym do poszanowania ich życia prywatnego i rodzinnego, a z drugiej strony uzasadnioną ochronę przez dane państwo członkowskie jego języka urzędowego i tradycji”[79].

Treścią art. 7 KPP UE objęte zostało życie rodzinne, które – jak podkreślił ETS – „w rozumieniu art. 8 EKPC stanowi część praw podstawowych, które zgodnie z utrwalonym orzecznictwem Trybunału są chronione we wspólnotowym porządku prawnym [obecnie unijnym – przyp. M.J. i J.W.]. To prawo do mieszkania z bliskimi krewnymi, co wiąże się dla państw członkowskich bądź z obowiązkami nieczynienia, jeśli jedno z nich jest zobowiązane do niewydalania osoby, bądź czynienia, jeśli jest zobowiązane do zezwalania osobie na wjazd i pobyt na swoim terytorium. […] nawet jeśli EKPC nie gwarantuje jako prawa podstawowego prawa cudzoziemca do wjazdu i pobytu na terytorium określonego państwa, to wydalenie osoby z kraju, w którym żyją jego bliscy krewni, może stanowić ingerencję w prawo do poszanowania życia rodzinnego, które jest chronione na podstawie art. 8 ust. 1 tej kon-

[79] *Ibidem.* Por. wyrok ETS z dnia 2 października 2003 r. w sprawie *Carlos Garcia Avello,* C-148/02; wyrok ETS z dnia 14 października 2008 r. w sprawie *Stefana Grunkina i Dorothee Regine Paul,* C-353/06, w którym Trybunał przypomniał, że orzekał już „w odniesieniu do dzieci mających obywatelstwo dwóch państw członkowskich, iż rozbieżności w nazwiskach mogą spowodować poważne niedogodności dla zainteresowanych zarówno w stosunkach zawodowych, jak i prywatnych, wynikające między innymi z trudności w korzystaniu w państwie członkowskim, którego są obywatelami, ze skutków prawnych aktów lub dokumentów wystawionych na nazwisko uznane w innym państwie członkowskim, którego również są obywatelami”.

wencji”[80]. ETS zwraca przy tym uwagę, że „Konwencja o prawach dziecka również uznaje zasadę poszanowania życia rodzinnego. Opiera się ona na uznaniu, wyrażonym w motywie szóstym, że w celu harmonijnego rozwoju osobowości dziecka powinno ono wyrastać w środowisku rodzinnym. Artykuł 9 ust. 1 tej konwencji przewiduje również, że państwa zapewnią, aby dziecko nie zostało oddzielone od swoich rodziców wbrew ich woli, a zgodnie z art. 10 ust. 1 z obowiązku tego wynika, że wszystkie wnioski składane przez dziecko lub przez jego rodziców odnośnie do wjazdu lub opuszczenia państwa-strony w celu łączenia rodziny będą rozpatrywane przez państwa-strony w sposób przychylny, humanitarny i w szybkim trybie. W art. 7 KPP UE zostało uznane również prawo do poszanowania życia prywatnego i rodzinnego”[81], co oznacza, że „postanowienie to należy interpretować w świetle obowiązku uwzględnienia najlepiej pojętego interesu dziecka, o którym mowa w art. 24 ust. 2 tej karty i zwracając uwagę na potrzebę regularnego utrzymywania osobistych stosunków z obydwojgiem rodziców przez dziecko, o czym mowa w art. 24 ust. 3. Dokumenty te podkreślają wagę życia rodzinnego dla dziecka i zalecają państwom uwzględnianie jego interesu, lecz nie tworzą prawa podmiotowego do wjazdu na terytorium państwa dla członków rodziny i nie mogą być interpretowane w sposób pozbawiający państwa pewnego zakresu uznania przy badaniu wniosków o łączenie rodzin”[82].

Elementem życia rodzinnego jest małżeństwo[83]. Nie ma przy tym znaczenia, czy związek małżeński został zawarty przez osoby odmien-

[80] Wyrok ETS z dnia 27 czerwca 2006 r. w sprawie C-540/03. Zob. wyrok ETS z dnia 11 lipca 2002 r. w sprawie C-60/06; wyrok ETS z dnia 23 września 2003 r. w sprawie C-109/01.

[81] *Ibidem.*

[82] *Ibidem.*

[83] Na temat małżeństwa zob. B. Banaszak, *Konstytucyjna regulacja małżeństwa a prawo do zawarcia małżeństwa,* [w:] M. Jabłoński (red.), *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym,* Wrocław 2014, s. 79.

nej, czy tej samej płci. Potwierdzeniem tego jest wyrok ETPC w sprawie *Schalk i Kopf przeciwko Austrii*[84], w którym Trybunał stwierdził, że związek osób tej samej płci „mieści się w pojęciu życie rodzinne na równi ze związkiem dwóch osób różnej płci. Europejska Konwencja o Ochronie Praw Człowieka nie nakłada jednak na Państwo obowiązku wydania zezwolenia na zawarcie małżeństwa parze osób tej samej płci. Władze krajowe były najlepiej umocowane do tego, aby ocenić i wyjść naprzeciw potrzebom społeczeństwa w tym zakresie, mając na uwadze fakt, że instytucja małżeństwa ma głęboko zakorzenione konotacje społeczne i kulturowe, różniące się znacznie pomiędzy społeczeństwami. Nie stwierdzono naruszenia artykułu 12 (prawo do zawarcia małżeństwa)[85] oraz artykułu 14 (zakaz dyskryminacji)[86] w związku z artykułem 8 (prawo do poszanowania życia prywatnego i rodzinnego) Europejskiej Konwencji o Ochronie Praw Człowieka"[87]. Powyższa interpretacja Europejskiego Trybunału Praw Człowieka świadczy o odejściu przez ten organ od dotychczasowej linii orzeczniczej, w której dominowało jedynie kryterium biologiczne determinujące płeć[88], co sprawia, że interpretacja ta odpowiada treści art. 9 KPP UE, który stanowi: „Prawo do zawarcia małżeństwa i prawo do założenia rodziny są gwarantowane zgodnie z ustawami krajowymi regulującymi korzystanie z tych praw".

[84] Wyrok ETPC z dnia 24 czerwca 2010 r.

[85] Art. 12 EKPC „Mężczyźni i kobiety w wieku małżeńskim mają prawo do zawarcia małżeństwa i założenia rodziny zgodnie z ustawami krajowymi regulującymi korzystanie z tego prawa".

[86] Art. 14 EKPC „Korzystanie z praw i wolności wymienionych w niniejszej Konwencji powinno być zapewnione bez dyskryminacji wynikającej z takich powodów jak płeć, rasa, kolor skóry, język, religia, przekonania polityczne i inne, pochodzenie narodowe lub społeczne, przynależność do mniejszości narodowej, majątek, urodzenie bądź z jakichkolwiek innych przyczyn".

[87] http://www.echr.coe.int/Documents/FS_Sexual_orientation_POL.pdf [dostęp: 10.09.2021].

[88] Nastąpiło to od wyroku ETPC z dnia 11 lipca 2002 r. w sprawie *Christine Goodwin przeciwko Zjednoczonemu Królestwu.*

Zgodnie z art. 7 KPP elementem składowym prawa do prywatności jest także prawo do poszanowania domu. „Domem jest stałe czy podstawowe miejsce przebywania (zamieszkania) danej osoby bądź rodziny, tzn. miejsce, z którym tę osobę (rodzinę) wiążą wystarczające (trwałe) związki fizyczne i emocjonalne, miejsce, które traktuje ona jako swoje”[89]. Przy czym pojęcie, o którym mowa, można rozumieć szeroko, obejmując nim pomieszczenia zawodowe lub handlowe[90].

Co do naruszeń prawa do poszanowania domu, Trybunał Sprawiedliwości w sprawie *Monika Kušinová przeciwko Smart Capital a.s.,* podkreślił za ETPC „po pierwsze, że utrata miejsca zamieszkania stanowi jedno z najpoważniejszych naruszeń prawa do poszanowania domu, a po drugie, że każda osoba, której grozi tak poważny skutek, powinna co do zasady mieć zagwarantowane prawo do zbadania proporcjonalności takiego środka”[91].

Ostatnim elementem wymienionym w art. 7 KPP UE jest prawo do komunikowania się, które należy rozumieć szeroko[92]. Obejmuje

[89] L. Garlicki, *Komentarz do art. 8,* [w:] L. Garlicki (red.), *Konwencja…,* s. 537 i n.

[90] Wyrok ETS z dnia 22 października 2002 r., C-94/00. Por. wyrok ETS z dnia 21 września 1989 r., C-46/87; wyrok ETPC z dnia 16 grudnia 1992 r. w sprawie *Niemietz przeciwko Niemcom.*

[91] Wyrok TSUE z dnia 10 września 2014 r., C-34/13. Zob. także wyrok ETPC z dnia 27 września 1995 r. w sprawie *McCann przeciwko Zjednoczonemu Królestwu*; wyrok ETPC z dnia 25 lipca 2013 r. w sprawie *Rousk przeciwko Szwecji.*

[92] W art. 8 EKPC wskazano m.in., że każdy ma prawo do poszanowania swojej korespondencji. W orzecznictwie ETPC termin „korespondencja” rozumiany jest w sposób szeroki, bowiem odnosi się on do:

- „wszelkich form technicznego przekazania wiadomości, w szczególności do rozmów telefonicznych, wymiany poczty elektronicznej i informacji internetowych […];
- przekazywania wiadomości zarówno przy wykorzystywaniu urządzeń własnych (domowych), publicznych czy stanowiących wyposażenie biurowe […];
- przekazywania wiadomości przez wszelkie osoby, także osoby poddane szczególnemu reżimowi podporządkowania […];
- przekazywania wiadomości o wszelkiej treści, nawet łączącej się z planowaniem czy popełnieniem przestępstwa”,

L. Garlicki, *Komentarz do art. 8,* [w:] L. Garlicki (red.), *Konwencja…,* s. 542 i n.

ono bowiem zarówno przekaz ustny, jak i pisemny, który może przybrać formę listowną, elektroniczną, telefoniczną itp. TSUE zwraca przy tym uwagę, że „przechwytywanie przekazów telekomunikacyjnych jest ingerencją w korzystaniu z prawa gwarantowanego w art. 8 ust. 1 EKPC[93] […], stanowi ono również ograniczenie wykonywania prawa ustanowionego w art. 7"[94] KPP UE. Ponadto, Trybunał, opierając się na orzecznictwie ETPC, wskazuje, że także „w przypadku przejęcia korespondencji elektronicznej dokonanego w ramach rewizji w lokalach przedsiębiorstwa lub w pomieszczeniach handlowych osoby fizycznej lub lokalach spółki handlowej […] przejęcie to stanowi ingerencję w korzystaniu z prawa gwarantowanego w art. 8 EKPC"[95]. W sprawie *Digital Rights Ireland Ltd.* Trybunał Sprawiedliwości za dodatkową ingerencję w prawa zagwarantowane w art. 7 KPP UE uznał „możliwość uzyskania dostępu do danych przez właściwe organy krajowe"[96]. Z naruszeniem praw wymienionych w art. 7 Karty mamy także do czynienia w przypadku podsłuchiwania rozmów telefonicznych[97].

W systemie prawnym Unii Europejskiej prawo do prywatności uregulowane zostało w art. 7 KPP. W przepisie tym prawodawca unijny nie zdefiniował pojęcia prywatności, lecz wymienił kilka jej aspektów, tj. życie prywatne, rodzinne, dom i komunikowanie się. W osobnym przepisie uregulowano natomiast prawo do ochrony danych osobo-

[93] Zob. wyrok ETPC z dnia 6 września 1978 r. w sprawie *Klass i inni przeciwko Niemcom*; wyrok ETPC z dnia 2 sierpnia 1984 r. w sprawie *Malone przeciwko Zjednoczonemu Królestwu*; wyrok ETPC z dnia 24 kwietnia 1990 r. w sprawie *Kruslin przeciwko Francji i Huvig przeciwko Francji*; postanowienie ETPC z dnia 29 czerwca 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom.*

[94] Wyrok TSUE z dnia 17 grudnia 2015 r., C-419/14.

[95] *Ibidem.* Zob. wyrok ETPC z dnia 26 grudnia 1992 r. w sprawie *Niemietz przeciwko Niemcom*; wyrok ETPC z 2 kwietnia 2015 r. w sprawie *Vinci Construction i GTM Génie Civil et Services przeciwko Francji.*

[96] Wyrok TSUE z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12.

[97] Wyrok Sądu (dziewiąta izba) z dnia 8 września 2016 r., T-54/14.

wych, które stanowi również „element szeroko rozumianego prawa do prywatności”[98], o czym szerzej w dalszej części opracowania.

Brak definicji prywatności zarówno w aktach prawa krajowego, międzynarodowego, jak i unijnego wynika „m.in. z faktu, że treść prawa do prywatności ewoluuje pod wpływem przemian kulturowych i społecznych. *Ergo* określenie jego zakresu zostało pozostawione w głównej mierze judykaturze”[99], co potwierdzają wskazane wyżej przykłady orzeczeń Trybunału Sprawiedliwości UE. Analizując orzeczenia tego organu, nie sposób nie zauważyć, że odnosi się on do bogatego dorobku orzeczniczego ETPC wykształconego na tle art. 8 EKPC, który stanowi dla niego źródło inspiracji w zakresie interpretacji art. 7 KPP UE. Jest to możliwe z uwagi na treść art. 6 ust. 2 i 3 Traktatu z Lizbony oraz art. 52 ust. 3 Karty. Przyjęcie takiego rozwiązania świadczy więc o uznaniu przez prawodawcę unijnego Europejskiej Konwencji Praw Człowieka „«za żyjący instrument» stale dostosowywany w drodze orzeczniczej do zmieniającego się kontekstu społecznego, politycznego i kulturowego”[100].

3.3. Prawo do prywatności w polskim porządku prawnym i w praktyce orzeczniczej Trybunału Konstytucyjnego

W polskim porządku prawnym prawo do prywatności chronione jest wieloaspektowo. Fundamentalne znaczenie ma w tym przypadku art. 47 Konstytucji RP[101], który wyraża prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. „Jak się okazuje, nie jest to jedyny przepis odnoszący się do zagadnienia związanego z prywatnością, bowiem

[98] M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, Wrocław 2002, s. 207.

[99] J. Sieńczyło-Chlabicz, *Ochrona prawa do prywatności*…, s. 21.

[100] L. Garlicki, *Komentarz do art. 8,* [w:] L. Garlicki (red.), *Konwencja…*, s. 482.

[101] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. Nr 78, poz. 483 ze zm.

jego uzupełnieniem są rozwiązania przyjęte na tle innych norm ustawy zasadniczej. Mowa tu o: ochronie godności człowieka (art. 30); zakazie dyskryminacji (art. 33); wolności osobistej (art. 41); prawie do sądu (art. 45); prawie rodziców do wychowywania dzieci zgodnie z własnymi przekonaniami (art. 48); tajemnicy komunikowania się (art. 49); gwarancji nienaruszalności mieszkania (art. 50); prawie do ochrony danych osobowych (art. 51); wolności przemieszczania się (art. 52), czy prawie do milczenia, a więc wyłączenia «możliwości zobowiązania jednostki przez organy władzy publicznej do ujawnienia swojego światopoglądu, przekonań religijnych lub wyznania»[102] (art. 53)"[103].

Odnosząc się do prywatności i ochrony jej aspektów z punktu widzenia postanowień Konstytucji, nie można pominąć orzecznictwa Trybunału Konstytucyjnego, które pełni rolę „wyznacznika" zarówno w procesie stanowienia, jak i stosowania prawa. Wobec tego, w dalszej części pracy, opierając się na wybranych przykładach orzeczeń tego organu, pokażemy zajęte przez niego stanowisko we wskazanym wyżej zakresie.

W wyroku o sygnaturze akt K 21/96 Trybunał zwrócił uwagę, iż „koncepcja prawa do prywatności […] zdołała już […] zyskać sobie trwałe miejsce we współczesnych państwach demokratycznych. Stanowią ją zasady i reguły odnoszące się do różnych sfer życia jednostki, a ich wspólnym mianownikiem jest przyznanie jednostce prawa «do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej». Tak rozumiana prywatność odnosi się przede wszystkim do życia osobistego, rodzinnego, towarzyskiego i czasem jest określana jako «prawo do pozostawienia w spokoju». Na ogół przyjmuje się, że prywatność odno-

[102] J. Rzucidło, J. Węgrzyn, *Prawne aspekty ochrony anonimowości konsumenta w Internecie,* „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie" 2013, s. 254.

[103] M. Jabłoński, J. Węgrzyn, *Ochrona tajemnic osób wykonujących prawnicze zawody zaufania publicznego,* Wrocław 2016, s. 191.

si 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”[104]. Wobec tego „prawo do prywatności obejmuje też ochronę tajemnicy danych dotyczących sytuacji majątkowej obywatela, a więc odnosi się także do posiadanych przez niego rachunków bankowych (i podobnych) oraz dokonywanych przez niego transakcji”[105]. „W sferze życia osobistego jednostki mieści się również prawo do decydowania o ochronie własnego życia i zdrowia”[106]. Przy czym – na co zwraca uwagę Trybunał – prawo, o którym mowa, podobnie jak inne prawa i wolności jednostki „nie ma charakteru absolutnego i może podlegać ograniczeniom. Konieczne jest jednak, by ograniczenia te formułowane były w sposób czyniący zadość wymaganiom konstytucyjnym”[107]. Nie można jednak utracić „z pola widzenia faktu, że prawo do prywatności ma charakter szczególny w systemie praw i wolności konstytucyjnych[108]. Jak zaznaczył Trybunał w wyroku w sprawie K 41/02, nawet stan wojenny i wyjątkowy «nie zezwalają ustawodawcy na złagodzenie przesłanek, przy spełnieniu których można wkroczyć w sferę życia prywatnego, nie narażając się na zarzut niekonstytucyjnej arbitralności»”[109].

[104] Wyrok TK z dnia 24 czerwca 1997 r., K 21/96.

[105] *Ibidem.*

[106] Wyrok TK z dnia 9 lipca 2009 r., SK 48/05. Por. wyrok TK z dnia 26 lutego 2014 r., K 22/10. Por. wyrok TK z dnia 5 marca 2013 r., U 2/11.

[107] Wyrok TK z dnia 19 maja 1998 r., U 5/97.

[108] Świadczy o tym art. 233 ust. 1 Konstytucji, który stanowi: „Ustawa określająca zakres ograniczeń wolności i praw człowieka i obywatela w czasie stanu wojennego i wyjątkowego nie może ograniczać wolności i praw określonych w art. 30 (godność człowieka), art. 34 i art. 36 (obywatelstwa), art. 38 (ochrona życia), art. 39, art. 40 i art. 41 ust. 4 (humanitarne traktowanie), art. 42 (ponoszenie odpowiedzialności karnej), art. 45 (dostęp do sądu), art. 47 (dobra osobiste), art. 53 (sumienie i religia), art. 63 (petycje) oraz art. 48 i art. 72 (rodzina i dziecko)”.

[109] Wyrok TK z dnia 20 marca 2006 r., K 17/05.

Nietykalność i wolność osobista to kolejny przejaw prawa do prywatności, na który zwrócił uwagę Trybunał Konstytucyjny. W sprawie U 7/12 organ ten stwierdził, że kontrola osobista cudzoziemców prowadzona na podstawie kwestionowanych przepisów − tj. Regulaminu organizacyjno-porządkowego pobytu cudzoziemców w strzeżonym ośrodku i areszcie w celu wydalenia, stanowiącego załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 26 sierpnia 2004 r. w sprawie warunków, jakim powinny odpowiadać strzeżone ośrodki i areszty w celu wydalenia – „stanowi ingerencję w nietykalność osobistą chronioną na podstawie art. 41 ust. 1 Konstytucji oraz prawo do prywatności chronione na podstawie art. 47 Konstytucji. W świetle wymogów stawianych ustawodawcy zarówno przez art. 31 ust. 3, jak i przez art. 41 ust. 1 Konstytucji, dopuszczalna jest, w przypadku ingerencji w obie te wolności osobiste, wyłącznie interwencja ustawodawcy. Ustawodawca musi uczynić to w sposób zupełny i precyzyjny. W akcie rangi podustawowej, pod warunkiem wyraźnego upoważnienia ustawodawcy, można określić jedynie kwestie porządkowe związane z przebiegiem kontroli osobistej […]. Trybunał podkreśla, że art. 41 ust. 1 zdanie drugie Konstytucji zakazuje ograniczenia wolności osobistej w podustawowych aktach prawnych i jednocześnie nakazuje wytyczanie w ustawie wszystkich materialnoprawnych przesłanek ingerowania w wolność osobistą. Ustawa musi też wytyczać procedurę jej ograniczania[110]. Ta sama reguła rządzi dopuszczalnością ingerencji w prawo do prywatności”[111]. Trybunał Konstytucyjny, „odwołując się do orzecznictwa Europejskiego Trybunału Praw Człowieka[112] […], zauważył, że z perspektywy tej wolności osobistej niezbędne jest stwierdzenie dostatecznie precyzyjnej i konkretnej podstawy ustawowej

[110] Por. wyrok TK z dnia 10 marca 2010 r., U 5/07.

[111] Wyrok TK z dnia 29 października 2013 r., U 7/12.

[112] Zob. wyrok ETPC z dnia 2 sierpnia 1984 r. w sprawie *Malone przeciwko Wielkiej Brytanii.*

wkroczenia w jej sferę i jest niedopuszczalne wprowadzenie ograniczeń aktami podustawowymi. Trybunał podkreśla również, że normy ograniczające prawo do prywatności winny być uregulowane na poziomie ustawowym”[113].

Zgodnie z orzecznictwem TK ochronę prywatności i zakaz ingerencji w tę sferę gwarantuje art. 47 Konstytucji[114], którego dopełnieniem jest m.in. art. 51 statuujący tzw. autonomię informacyjną[115]. „Z ochroną prywatności i autonomii informacyjnej koresponduje też prawo do ochrony tajemnicy komunikowania się, ustanowione w art. 49 Konstytucji. W piśmiennictwie wskazuje się niekiedy, że wolność komunikowania się dotyczy raczej porozumiewania się za pomocą pewnego środka przekazu, nie zaś bezpośredniej rozmowy osób w jakimś miejscu, albowiem to ostatnie jest raczej wyrazem prawa do prywatności. Trybunał Konstytucyjny przyjmuje jednak szersze rozumienie wolności komunikowania się, nie przeciwstawiając jej tak kategorycznie prawu do ochrony prywatności[116] […]. Konstytucyjną ochroną wynikającą z art. 49 Konstytucji objęta jest tym samym treść komunikowana bezpośrednio, jak i za pomocą środków komunikowania się na odległość. Według Trybunału, «przejawem prawa do prywatności jest również wolność komunikowania się, która obejmuje nie tylko tajemnicę korespondencji, ale i wszelkiego rodzaju kontakty międzyosobowe»[117] […]. Z punktu widzenia prawa do ochrony tajem-

[113] Wyrok TK z dnia 29 października 2013 r., U 7/12. Zob. także wyrok TK z dnia 5 marca 2013 r., U 2/11.

[114] Wyrok TK z dnia 30 lipca 2014 r., K 23/11.

[115] „Ochrona prywatności i autonomii informacyjnej, jak już podkreślono, jest konsekwencją ochrony przyrodzonej i niezbywalnej godności człowieka (art. 30 Konstytucji). Jak wskazano w dotychczasowym orzecznictwie, zachowanie przez człowieka godności wymaga poszanowania jego czysto osobistej sfery, w której nie jest narażony na konieczność «bycia innym» czy «dzielenia się z innymi» swoimi przeżyciami czy doznaniami”, *ibidem*. Zob. także wyrok TK z dnia 12 grudnia 2005 r., K 32/04; wyrok TK z dnia 23 czerwca 2009 r., K 54/07.

[116] Por. wyrok TK z dnia 12 grudnia 2005 r., K 32/04.

[117] Wyrok TK z dnia 20 czerwca 2005 r., K 4/04.

nicy komunikowania się (art. 49 Konstytucji) «sposób porozumiewania się istotny jest tylko o tyle, o ile jego zastosowanie w danych warunkach (okolicznościach) pozbawia osoby trzecie, które nie są adresatami danych treści, możliwości zapoznania się z nimi. Tylko wtedy bowiem można sensownie mówić o istnieniu jakiejś «tajemnicy», którą można byłoby objąć ochroną. W konsekwencji, w tym jedynie znaczeniu forma komunikacji może mieć *in casu* wpływ na zakres prawa do ochrony tajemnicy komunikowania się»"[118]. Mając powyższe na względzie, Trybunał stwierdził, że „konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji objęte są wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna 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 IMEI. W ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się nadto ochrona przed niejawnym monitorowaniem jednostki oraz prowadzonych przez nią rozmów, nawet w miejscach publicznych i ogólnie dostępnych. Nie ma znaczenia, czy wymiana informacji dotyczy życia ściśle prywatnego, czy też prowadzonej działalności zawodowej, w tym działalności gospodarczej. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której konstytucyjna ochrona byłaby wyłączona bądź samoistnie ograniczona. W każdej z tych sfer jednostka ma więc konstytucyjnie gwarantowaną wolność

[118] Wyrok TK z dnia 30 lipca 2014 r., K 23/11. Zob. także wyrok TK z dnia 2 lipca 2007 r., K 41/05.

przekazywania i pozyskiwania informacji, w tym udostępniania informacji o sobie samej”[119]. Trybunał zwraca przy tym uwagę, że mimo iż Konstytucja nie odnosi się wprost do korzystania przez jednostkę z przestrzeni wirtualnej, to „ochrona konstytucyjnych wolności i praw jednostek w związku z korzystaniem z Internetu oraz innych elektronicznych sposobów porozumiewania się na odległość nie różni się niczym od ochrony dotyczącej tradycyjnych form komunikowania się czy też innej aktywności. Dane przekazywane za pomocą Internetu nie mogą być postrzegane jako funkcjonujące niejako obok, czy na marginesie konstytucyjnie chronionych form aktywności człowieka. Nie ma tym samym uzasadnionych powodów, które pozwalałyby oderwać przekazywanie danych czy komunikowanie się za pomocą Internetu od sfery wolności i praw konstytucyjnych. Ze względu na złożoność zjawiska, jakim jest Internet, aktywność jednostek w tej sferze odpowiada właściwym postaciom aktywności chronionej konstytucyjnie. I tak przekazywanie korespondencji drogą elektroniczną (np. e-mail) podlega takiej samej ochronie konstytucyjnej, jak przekazywanie listu w tradycyjnej formie papierowej (art. 47, art. 49, art. 51). Przekazywanie informacji obrońcy za pomocą Internetu lub innych środków komunikacji elektronicznej podlega takim samym gwarancjom, jak przekazanie ich w rozmowie osobistej (art. 42). Ochrona intymności w kontaktach z osobami wykonującymi zawód zaufania publicznego jest jednakowa bez względu na formę komunikowania się (art. 47). Wyrażanie poglądów, pozyskiwanie i rozpowszechnianie informacji drogą elektroniczną podlega w pełni ochronie przewidzianej w art. 54 Konstytucji. Podobnie ochrona wolności prasy i środków społecznego przekazu jest taka sama, bez względu na formę korzystania z tej wolności (art. 14, art. 54). Konstytucyjna ochrona wolności działalności gospodarczej (art. 20 i art. 22) obejmuje swym zakresem również po-

[119] *Ibidem.*

dejmowanie oraz prowadzenie tej działalności w Internecie lub za pomocą innych form komunikacji elektronicznej. To samo dotyczy też ochrony wolności wyboru i wykonywania zawodu (art. 65), wolności twórczości artystycznej, badań naukowych oraz ogłaszania ich wyników, jak również wolności nauczania i wolności korzystania z dóbr kultury (art. 73) czy prawa składania petycji, wniosków oraz skarg do organów władzy publicznej (art. 63)"[120].

Permanentny rozwój technologiczny, którego jesteśmy świadkami, a także powszechny dostęp do Internetu przyczyniają się do poszerzania sfery funkcjonowania jednostki. Z jednej strony otwiera to „nowe i nieznanie dotąd możliwości korzystania z konstytucyjnie zagwarantowanych wolności i praw"[121], z drugiej zaś – stanowi poważne źródło zagrożeń prywatności. „Pokonywanie bariery czasu i przestrzeni w komunikowaniu się […]; przekazywanie informacji na każdy temat oraz w dowolnej formie, bez względu na odległość dzielącą rozmówców […]; możliwość nabywania dóbr i usług […]; decydowanie o sposobach realizacji własnych potrzeb"[122], a także wykorzystywanie Internetu do tworzenia, przechowywania i przekazywania różnego rodzaju danych – to nieocenione dobra we współczesnym świecie, z których należy korzystać z rozwagą. Niestety, większość użytkowników tych rozwiązań podchodzi do nich bezkrytycznie, często rezygnując z ochrony prywatności. Należy jednak pamiętać, że to od każdego z nas w dużym stopniu zależy, czy poprzez swoje postępowanie doprowadzimy do erozji własnej sfery prywatności, dostarczając przy tym innym podmiotom, w tym także i państwu, wielu informacji na swój temat i nie tylko, czy prywatność będzie stanowić dla nas cenną wartość, pomimo że ani my sami, ani państwo nie jesteśmy/nie jest w stanie jej w 100% chronić. Wobec tego nie budzi wątpliwości, że do sku-

[120] *Ibidem.*
[121] *Ibidem.*
[122] *Ibidem.*

tecznej ochrony prywatności niezwykle ważne jest nie tylko otoczenie prawne, ale także stopień świadomości każdego człowieka korzystającego ze zdobyczy nowych technologii.

3.4. Prawo do ochrony danych osobowych w unijnym porządku prawnym i w praktyce orzeczniczej Trybunału Sprawiedliwości Unii Europejskiej

W systemie Unii Europejskiej prawo do ochrony danych osobowych uregulowane zostało zarówno w aktach prawa pierwotnego, jak i wtórnego. Do tych pierwszych zalicza się TFUE[123] oraz KPP UE[124]. Do drugich zaś rozporządzenia i dyrektywy. Przykładem jest: rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE[125] oraz dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych

[123] Art. 16 TFUE:

„Ust. 1. Każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Ust. 2. TFUE 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. Przestrzeganie tych zasad podlega kontroli niezależnych organów.

Zasady przyjęte na podstawie niniejszego artykułu pozostają bez uszczerbku dla zasad szczególnych przewidzianych w art. 39 Traktatu o Unii Europejskiej".

[124] Art. 8 KPP UE:

„Ust. 1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.

Ust. 2. 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 dokonania ich sprostowania.

Ust. 3. Przestrzeganie tych zasad podlega kontroli niezależnego organu".

[125] Dz. Urz. UE L 295 z 2018 r.

i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[126]. Ponadto warto wspomnieć o nieobowiązującej już dyrektywie 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[127], która przed 25 maja 2018 r. była pierwszoplanową regulacją w zakresie ochrony danych osobowych. W związku z tym, w dalszej części pracy, opierając się na wybranym orzecznictwie TSUE, pokażemy, w jaki sposób organ ten dokonał interpretacji postanowień powyższej dyrektywy.

Na przykład w wyroku o sygnaturze C-101/01[128] Trybunał wypowiedział się na temat przetwarzania danych osobowych w Internecie. Sprawa dotyczyła katechetki *Bodli Lindvist*, która na potrzeby parafii utworzyła strony internetowe. Zawierały one informacje na temat katechetki, a także jej kolegów z parafii, m.in. nazwiska lub w niektórych przypadkach tylko imiona, pełnione funkcje, sposób spędzania wolnego czasu, numer telefonu. Ponadto na stronie internetowej zamieszczona została informacja o koleżance katechetki, która „doznała urazu stopy i w związku z tym przebywała na zwolnieniu lekarskim w niepełnym wymiarze"[129]. Jak się okazało działania pani *Lindqvist* naruszyły przepisy szwedzkiej ustawy o ochronie danych osobowych ze względu na przetwarzanie danych bez zgody osób, których one dotyczą, a także z uwagi na niezgłoszenie takich działań do *Datainspektion*, tj. „instytucji publicznej zajmującej się ochroną danych przekazy-

[126] Dz. Urz. WE L 201 z 2002 r. W tym miejscu należy wspomnieć, że w dalszym ciągu trwają pracę nad uchwaleniem rozporządzenia w sprawie prywatności i łączności elektronicznej, które uchyli dyrektywę 2002/58.

[127] Dz. Urz. WE L 281 z 1995 r.

[128] Wyrok ETS z dnia 6 listopada 2003 r., C-101/01.

[129] http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1586575 [dostęp: 10.09.2021].

wanych drogą informatyczną”[130]. W konsekwencji katechetka została skazana na karę grzywny, jednak wniosła apelację do sądu wyższej instancji, który z uwagi na wątpliwości w zakresie wykładni dyrektywy 95/46 zwrócił się do ETS z pytaniami prejudycjalnymi. W odpowiedzi na zadane pytania Trybunał stwierdzi, że:

– „operacja polegająca na zamieszczeniu na stronie internetowej danych różnych osób pozwalających je zidentyfikować za pomocą nazwiska albo innych środków, np. numeru telefonu lub informacji dotyczących ich warunków pracy i sposobu spędzania przez nie wolnego czasu, stanowi przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany w rozumieniu art. 3 ust. 1 dyrektywy 95/46”[131];
– przetwarzanie danych osobowych, o których wyższej mowa, „nie jest objęte żadnym z wyłączeń określonych w art. 3 ust. 2 dyrektywy 95/46 […];
– informacja, iż dana osoba doznała urazu stopy i przebywa na zwolnieniu lekarskim w niepełnym wymiarze, stanowi dane dotyczące zdrowia w rozumieniu art. 8 ust. 1 dyrektywy 95/46 […];
– przekazywanie danych do państw trzecich w rozumieniu art. 25 dyrektywy 95/46 nie ma miejsca, w przypadku, gdy osoba, która znajduje się w jednym z państw członkowskich, zamieszcza na stronie internetowej, przechowywanej przez dostawcę usług hostingowych mającego swoją siedzibę w tym samym państwie lub w innym państwie członkowskim, dane osobowe, czyniąc je w ten sposób dostępnymi dla każdego, kto połączył się w Internecie, w tym również dla osób, które znajdują się w państwie trzecim […];

[130] *Ibidem.*
[131] *Ibidem.*

– przepisy dyrektywy 95/46 nie zawierają same w sobie ograniczeń sprzecznych z ogólną zasadą swobody wypowiedzi lub z innymi prawami i swobodami obowiązującymi w ramach Unii Europejskiej, które odpowiadają w szczególności art. 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności […]. Do władz publicznych i sądów państw członkowskich odpowiedzialnych za stosowanie przepisów krajowych dokonujących transpozycji dyrektywy 95/46 należy zapewnienie właściwej równowagi między wchodzącymi w grę prawami i interesami, w tym prawami podstawowymi chronionymi przez wspólnotowy porządek prawny;
– środki podejmowane przez państwa członkowskie w celu zapewnienia ochrony danych muszą być zgodne zarówno z przepisami dyrektywy 95/46, jak i z jej celem, jakim jest utrzymanie równowagi między swobodnym przepływem danych osobowych a ochroną życia prywatnego. Natomiast nic nie stoi na przeszkodzie rozszerzeniu przez państwo członkowskie zakresu ustawodawstwa krajowego dokonującego transpozycji przepisów dyrektywy 95/46 na dziedziny nieobjęte zakresem jej stosowania, pod warunkiem że nie sprzeciwia się temu żaden przepis prawa wspólnotowego”[132].

Kolejny wyrok, który zasługuje na uwzględnienie, dotyczy dynamicznych adresów IP. W sprawie *Patrick Breyer przeciwko Bundesrepublik Deutschland* przedmiotem sporu było rejestrowanie i przechowywanie przez Republikę Federalną Niemiec adresu IP skarżącego podczas przeglądania przez niego stron internetowych niemieckich służb federalnych[133]. Jako że powództwo *Patricka Breyera* zostało od-

[132] *Ibidem.*

[133] Wyrok TSUE z dnia 19 października 2016 r., C-582/14. Wyrok dostępny na stronie: http://curia.europa.eu/juris/document/document.jsf?text=%2522dyrektywa-%2B95%252F46%2522&docid=184668&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=994471#ctx1 [dostęp: 10.09.2021].

dalone przez niemiecki sąd administracyjny, skarżący wniósł apelację. Sąd apelacyjny, rozpatrując przedłożoną mu sprawę, uznał, że „dynamiczny adres IP w połączeniu z datą sesji, do której się on odnosi, stanowi, w sytuacji gdy dany użytkownik strony internetowej ujawnił swoją tożsamość w trakcie tej sesji, dane osobowe, ponieważ operator tej strony może zidentyfikować tego użytkownika poprzez zestawienie jego nazwiska z adresem IP jego komputera. […]. W przypadku bowiem gdy *P. Breyer* nie podaje swojej tożsamości w trakcie przeglądania strony, jedynie dostawca dostępu do Internetu może powiązać adres IP ze zidentyfikowanym abonentem. Natomiast w rękach Republiki Federalnej Niemiec, jako dostawcy usług medialnych online, adres IP nie stanowi jednej z danych osobowych, nawet w połączeniu z datą przeglądania strony, do której się on odnosi, zważywszy że użytkownik rozpatrywanych stron internetowych nie może zostać zidentyfikowany przez to państwo członkowskie”[134]. Na orzeczenie sądu apelacyjnego strony postępowania wniosły skargę rewizyjną do *Bundesgerichtshof* (federalnego trybunału sprawiedliwości), który z uwagi na wątpliwości interpretacyjne powstałe na tle rozpatrywanej sprawy, zwrócił się do Trybunału Sprawiedliwości UE z pytaniami prawnymi. W odpowiedzi Trybunał stwierdził, że:

– art. 2 lit. a) dyrektywy 95/46 – dotyczący definicji danych osobowych – „należy interpretować w ten sposób, że dynamiczny adres IP zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego dostawcy dane osobowe w rozumieniu tego przepisu, w sytuacji gdy dysponuje on środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki

[134] *Ibidem.*

dodatkowym informacjom, jakimi dysponuje dostawca dostępu do Internetu dla tej osoby”[135];

– art. 7 lit. f) dyrektywy 95/46 – dotyczący kryteriów legalności przetwarzania danych osobowych – „należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu państwa członkowskiego, na podstawie którego dostawca usług medialnych online może gromadzić i wykorzystywać dane osobowe użytkownika tych usług – w braku jego zgody – tylko wtedy, gdy takie gromadzenie i wykorzystywanie są konieczne do umożliwienia konkretnego skorzystania ze wspomnianych usług przez tego użytkownika i zafakturowania kosztów takiego korzystania, przy czym cel polegający na zapewnieniu ogólnej funkcjonalności tychże usług nie może uzasadniać korzystania z tych danych po zakończeniu przeglądania danych mediów”[136].

Odnosząc się do kwestii związanej z adresem IP warto wspomnieć, że we wcześniejszym wyroku *Scarlet Extended*[137], Trybunał stwierdził, że adresy IP użytkowników „stanowią chronione dane osobowe, jako że pozwalają na precyzyjną identyfikację tych użytkowników”[138]. Należy jednak zaznaczyć, że stanowisko to tyczyło się dostawców dostępu do Internetu, którzy gromadzą i identyfikują adresy IP użytkowników Internetu[139], a nie dostawców usług medialnych online, o czym wspomnieliśmy wyżej.

[135] *Ibidem.*

[136] *Ibidem.*

[137] Wyrok ETS z dnia 24 listopada 2011 r., C-70/10. Wyrok dostępny na stronie: http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=263718 [dostęp: 10.09.2021].

[138] *Ibidem.*

[139] http://curia.europa.eu/juris/document/document.jsf?text=%2522dyrektywa-%2B95%252F46%2522&docid=184668&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=994471#ctx1 [dostęp: 10.09.2021].

Interpretacji postanowień dyrektywy 95/46 Trybunał Sprawiedliwości dokonał także w sprawie *Maximillian Schrems przeciwko Data Protection Commissioner,* w której przedmiotem sporu była odmowa rozpatrzenia przez komisarza ds. ochrony danych osobowych skargi *M. Schremsa* z powodu przekazania przez *Facebook Ireland Ltd* do Stanów Zjednoczonych danych osobowych swoich użytkowników i przechowywania tych danych na serwerach położonych w tym państwie[140]. W niniejszej sprawie skarżący wystąpił z żądaniem do komisarza, aby ten zakazał spółce *Facebook Ireland* przekazywania jego danych osobowych do Stanów Zjednoczonych, ponieważ prawo i praktyka obowiązujące w tym państwie „nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na jego terytorium przed działaniami nadzorczymi prowadzonymi w nim przez władze publiczne. *Maximillian Schrems* odniósł się w tym względzie do informacji ujawnionych przez *E. Snowdena* na temat działalności amerykańskich służb wywiadowczych, a w szczególności służb *National Security Agency*"[141]. Komisarz uznał wniesioną skargę za bezpodstawną, argumentując przy tym, że kwestie związane z odpowiednim stopniem ochrony należy rozpatrywać zgodnie z decyzją Komisji 2000/520 przyjętą na podstawie art. 25 ust. 6 dyrektywy 95/46, w której Komisja stwierdziła odpowiedni stopień ochrony danych osobowych w Stanach Zjednoczonych. Na decyzję komisarza *M. Schrems* wniósł skargę do Sądu Najwyższego, który z uwagi na problem interpretacyjny powstały na tle art. 25 ust. 6 dyrektywy 95/46 zwrócił się z pytaniem prawnym do TSUE. Udzielając odpowiedzi na postawione przez sąd pytanie, Trybunał stwierdził, że „art. 25 ust. 6 dyrektywy 95/46 w związku z art. 7, 8 i 47 karty należy interpretować w ten sposób, iż decyzja

[140] Wyrok TSUE z dnia 6 października 2015 r., C-362/14. Wyrok dostępny na stronie: http://curia.europa.eu/juris/document/document.jsf?text=%2522dyrektywa-%2B95%252F46%2522&docid=169195&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=303606#ctx1 [dostęp: 10.09.2021].

[141] *Ibidem.*

przyjęta na podstawie tego przepisu, taka jak decyzja 2000/520, w której Komisja stwierdza, że państwo trzecie zapewnia odpowiedni stopień ochrony, nie stoi na przeszkodzie temu, aby krajowy organ nadzorczy państwa członkowskiego, w rozumieniu art. 28 tej dyrektywy, rozpatrzył skargę danej osoby dotyczącą ochrony jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, które zostały przekazane z państwa członkowskiego do tego państwa trzeciego, kiedy osoba ta podnosi, że obowiązujące w tym państwie trzecim prawo i praktyki nie zapewniają odpowiedniego stopnia ochrony"[142]. Natomiast co do decyzji 2000/520 dotyczącej, tzw. bezpiecznej przystani, Trybunał uznał ją za nieważną. „W następstwie tego wyroku sąd odsyłający uchylił oddalenie skargi *M. Schremsa* i przekazał ją komisarzowi do ponownego rozpoznania. W ramach wszczętego przez komisarza dochodzenia *Facebook Ireland* wyjaśniła, że znaczna część danych osobowych została przekazana *Facebook Inc.* na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych. Mając na uwadze te okoliczności, komisarz wezwał *M. Schremsa* do przeformułowania skargi"[143]. *Schrems* podniósł w niej, że prawo amerykańskie nakłada na *Facebook Inc.* obowiązek udostępnienia władzom amerykańskim, takim *jak National Security Agency (NSA) i Federal Bureau of Investigation (FBI)* w ramach programów nadzoru m.in. PRISM i UPSTREAM, przekazanych tej spółce danych osobowych. W związku z tym, *Schrems* zwrócił się do komisarza o zakazanie lub zawieszenie przekazywania jego danych osobowych do *Facebook Inc.* W wyniku prowadzonego w tej sprawie postępowania Sąd Najwyższy uznał, że zaszła konieczność wystąpienia z wnioskiem o wydanie przez TSUE orzecze-

[142] *Ibidem*.

[143] Wyrok TSUE z dnia 16 lipca 2020 r., C-311/18. Wyrok dostępny na stronie: https://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=PL&part=1&occ=first&mode=lst&pageIndex=0&cid=4517014 [dostęp: 10.09.2021].

nia w trybie prejudycjalnym. Stąd też w wyroku z dnia 16 lipca 2020 r. w sprawie *Schrems II*[144] dotyczącym transferu danych osobowych do USA Trybunał:

- unieważnił decyzję Komisji UE 2016/1250 dotyczącą tzw. tarczy prywatności;
- utrzymał w mocy decyzję Komisji UE 2010/87/UE zmienioną następnie decyzją Komisji UE 2016/2297 w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podwykonawcom mających siedzibę w państwach trzecich;
- zwrócił uwagę, by administratorzy i podmioty przetwarzające w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, które stanowić będą uzupełnienie dla standardowych klauzul ochrony.

Z uwagi jednak na brak doprecyzowania przez TSUE ostatniego z powyższych wymogów, EROD wydała w tym celu stosowne zalecenia. Sprowadzają się one do sześciu kroków, jakie administratorzy lub podmioty przetwarzające muszą podjąć. Zalicza się do nich:

1) zidentyfikowanie wszystkich transferów przekazywania danych osobowych do państw trzecich;
2) zweryfikowanie, czy wykorzystywane narzędzie przekazywania jest wymienione w rozdziale V RODO;
3) ocenę, czy prawo i/lub praktyki obowiązujące w państwie trzecim mogą mieć wpływ na skuteczność odpowiednich zabezpieczeń narzędzi transferu, które stosowane są w kontekście konkretnego transferu;
4) określenie i przyjęcie środków uzupełniających, które są niezbędne do dostosowania poziomu ochrony przekazywanych danych do unijnego standardu (np. szyfrowanie transmisji);

[144] *Ibidem.*

5) podjęcie formalnych kroków proceduralnych w celu przyjęcia dodatkowego środka ochrony danych;
6) ponowną ocenę – w odpowiednich odstępach czasu – poziomu ochrony danych osobowych przekazywanych do państw trzecich oraz monitorowanie, czy zaszły lub będą miały miejsce zmiany, które mogą mieć na to wpływ[145].

W tym miejscu należy także podkreślić, że 27 czerwca 2021 r. weszła w życie decyzja Komisji UE 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[146]. Decyzja ta zastąpiła wskazaną w wyroku *Schrems II* decyzję 2010/87, która utraciła moc 27 września 2021 r. Stosowanie nowych standardowych klauzul nie wyłącza jednak stosowania wskazanych wyżej zaleceń dotyczących wdrożenia skutecznych środków uzupełniających.

Korzystanie z usług, jakie oferowane są nam w Internecie i nie tylko, wymaga przetwarzania danych osobowych. Czynność ta może być dokonywana przez różne podmioty do realizacji określonych celów. Sama Unia Europejska oraz jej państwa członkowskie dostrzegają potrzebę przetwarzania danych osobowych ze względu na zapewnienie bezpieczeństwa obywatelom przed zagrożeniami stwarzanymi np. przez terroryzm[147]. Również i podmioty prywatne nie pozostają obojętne na pozyskiwanie informacji na temat użytkowników sieci, bowiem

[145] Recommendations 01/2020 on measures that suplement transfer tools to ensure compliance with EU level of protection of personal data. Version 2,0 adopted on 18 June 2021. Zalecenia dostępne na stronie: https://edpb.europa.eu/system/files/202106/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [dostęp: 10.09.2021].

[146] Dz. Urz. UE L 199 z 2021 r.

[147] E. Czarny-Drożdżejko, *Ochrona danych osobowych w internecie w świetle orzecznictwa Trybunału Sprawiedliwości,* „Przegląd Sądowy", listopad-grudzień 2015, s. 82.

przynosi im to korzyści majątkowe[148]. Aby zapewnić więc odpowiedni stopień ochrony danych osobowych, prawodawca unijny wdrożył w życie wiele regulacji prawnych. Kluczowe znaczenie przypisywało się dotychczas dyrektywie 95/46, którą Trybunał Sprawiedliwości UE miał okazję wielokrotnie interpretować. Na tle tej dyrektywy pojawiło się także orzecznictwo dotyczące prawa do bycia zapomnianym, które stanowi odrębny przedmiot rozważań w rozdziale drugim. Co ważne, prawo to zostało wprost uregulowane w przepisach RODO, które stosowane są od dnia 25 maja 2018 r. i opierając się na których miał okazję wypowiedzieć się Trybunał Sprawiedliwości UE, o czym także piszemy w rozdziale drugim.

3.5. Prawo do ochrony danych osobowych w polskim porządku prawnym i w praktyce orzeczniczej Trybunału Konstytucyjnego

W polskim porządku prawnym prawo do ochrony danych osobowych po raz pierwszy uregulowane zostało w Konstytucji RP. Kluczowe znaczenie ma w tym przypadku art. 51, wyrażający „prawo jednostki do ochrony danych osobowych, w zakresie którego wchodzi m.in. wymaganie ustawowej podstawy nałożenia obowiązku ujawnienia przez daną osobę informacji jej dotyczących (ust. 1), zakaz pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (ust. 2), prawo dostępu jednostki do dokumentów i zbiorów danych oraz żądania sprostowania bądź usunięcia danych nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (ust. 3 i 4). Art. 51 ust. 5 Konstytucji przewiduje natomiast, że zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa”[149].

[148] *Ibidem.*

[149] Wyrok TK z dnia 18 grudnia 2014 r., K 33/13.

Wskazany wyżej przepis gwarantuje autonomię informacyjną jednostki. Jak podkreślił Trybunał Konstytucyjny, istotą tej autonomii jest pozostawienie „każdej osobie swobody w określeniu sfery dostępności dla innych wiedzy o sobie”[150], przy czym „zasadą powszechnie przyjmowaną […] jest ochrona każdej informacji osobowej i przyznanie podstawowego znaczenia przesłance zgody osoby zainteresowanej na udostępnienie informacji”[151].

Z wyjątkiem regulacji konstytucyjnej, prawo do ochrony danych osobowych zostało określone na poziomie ustawodawstwa zwykłego. Fundamentalne znaczenie odegrała w tym przypadku ustawa o ochronie danych osobowych z 1997 r., która „oparta została na założeniu, że przetwarzanie danych, z uwagi na potencjalne zagrożenie dla praw jednostki, dopuszczalne jest tylko w przypadkach i przy spełnieniu warunków”[152] w niej określonych. Mimo że ustawa ta została uchylona, warto jednak zwrócić uwagę na jej art. 27 ust. 2 pkt 7[153], który był przedmiotem rozważań Trybunału Konstytucyjnego w zakresie użytego w tym przepisie sformułowania „usługi medyczne”. Wątpliwości powstałe na tle rozpatrywanej przez Trybunał sprawy dotyczyły tego, czy apteki mają prawo przetwarzania danych osobowych na temat stanu zdrowia osób ubezpieczonych. W literaturze przedmiotu wyrażone zostało stanowisko, że „«osobami zawodowo świadczącymi usługi

[150] Wyrok TK z dnia 12 listopada 2002 r., SK 40/01.

[151] *Ibidem.*

[152] Wyrok TK z dnia 19 lutego 2002 r., U 3/01.

[153] Art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. stanowił: Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:

„7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych”.

medyczne są również aptekarze»[154]. Trybunał Konstytucyjny podziela ten pogląd. Zdaniem Trybunału […] termin «usługi medyczne» użyty w art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych obejmuje m.in. zaopatrzenie pacjentów w leki. Analiza przepisów obowiązujących ustaw prowadzi do wniosku, że przetwarzanie przez apteki danych osobowych dotyczących stanu zdrowia spełnia przesłankę wymienioną"[155] we wskazanym przepisie. Wobec powyższego należy uznać, że „apteki mogą przetwarzać dane dotyczące stanu zdrowia zawarte na receptach przedstawionych do realizacji, w zakresie niezbędnym dla zaopatrywania pacjentów w leki i materiały medyczne"[156].

Co do przetwarzania tzw. danych wrażliwych, Trybunał Konstytucyjny wypowiedział się również w sprawie K 39/12, która dotyczyła wątpliwości powstałych na tle art. 29 ust. 1 pkt 2 lit i) ustawy o Najwyższej Izbie Kontroli, pozwalającego upoważnionym przedstawicielom NIK do przetwarzania danych wrażliwych, o których mowa w art. 27 ust. 1 u.o.d.o.[157]. Rozpatrując tę sprawę, Trybunał zaznaczył, że „analiza zakresu zadań powierzonych przez ustrojodawcę i ustawodawcę Najwyższej Izbie Kontroli wskazuje, iż w obszarze zainteresowania tego organu znajdują się głównie stosunki o charakterze publicznoprawnym, w których dochodzi do wydatkowania środków publicznych w związku z realizacją konkretnych zadań o znaczeniu ogólnospołecznym lub też świadczeń na rzecz obywateli. Można za-

[154] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz,* Kraków 2001, s. 434.

[155] Wyrok TK z dnia 19 lutego 2002 r., U 3/01.

[156] *Ibidem.*

[157] Art. 27 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. stanowił: Ust. 1. „Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym".

tem powiedzieć, iż przydatne dla realizowania powierzonych NIK kompetencji będą dane osobowe relewantne dla stosunków publicznoprawnych, ujawniane w ramach kontaktów jednostki z szeroko rozumianymi organami władzy publicznej, przede wszystkim administracją rządową i samorządową oraz podmiotami prawa świadczącymi usługi publiczne finansowane ze środków publicznych. […] Trudno jednak wykazać funkcjonalny związek kompetencji NIK z obszarem aktywności jednostek, w których dochodzi do ujawnienia danych dotyczących […] przekonań religijnych lub filozoficznych, […] kodu genetycznego, nałogów i życia seksualnego. W konsekwencji dane tego typu należy uznać za nieprzydatne z perspektywy konstytucyjnego i ustawowego zakresu działania NIK […]"[158]. Co do przetwarzania przez upoważnionych przedstawicieli NIK pozostałych danych wrażliwych, tj. ujawniających pochodzenie rasowe, etniczne, przynależność wyznaniową, partyjną lub związkową, stan zdrowia, dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, Trybunał uznał, że czynność ta jest przydatna do „zapewnienia efektywności realizacji konstytucyjnych i ustawowych kompetencji NIK"[159].

[158] Wyrok TK z 20 stycznia 2015 r., K 39/12.

[159] *Ibidem*. W tym miejscu warto dodać, że Trybunał, odnosząc się do art. 27 ust. 2 pkt 2 u.o.d.o., zwrócił także uwagę na to, iż „z przepisu tego *per se* nie wynika kompetencja podmiotów przetwarzających dane. […] przepis ten nie ma też charakteru odsyłającego lub upoważniającego do dokonania dalszych czynności prawodawczych. Prawodawca, korzystając z konstytucyjnej kompetencji prawodawczej, w każdej chwili może bowiem wprowadzić wyjątki od regulacji zawartej w ustawie o ochronie danych, o ile wyjątki te są zgodne z normami hierarchicznie wyższymi. […]. Formułując m.in. wymóg zapewnienia «pełnych gwarancji ochrony danych» w wypadku każdego odstępstwa od zakazu przetwarzania danych wrażliwych, art. 27 ust. 2 pkt 2 ustawy o ochronie danych pełni rolę przepisu o istotnym systemowym znaczeniu. Jego treść musi być bowiem każdorazowo brana pod uwagę przez interpretatora podczas rekonstrukcji norm z przepisów innych ustaw, które upoważniają określone podmioty w konkretnych okolicznościach do przetwarzania danych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych. Innymi słowy, z art. 27 ust. 2 pkt 2 ustawy o ochronie danych wynika w szczególności ograniczenie kompetencji każdego z podmiotów usta-

Innym przykładem, w którym Trybunał Konstytucyjny odniósł się do ochrony danych osobowych, jest sprawa dotycząca niekonstytucyjności „druku L-4". Problem, o którym mowa, pojawił się na gruncie § 5 ust. 1 rozporządzenia[160], które zobowiązywało do uwidocznienia w zaświadczeniu lekarskim numeru statystycznego choroby[161]. Poddana kontroli regulacja wykraczała poza obszar delegacji ustawowej, określonej w art. 50 ustawy z 17 grudnia 1974 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, bowiem ustawa ta nie uzależniała „prawa pracownika do zasiłku chorobowego od przekazania zakładowi informacji o przyczynie niezdolności do pracy, a zwłaszcza rodzaju jego choroby"[162]. W konsekwencji Trybunał orzekł niezgodność § 5 ust. 1 rozporządzenia z art. 31 ust. 3, art. 47, art. 51 ust. 1, 2 i 5 Konstytucji RP oraz z art. 8 EKPC i art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych, a także z art. 50 ust. 2 wskazanej wyżej ustawy, ponieważ ustanawia ograniczenia w zakresie korzystania z konstytucyjnych praw i wolności obywatelskich, zastrzeżone do wyłączności ustawowej.

W wyroku K 32/04 dotyczącym ustawy o Policji, Trybunał Konstytucyjny, mając na uwadze m.in. art. 51 Konstytucji będący wzorcem kontroli, podkreślił, że „w demokratycznym państwie prawnym nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji. Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy do-

wowo upoważnionych do przetwarzania danych wrażliwych. Mogą one wykonywać swą kompetencję jedynie, jeśli istnieją «pełne gwarancje ochrony» danych wrażliwych przetwarzanych bez zgody osoby, której dane dotyczą. Przepis ten pełni doniosłą funkcję w procesie rozstrzygania horyzontalnych niezgodności norm", *ibidem.*

[160] Rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 r. w sprawie orzekania o czasowej niezdolności do pracy.

[161] Wyrok TK z dnia 19 maja 1998 r., U 5/97.

[162] *Ibidem.*

puszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny. Ingerencja policji w sferę praw i wolności obywatelskich, związana z czynnościami operacyjnymi podejmowanymi w interesie publicznym, nie może być nieograniczona”[163].

Z kolei w sprawie K 23/11 dotyczącej retencji danych telekomunikacyjnych, Trybunał Konstytucyjny zwrócił uwagę, że „warunkiem niejawnego uzyskania informacji o jednostkach, w tym dotyczących ich danych telekomunikacyjnych, jest ustanowienie procedury niezwłocznej selekcji oraz niszczenia materiałów zbędnych i niedopuszczalnych. Rozwiązanie to zapobiega nieuprawnionemu wykorzystaniu przez organy państwa zebranych legalnie informacji i ich przechowywaniu na wszelki wypadek, gdyby w przyszłości okazały się przydatne do innych celów”[164]. Jak podkreślił Trybunał, zakwestionowane przepisy, tj. art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym i art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, nie regulują postępowania z danymi telekomunikacyjnymi po ich zgromadzeniu. Wobec tego nie ma „prawnych podstaw do odpowiedniego stosowania przepisów regulujących niszczenie danych zgromadzonych w kontroli operacyjnej czy przepisów k.p.k. regulujących kontrolę i utrwalanie treści rozmów”[165]. Oznacza to, że na gruncie wskazanych wyżej przepisów „nie ma żadnych regulacji dotyczących weryfikacji oraz niszczenia danych zbędnych. Nie jest wobec tego wykluczone przechowywanie danych nieprzydatnych w prowadzonym postępowaniu, w toku którego wystąpiono o te dane, ani nawet do innych usprawiedliwionych konstytucyjnie celów”[166]. Mając powyższe na względzie, Trybunał orzekł, że „art. 28 ustawy o ABW, art. 18

[163] Wyrok TK z dnia 12 grudnia 2005 r., K 32/04.
[164] Wyrok TK z dnia 30 lipca 2014 r., K 23/11.
[165] *Ibidem.*
[166] *Ibidem.*

ustawy o CBA oraz art. 32 ustawy o SKW w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzącego postępowanie, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. Art. 75d ust. 5 ustawy o Służbie Celnej w zakresie w jakim zezwala na zachowanie materiałów innych niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 ustawy Kodeks karny skarbowy, jest niezgodny z art. 51 ust. 4 Konstytucji"[167].

Jak wynika z przedstawionych powyżej rozwiązań, prawo do ochrony danych osobowych uregulowane zostało dopiero w obecnie obowiązującej Konstytucji. Kluczowe znaczenie ma w tym przypadku art. 51, który „ma charakter kompleksowy, co oznacza, że prawo to kształtuje kilka powiązanych ze sobą uprawnień, odnoszących się do poszczególnych obszarów ochrony danych osobowych i stanowiących swego rodzaju elementy składowe tego prawa"[168]. Elementy te wyrażone zostały w pięciu ustępach art. 51, który dla Trybunału Konstytucyjnego wielokrotnie był wzorcem kontroli. Przepis ten pełni rolę gwaranta autonomii informacyjnej jednostki, rozumianej jako „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"[169].

Rozwinięciem wspomnianego wyżej przepisu Konstytucji była obowiązująca do maja 2018 r. ustawa o ochronie danych osobowych z 1997 r., z postanowień której można było przyjąć, że wyróżniała ona

[167] *Ibidem.*

[168] M. Sakowska-Baryła, *Konstytucjonalizacja prawa do ochrony danych osobowych w Polsce*, „Przegląd Prawa Konstytucyjnego" 2016, nr 4 (32), s. 129. Por. M. Wyrzykowski, *Ochrona danych – zagadnienia konstytucyjne,* [w:] M. Wyrzykowski (red.), *Ochrona danych osobowych,* Warszawa 1999, s. 24; P. Sarnecki, *Komentarz do art. 51,* [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. III, Warszawa 2003, s. 1 i n.

[169] Wyrok TK z dnia 18 grudnia 2014 r., K 33/13. Zob. też: wyrok TK z dnia 19 lutego 2002 r., U 3/01; wyrok TK z dnia 20 listopada 2002 r., K 41/02.

dwa rodzaje danych, tj. dane zwykłe (np. imię, nazwisko, adres zamieszkania, datę urodzenia, PESEL) i dane wrażliwe (szczególnie chronione, o których mowa w art. 27 ust. 1 u.o.d.o.). Ponadto warto dodać, że w orzecznictwie Trybunału Konstytucyjnego zwrócono uwagę, iż „nawet dane osobowe, które w innych okolicznościach mogą być uznane za tzw. dane wrażliwe (dotyczące np. przynależności politycznej, przekonań politycznych i religijnych), nie mogą podlegać ochronie przewidzianej dla danych sensytywnych, jeśli dotyczą osób pełniących funkcje publiczne i są przechowywane przez odpowiednie instytucje publiczne. Udostępnianie takich danych zwiększa jawność życia publicznego, a to z kolei sprzyja ochronie praw osób trzecich”[170]. Wobec powyższego, nie ulega wątpliwości, że zarówno art. 51 Konstytucji, jak i u.o.d.o. 1997, a obecnie RODO i u.o.d.o. 2018 mają istotne znaczenie w procesie wyznaczania standardów ochrony danych osobowych.

3.6. Współczesne zagrożenia prywatności i danych osobowych w Internecie

Powszechny dostęp do Internetu i towarzyszący mu rozwój nowych technologii sprawiły, że różnego rodzaju informacje – także te ze sfery prywatnej – zaczęły być udostępniane w świecie wirtualnym przez bardzo wiele osób. Wszystko to za sprawą popularnych portali społecznościowych, aplikacji, dzięki którym możemy monitorować stan zdrowia, dostosowywać dietę do własnych potrzeb, dokonywać płatności itp., czy dostępnych dla każdego usług − za które w większości nie płacimy pieniędzmi, lecz naszymi danymi osobowymi.

Często wiele osób nie zdaje sobie sprawy z tego, że dane, które dobrowolnie udostępniają, np. na własnym profilu, są coraz cenniejsze dla firm oferujących usługi internetowe. Bezkrytyczne zachowanie internautów korzystających – jakby się mogło wydawać – z „dobro-

[170] Wyrok TK z dnia 20 marca 2006 r., K 17/05.

dziejstw wirtualnych" sprawia, że sfera prywatności staje się na własne życzenie sferą przezroczystą. Najlepszym przykładem jest *Facebook*, bowiem jego użytkownicy, aby stać się rozpoznawalnymi, podają przy rejestracji swoje dane osobowe, tj. imię i nazwisko, datę urodzenia, płeć, adres e-mail. Korzystanie z tego serwisu daje w zamian wiele możliwości, np. kontakt z innymi osobami, przystąpienie do określonych grup zainteresowań, zamieszczanie zdjęć, wymianę opinii, polecanie stron internetowych naszym znajomym itp. Co prawda, w ustawieniach prywatności każdy użytkownik może wybrać opcję, aby jego profil był ogólnie dostępny lub tylko dla wybranych przez siebie osób, niemniej należy pamiętać, że informacje na nasz temat przekazywane są innym podmiotom, np. firmom należącym do *Facebooka* czy partnerom zewnętrznym[171].

W świecie wirtualnym występuje wiele zagrożeń naszej prywatności, w tym danych osobowych, których przykładów nie sposób zliczyć. Warto zwrócić uwagę nie tylko na serwisy społecznościowe[172], lecz także na inne e-usługi. Za przykład posłuży nam „chmura obliczeniowa"[173], dzięki której użytkownik ma zapewniony dostęp do wirtualnego dysku i aplikacji na różnych serwerach[174]. Z usługi tej obecnie

[171] https://pl-pl.facebook.com/about/privacy/ [dostęp: 10.09.2021].

[172] Zob. na ten temat, P. Gawrysiak, *Portale internetowe – zagrożenia realne i pozorne,* [w:] G. Szpor, W.R. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012, s. 145 i n.; M. Czerniawski, *Portale społecznościowe a prawo do ochrony danych osobowych – zarys problemu,* [w:] G. Szpor i W.R. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012, s. 163 i n.

[173] Zob. na ten temat, B. Fischer, *Cloud computing – nowy technologiczny paradygmat zagrożeniem dla ochrony danych osobowych i prywatności,* Kraków 2013; B. Fischer, *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych – wybrane zagadnienia,* „Monitor Prawniczy" 2014, nr 9 – dodatek; E. Molenda-Kropielnicka, *Cloud computing – zagadnienia prawne,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2013, nr 1.

[174] „Zgodnie z szeroko akceptowaną definicją Krajowego Instytutu Norm i Technologii Stanów Zjednoczonych (NIST) chmura obliczeniowa to model umożliwiający powszechny, wygodny, udzielany na żądanie dostęp za pośrednictwem sieci do wspól-

korzysta wiele podmiotów głównie do celów biznesowych i prywatnych. Potwierdza to raport zaprezentowany przez *Netscope*, z którego wynika, że „przeciętne przedsiębiorstwo korzysta z 755 aplikacji chmurowych (w Europie 608), a ta liczba nieustannie wzrasta”[175]. Jeśli chodzi o dane przechowywane w chmurze, to według wyników „za ostatni kwartał 2016 r. 18,1% to dane o szczególnym znaczeniu, czyli:

– dane poufne: 4,4% (np. wyniki finansowe, biznesplany, kody źródłowe, algorytmy);
– dane dotyczące płatności: 2,3% (np. numery kart kredytowych, numery kont);
– dane medyczne: 1,6% (np. wyniki badań, informacje dotyczące terapii)”[176].

Chmura obliczeniowa jako jeden ze sposobów przechowywania danych, z pewnością jest wygodnym rozwiązaniem. Warto jednak pamiętać, że zanim zdecydujemy się z niego skorzystać, należy sprawdzić m.in. „czy zasady ochrony danych gwarantują zapewnienie bezpieczeństwa przekazywanych informacji, ich poufności, integralności itd. Problem staje się o wiele bardziej skomplikowany w sytuacji, w której przetwarzanie danych odbywa się na terenie kilku państw bądź nawet podległym wyłącznie jurysdykcji międzynarodowej. Przed wyborem stosownej usługi niezbędne jest zatem przeprowadzenie audytu, który umożliwi ustalenie sytuacji prawnej ADO-klienta i jego

nej puli możliwych do konfiguracji zasobów przetwarzania (np. sieci, serwerów, przestrzeni przechowywania, aplikacji i usług), które można szybko dostarczyć i uwolnić przy minimalnym wysiłku zarządzania lub działania dostawcy usługi. […]. Do głównych typów chmur zaliczają się chmury publiczne, prywatne i hybrydowe; najważniejszymi usługami oferowanymi przez takie chmury są oprogramowanie jako usługa (SaaS), platforma jako usługa (PaaS) i infrastruktura jako usługa (IaaS)”, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf [dostęp: 10.09.2021].

[175] K. Alama, M. Kawecki, *Zmiana pogody dla usług chmurowych,* „ABI Expert” 2017, nr 1 (2), s. 40.

[176] *Ibidem.*

relacji z usługodawcą”[177]. Z uwagi na konkurencyjność ofert dostawców wspomnianej usługi, użytkownik w celu zwiększenia bezpieczeństwa danych może skorzystać z opcji ich szyfrowania. Jest to bardzo istotne, zwłaszcza że użytkownicy chmury najczęściej korzystają z modelu SaaS[178], który zapewnia dostawcy tej usługi pełny dostęp do danych, jeśli nie zostaną one uprzednio zaszyfrowane[179]. W przypadku modelu IaaS i modelu PaaS „skuteczna ochrona danych, w tym danych osobowych, leży w rękach użytkownika”[180], bowiem w modelach tych „dostawca nie ma do nich rzeczywistego dostępu”[181]. Jak się okazuje, poza szyfrowaniem, „warunkiem istnienia i konkurowania na rynku usług chmurowych”[182] stała się również możliwość wyboru przez użytkownika lokalizacji serwerów, na których są przetwarzane dane, co niewątpliwie zwiększa gwarancje ochrony danych osobowych.

Z wyjątkiem wskazanych wyżej przykładów szczególnym źródłem zagrożenia danych osobowych w Internecie jest np. *phishing, pharming, sniffing. Phishing* określany jako wyłudzenie informacji,

[177] T.A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Wrocław 2014, s. 170 i n.

[178] „Pomiędzy modelami usług chmurowych istnieją znaczne różnice w zakresie kontroli poszczególnych jej warstw, wśród których wyróżniamy: infrastrukturę techniczną, sieć, przestrzeń dyskową (ang. *storage*), moc obliczeniową, aplikacje oraz dane.

Model IaaS. Dostawca posiada kontrolę jedynie nad warstwą infrastrukturalną, ponieważ to właśnie jej zapewnienie jest przedmiotem świadczonej usługi. Pozostałe elementy zapewnia i kontroluje użytkownik, przy czym zdarza się, że strony wspólnie kontrolują warstwę sieciową praz przestrzeń dyskową.

Model PaaS. Użytkownik dysponuje obszernym zakresem kontroli dostawcy, który w tym przypadku jest głównym podmiotem odpowiedzialnym za pierwsze trzy warstwy, natomiast zarządzanie mocą obliczeniową oraz warstwą aplikacyjną jest dzielone między stronami. Tu jedyną warstwą, nad którą kontrolę ma wyłącznie użytkownik usługi, są dane.

Model SaaS. W przypadku SaaS użytkownik traci wyłączność kontroli nawet nad warstwą «danową», podczas gdy to dostawca usługi chmurowej ma dostęp do wszystkich jej warstw”, K. Alama, M. Kawecki, *Zmiana pogody*…, s. 41.

[179] *Ibidem.*

[180] *Ibidem.*

[181] *Ibidem.*

[182] *Ibidem*, s. 42.

oszustwo, kradzież tożsamości, jest metodą „pozyskiwania informacji (np. imienia i nazwiska, numeru konta bankowego, hasła do konta na portalu społecznościowym – przyp. M.J. i J.W.) od użytkownika np. poprzez fałszywe maile lub strony WWW”[183]. Następuje to „przez wstrzyknięcie kodu programu i wykonywanie złośliwego kodu, oszukiwanie/udawanie czy manipulację”[184]. Wystarczy więc np. otworzyć wiadomość lub wejść na daną stronę internetową i kliknąć zamieszczony tam link, aby rozpoczął się proces instalacji oprogramowania, które ma szkodliwe działanie dla użytkownika[185]. Zdecydowanie „trudniejszą do rozpoznania i przez to bardziej niebezpieczną dla użytkownika formą *phishingu*”[186] jest *pharming,* który może przybrać dwie formy[187]. Pierwsza polega na zainstalowaniu przez hakera złośliwego oprogramowania na komputerze użytkownika, w efekcie czego następuje automatyczne jego przekierowanie „na fałszywe strony internetowe, które do złudzenia przypominają oryginalne”[188]. Natomiast druga forma *pharmingu,* która jest bardziej niebezpieczna, wymaga przeprowadzenia ataku polegającego na infekcji całego serwera DNS, w związku z czym każda osoba, która będzie próbować wejść na prawdziwą stronę w rzeczywistości trafi na fałszywą[189].

Kolejną wyżej wymienioną metodą przechwytywania danych jest *sniffing*. „Jest ona niezmiernie trudna do wykrycia, ponieważ działalność osoby sniffującej pozostaje niezauważona dla użytkownika. W zakresie *sniffingu* mieści się monitorowanie, słuchanie zawartości transmisji danych komputerowych, obserwowanie, bądź przechwyty-

[183] A. Cieślik, *Zagrożenia dla prywatności – Phishing,* „ABI Expert” 2016, nr 1, s. 28.
[184] *Ibidem*, s. 29.
[185] http://bitdefender.pl/phishing-co-to-jest-i-czy-potrafisz-go-rozpoznac [dostęp: 10.09.2021].
[186] M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, s. 299.
[187] https://www.avast.com/pl-pl/c-pharming [dostęp: 10.09.2021].
[188] M. Siwicki, *Cyberprzestępczość,* s. 299.
[189] https://www.avast.com/pl-pl/c-pharming [dostęp: 10.09.2021].

wanie cudzych haseł dostępu, w skrajnych przypadkach także tych do banków”[190].

Świat wirtualny, do którego każdy ma obecnie dostęp, daje wiele możliwości, ale także niesie ze sobą wiele zagrożeń. Te ostatnie spowodowane są nie tylko przez postępowanie firm będących dostawcami usług, ale także wynikają z braku świadomości internatów, który przejawia się m.in. w bezkrytycznym udostępnianiu informacji o sobie, lekceważeniu nieścisłości w adresach e-mail, otwieraniu załączników w e-mailach nieznanego pochodzenia[191]. Wystarczy odnieść się np. do sposobu postępowania niektórych użytkowników *Facebooka*, którzy nie korzystają z ustawienia „prywatne”, lecz „publiczne”, co wiąże się tym, że publikując treści lub informacje zezwalają oni „wszystkim, w tym osobom niebędącym użytkownikami *Facebooka* na uzyskiwanie dostępu do tych informacji i wykorzystywanie ich, a także na wiązanie tych informacji z użytkownikiem (tj. jego imieniem i nazwiskiem oraz zdjęciem profilowym)”[192]. Ponadto „większość użytkowników – zarówno młodzież, jak i dorośli – nie zdaje sobie […] sprawy, że warunki korzystania z popularnych serwisów internetowych, jak *Flickr* czy *Twitter*, zapewniają tym firmom prawo wykorzystania udostępnionych przez użytkownika zdjęć bądź tekstów, jak im się tylko spodoba. […]. Dane wszak mogą zostać sprzedane i z dobrem użytkowników nikt nie będzie się liczył, gdy usługa przejdzie w ręce konkurencji lub firma splajtuje”[193].

Udostępnianie danych osobowych i innych informacji przychodzi niektórym zdecydowanie łatwiej w świecie wirtualnym niż rzeczywi-

[190] A. Rogacka-Łukasik, *Prawo do prywatności w dobie współczesnej ekspansji Internetu,* [w:] A. Kalisz (red.), *Prawa człowieka. Współczesne zjawiska, wyzwania, zagrożenia,* t. II, Sosnowiec 2015, s. 67.

[191] Por. A. Cieślik, *op. cit.,* s. 31.

[192] Regulamin Facebooka.

[193] C. Kurz, F. Rieger, *Pożeracze danych. O zawłaszczaniu danych i o tym, jak odzyskać nad nimi kontrolę,* Warszawa 2013, s. 70.

stym. Szczególnie widać to na przykładzie portali społecznościowych. Z analizy przeprowadzonej przez firmę Gartner wynika, że „rozwój technologii w serwisach społecznościowych jest o dwa kroki przed świadomością klientów na temat tego, jak ważna jest ochrona prywatności. Koncerny wykorzystują tę wyrwę i nieustannie przesuwają granicę, jeśli chodzi o rodzaj przechowywanych danych”[194]. Nic więc dziwnego, że sami założyciele serwisów społecznościowych mówią o końcu sfery prywatności. Mark Zuckerberg założyciel *Facebooka* powtarza, że „ochrona danych osobowych straciła znaczenie w społeczeństwie i w relacjach międzyludzkich”[195].

Mając powyższe na względzie, rację należy przyznać Ryszardowi Piotrowskiemu, który podkreśla że „rezygnacja z prywatności, stymulowana przez modę kreującą atrakcyjność nowych rozwiązań technicznych, staje się charakterystyczną cechą nowej kultury kształtującej sposób istnienia jednostki w cyfrowej społeczności, oparty na mniej lub bardziej świadomym wyrzeczeniu się autonomii informacyjnej i związanego z nią prawa do decydowania o tym, jakie informacje o sobie jednostka udostępnia innym, w tym zwłaszcza władzom publicznym oraz podmiotom gospodarczym”[196]. Wobec tego należy zastanowić się, czy chcąc „iść z duchem cyfryzacji” warto pod każdym względem dostosowywać się do trendu ograniczania prywatności, nie licząc się z ewentualnymi tego konsekwencjami, czy w trosce o swoją

[194] http://www.voxeurop.eu/pl/content/article/1090601-europa-kontra-facebook [dostęp: 10.09.2021].

[195] C. Kurz, F. Rieger, *op. cit.,* s. 83. Por. A. Jaskiernia, *Ochrona prywatności w epoce cyfrowej w perspektywie regulacyjnej Unii Europejskiej,* [w:] J. Jaskiernia (red. nauk.), *Europejski system ochrony praw człowieka. Aksjologia – instytucje – efektywność*, Toruń 2015, s. 135.

[196] R. Piotrowski, *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne,* [w:] A. Mednis (red.), *Prywatność a jawność – Bilans 25-lecia i perspektywy na przyszłość,* Warszawa 2016, s. 25. Zob. także A. Demczuk, *„Prawo do bycia zapomnianym” jako szczególne prawo jednostki do kontroli informacji o sobie w społeczeństwie informacyjnym w kontekście RODO,* „Zarządzenie i Finanse. Journal of Management and Finance” 2018, Vol. 16, No. 4/2, s. 90 i n.

prywatności, postępować ostrożnie w świecie wirtualnym, rezygnując przy tym ze zbędnych e-usług.

3.7. Autonomia cyfrowa jednostki jako element ochrony danych osobowych

Zgodnie z orzecznictwem Trybunału Konstytucyjnego, „autonomia informacyjna, wskazana w art. 51 Konstytucji, jest jednym z komponentów prawa do prywatności w szerokim znaczeniu, przyjętym w art. 47 Konstytucji[197]. Obejmuje ona […], prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących siebie, jak również prawo do kontrolowania tych informacji, jeżeli znajdują się w dyspozycji innych podmiotów. […]. Istotą autonomii informacyjnej jest pozostawienie każdej osobie swobody określenia sfery dostępności dla innych wiedzy o sobie. Zasadą powszechnie przyjmowaną wedle takiego ujęcia jest ochrona każdej informacji osobowej i przyznanie podstawowego znaczenia przesłance zgody osoby zainteresowanej na udostępnienie informacji”[198].

Przedstawiona powyżej definicja ma szeroki zakres oddziaływania. Odnosi się ona nie tylko do swobody decydowania o ujawnieniu informacji o sobie w świecie rzeczywistym, ale także i w świecie wirtualnym. W tym ostatnim na ujawnieniu naszych danych szczególnie zależy dostawcom e-usług, którzy zapewniają darmowy do nich dostęp, aby zachęcić klientów do korzystania z nich w zamian za ich dane osobowe i inne informacje z życia prywatnego. Użytkowanie staje się tym bardziej intensywne, im większą popularnością cieszy się dana usługa. Dlatego przywiązanie do niej użytkownika sprawia, że trudno mu z niej zrezygnować. Nie wyobraża on sobie wręcz takiego scena-

[197] Por. wyrok TK z dnia 20 czerwca 2005 r., K 4/04; wyrok TK z dnia 20 marca 2006 r., K 17/05; wyrok TK z dnia 22 lipca 2014 r., K 25/13.

[198] Wyrok TK z dnia 11 października 2016 r., SK 28/15.

riusza, skoro wszyscy bądź większość jego znajomych także korzysta z usług wirtualnych.

Dostarczanie informacji i danych w sieci następuje na wiele sposobów, np. przez używanie aplikacji na smartfonach. Ponadto, coraz większym zainteresowaniem cieszą się urządzenia typu *wearables*[199], np. *smartwatchach* (inteligentne zegarki), *smartband* (inteligentna opaska na rękę, która służy do rejestrowania naszej codziennej aktywności fizycznej), *watchband* (inteligentna zegarko-opaska), *Google Glass*[200]. Nie można przy tym pominąć portali społecznościowych, do których codziennie „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 z nas nie wie nawet, że w różnych serwisach można znaleźć o nich różne – mniej lub bardziej prywatne – informacje"[201].

Przejawów aktywności jednostki w sieci nie sposób zliczyć. Jednostka nie może także zapanować nad kontrolą udostępnianych przez nią danych, które często są udostępniane „pod silną presją wymagań współczesnej cywilizacji"[202]. W konsekwencji prowadzi to do tego, że

[199] Por. A. Mednis, *Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?,* [w:] A. Mednis (red.), *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość,* Warszawa 2016, s. 12.

[200] M. Jabłoński, J. Węgrzyn, *Zmiana modelu ochrony danych osobowych – podejście oparte na ryzyku, privacy by design i privacy by default,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne,* Wrocław 2017, s. 75. Na temat Internetu rzeczy zob. P. Leja, *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, „Prawo Mediów Elektronicznych" 2017, nr 3, s. 11 i n.

[201] K. Siewicz, *Prywatność w serwisach społecznościowych. Nowe wyzwania dla ruchu wolnego oprogramowania,* [w:] G. Szpor i W. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012, s. 189. Zob. K. Darowska, J. Lewandowska, *Ochrona dóbr osobistych w Internecie ze szczególnym uwzględnieniem portali społecznościowych,* [w:] A. Kalisz (red.), *Prawa człowieka. Współczesne zjawiska, wyzwania, zagrożenia,* T. II, Sosnowiec 2015, s. 73 i n.

[202] M. Sakowska-Baryła, *Prawo do ochrony*…, s. 33.

autonomia cyfrowa jednostki staje się fikcją w przestrzeni wirtualnej. Dlatego bardzo ważnym „krokiem na drodze do odzyskania cyfrowej autonomii jest krytyczne spojrzenie na to, jakie informacje o nas są naprawdę potrzebne, muszą zostać podane i będą gdzieś przechowywane przez całą wieczność”[203]. Wobec tego, bezsprzeczne jest, że to od jednostki zależy, czy chce ona korzystać z przyznanej jej autonomii cyfrowej w sposób świadomy, czy chce podążać za trendami internetowymi, udostępniając „za każdym kliknięciem” informacje o sobie, a tym samym przyczyniać się do tego, że autonomia, o której mowa, „będzie polegać nie tyle na jej samodzielnym, nieskrępowanym decydowaniu o zakresie udzielanych informacji, ale przede wszystkim na możliwości decydowania o samym fakcie uczestnictwa w wybranych przez nią (choć nie zawsze jest to wolny wybór) układach społecznych, zawodowych lub środowiskowych. Konsekwencje tego wyboru będą jednak pozostawać poza jej kontrolą”[204]. Dla większości osób nie ma to jednak znaczenia, ponieważ chęć bycia na bieżąco z popularnymi rozwiązaniami jest silniejsza. Jednostka w dobie powszechnej cyfryzacji, nie ma więc potrzeby bycia anonimową. Wynika to przede wszystkim z braku świadomości, braku zainteresowania się tym, co się dzieje z jej danymi, a także niezdawaniem sobie sprawy z zagrożeń występujących w sieci. Nie zawsze też jednostka może pozostać anonimowa, zwłaszcza gdy dokonuje różnego rodzaju transakcji. Pomimo tego należy pamiętać, że to anonimowość gwarantuje użytkownikowi „ochronę przed inwigilacją i wykorzystaniem informacji”[205].

Korzystając z Internetu każdy z nas pozostawia pewne ślady, tj. informacje będące pożywką dla algorytmów, które „analizują dane dotyczące zachowań czy historii przeglądanych stron użytkowników. Wykorzystywane są do tego głównie pliki *cookies*. Na tej podstawie

[203] C. Kurz, F. Rieger, *op. cit.,* s. 79.
[204] M. Sakowska-Baryła, *Prawo do ochrony*…, s. 34.
[205] C. Kurz, F. Rieger, *op. cit.,* s. 95.

można stworzyć profil użytkownika[206] i dopasować do niego «potencjalnie» interesującą reklamę czy rekomendować produkt. Coraz większe znaczenie ma analizowanie informacji pochodzących z porali społecznościowych. W tym przypadku w grę wchodzą nie tylko informacje o przeglądanych stronach, ale wszystkie dane dotyczące konkretnej osoby, jej powiązaniach, miejscu zamieszkania, znajomych itp."[207]. Dlatego, jeśli nie chcemy być „śledzeni" przez te pliki, możemy wyłączyć ich obsługę w ustawieniach naszej przeglądarki. W przeciwnym wypadku pliki *cookies* będą towarzyszyć nam na każdym kroku.

Swoboda udostępniania informacji w świecie wirtualnym przysługuje każdemu. Niektórzy korzystają z niej roztropnie, inni wręcz odwrotnie. Trzeba jednak mieć na uwadze, że im bardziej szczerzy są internauci korzystający z e-usług, tym szybciej tracą oni kontrolę nad własnymi danymi. Wobec powyższego można stwierdzić, że autonomia cyfrowa jednostki, z której umiejętnie ona korzysta, stanowi ważny element ochrony danych osobowych, a co za tym idzie i sfery prywatności.

[206] Na temat profilowania zob. M. Hildebrandt, *Defining profiling: new type of knowledge?,* [w:] M. Hildebrandt, S. Gutwirth (eds.), *Profiling the European Citizens, Cross-Disciplinary Perspectives,* Springer 2008, s. 17 i n.; K. Vries, *Identity, profiling algorithms and a world of ambient intelligence*, "Ethics and Information Technology" 2010, vol. 12, no. 1, s. 71 i n.; J.M. Such, A. Garcia-Fornes, V. Botti, *Automated buyer profiling control based on human privacy attitudes*, "Electronic Commerce Research and Applications" November 2013, vol. 12, no. 6, s. 386 i n.; X. Konarski, *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce,* „Monitor Prawniczy" 2016, nr 2, s. 48 i n.

[207] http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf [dostęp:10.09.2021]. Por. A. Banaszewska, *Prawo do prywatności we współczesnym świecie*, „Białostockie Studia Prawnicze" 2013, z. 13, s. 132.

4. Granice prywatności i danych osobowych w Internecie

Nie ulega wątpliwości, że obowiązkiem organów państwa jest zagwarantowanie odpowiedniej ochrony prywatności i danych osobowych jednostki także przed zagrożeniami płynącymi spoza jego granic. Jak podkreśla Trybunał Konstytucyjny, obowiązek ten „rozciąga się […] na zapewnienie ochrony prywatności przed monitorowaniem rozmaitych sfer aktywności życiowej obywateli, w tym wiadomości przesyłanych za pomocą sieci telekomunikacyjnych przez podmioty zagraniczne, a zwłaszcza państwa obce. Naruszenie prawa do ochrony prywatności zagwarantowanego w art. 47 Konstytucji (a także prawa do ochrony danych osobowych – art. 51 Konstytucji, przyp. M.J. i J.W.) może […] nastąpić nie tylko przez bezpośrednie działanie polskich organów państwa, pozyskujących informacje o jednostkach w sposób niejawny. Nastąpi to również w sytuacji braku dostatecznej ochrony obywateli przez państwo przed ingerencją w tę wolność, spowodowaną działaniami innych podmiotów”[208].

Nie sposób odmówić słuszności zajętemu przez Trybunał stanowisku, zwłaszcza że w świecie epoki cyfrowej społeczeństwo „z pomocą subtelnych technologii informacyjnych i komunikacyjnych, wkracza w wirtualne przestrzenie wraz z ich licznymi sieciami społecznościowymi, w których za pomocą słów i obrazów udziela informacji prywatnych i intymnych”[209], do których mają lub mogą mieć dostęp zarówno organy państwa, jak i podmioty prywatne. Co prawda, wszelkie przejawy działalności podmiotów pozyskujących informacje na nasz temat muszą być unormowane w ustawie, „ograniczone do koniecznych sytuacji, dopuszczalnych w demokratycznym państwie

[208] Wyrok TK z dnia 30 lipca 2014 r., K 23/11.

[209] M.T. Tinnefeld, *Jak Internet zmienia prawne ramy prywatności?,* [w:] G. Szpor, W. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012, s. 3 i n.

wyłącznie dla ochrony konstytucyjnie uznanych wartości i zgodnie z zasadą proporcjonalności”[210], to jednak w praktyce pojawiają się nadużycia w tym zakresie. W konsekwencji prowadzi to do tego, że granice prywatności i danych osobowych jednostki w przestrzeni wirtualnej, bo o niej tu mowa, mają charakter iluzoryczny.

Odnosząc się do niejawnego pozyskiwania informacji przez funkcjonariuszy służb odpowiedzialnych za bezpieczeństwo i porządek publiczny, należy zaznaczyć, że wejście ich w posiadanie danych o jednostce „następuje w sposób praktycznie niezauważalny dla zainteresowanego. Zazwyczaj nie wie on nawet, że dane dotyczące jego osoby zostały pozyskane lub zatrzymane ani jak szeroka jest wiedza służb policyjnych bądź służb ochrony państwa na jego temat, czy w jakich sytuacjach wiedza ta zostanie potem wykorzystana. Chociaż na podstawie pojedynczych danych, w tym danych telekomunikacyjnych, zebranych w toku czynności operacyjno-rozpoznawczych, nie sposób jeszcze zrekonstruować całej społecznej aktywności jednostki, to po szczegółowej ich analizie możliwe jest zbudowanie profilu osobowego osób uczestniczących w procesie komunikacji, a co za tym idzie ustalanie ich trybu życia, przynależności do organizacji społecznych czy politycznych, kontaktów z takimi organizacjami, a także

[210] Wyrok TK z dnia 30 lipca 2014 r., K 23/11. W wyroku TK z dnia 23 czerwca 2009 r., Trybunał podkreślił, że „Czynności operacyjne służb państwowych pozostają usprawiedliwione, o ile ich celem jest obrona wartości demokratycznego państwa prawnego. Wymogiem konstytucyjnym jest to, by sprostały one testowi «konieczności w demokratycznym państwie prawnym». Nie wystarczy ich celowość, użyteczność, taniość czy łatwość posługiwania się przez władzę. Nie ma rozstrzygającego znaczenia argument, że podobne środki są stosowane w innych państwach. Usprawiedliwione jest stosowanie środków niezbędnych w tym sensie, że chronią wartości istotne w państwie demokratycznym, i to w sposób (bądź w stopniu), który nie mógłby zostać osiągnięty przy stosowaniu innych środków. Jednocześnie winny to być «środki najmniej uciążliwe dla podmiotów, których prawo bądź wolność ulegają – w wyniku stosowania tych środków – ograniczeniu» (por. uzasadnienie wyroku TK z 3 października 2000 r., sygn. K 33/99, OTK ZU nr 6/2000, poz. 188, s. 1003 i 1004)”.

osobistych upodobań i skłonności osób poddanych obserwacji”[211]. Wprawdzie przyznanie organom państwa instrumentów pozwalających na pozyskiwanie różnego rodzaju danych służy do walki z przestępczością, to nie jest dozwolone, aby w demokratycznym państwie prawa dochodziło do rejestrowania „całokształtu życia prywatnego jednostek, zwłaszcza w sposób umożliwiający rekonstrukcję wszelkich przejawów ich życiowej aktywności. Stanowiłoby to naruszenie istoty prawa do prywatności, tajemnicy komunikowania się i autonomii informacyjnej, czego bezwzględnie zabrania art. 31 ust. 3 zdanie drugie Konstytucji”[212].

Pozyskiwanie danych osobowych i informacji ze sfery prywatności musi – na co zwrócił uwagę Trybunał Konstytucyjny – odbyć się w zgodzie z zasadami przyjętymi w Konstytucji RP. Zasady te wyznaczają więc pewne granice, poza które organy państwa, jak i podmioty prywatne nie mogą wychodzić. O ile w przypadku tych pierwszych, tj. służb państwowych, gromadzone przez nich dane służą przeciwdziałaniu przestępczości, to już w przypadku tych drugich, tj. podmiotów prywatnych, mają one na celu osiągnięcie korzyści majątkowych. Zysk dostawców e-usług uzależniony jest od tego, jak bardzo popularna stanie się dana usługa i jak wielu użytkowników będzie z niej korzystać. Doskonałym przykładem są portale społecznościowe, w których pozostawiamy wiele danych. Problem w tym, że większość ich użytkowników nie czyta regulaminów lub robi to niedokładnie, bez zrozumienia, a przecież to w nich zamieszczone są lub powinny być najważniejsze informacje. Akceptacja warunków danej usługi prowadzi lub może

[211] Wyrok TK z dnia 30 lipca 2014 r., K 23/11.

[212] *Ibidem.* Art. 31 ust. 3 Konstytucji RP „Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanowione tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw”.

prowadzić do utraty kontroli nad własnymi danymi. Praktyka pokazuje, że faktycznie nadużycia zdarzają się, o czym wspomniał Edward Snowden. Zwrócił on bowiem uwagę na to, że „firmy o ogromnym potencjale, jak *Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, YouTube i Apple* udostępniają NSA (*National Security Agency* – przyp. M.J. i J.W.) swoje serwery i zasoby"[213]. Wobec powyższego, bezsprzeczne jest, że to jednostka przez swoje zachowanie w sieci „zamazuje" granice prywatności i danych osobowych, co wynika z deficytu informacji na temat zagrożeń występujących w przestrzeni wirtualnej. Bez winy nie pozostają także dostawcy usług, którzy celowo czasami tworzą lakoniczne lub niezrozumiałe regulaminy, aby czerpać korzyści z danych o jednostce.

Z określeniem granic prywatności i danych osobowych w Internecie wiąże się także zagadnienie dotyczące poczty elektronicznej[214]. W przypadku tej usługi, problemem jest spam, a więc niechciana wiadomość elektroniczna. Nadawcą tej wiadomości są przede wszystkim firmy, które dopuszczają się naruszenia granicy naszej prywatności, przesyłając ją regularnie bez naszej wiedzy i przyzwolenia. Z pewnością „nękanie" niechcianymi e-mailami jest uporczywe dla internauty, niemniej bardziej ingerujące – bo naruszające nie tylko prywatność, ale także i dane osobowe − są działania hakerów, którzy przesyłają do adresata, e-mail, po kliknięciu którego dochodzi do instalacji złośliwego trojana (*phishing, pharming*)[215]. Nie budzi zatem wątpliwości, że spam i jego odmiany są nie tylko uciążliwe, ale także mogą być szkodliwe dla użytkownika poczty elektronicznej. Do najczęstszych szkód zalicza się:

[213] M. Czakowski, *Zagrożenie prywatności w obliczu wojny w sieci,* [w:] *Sapientiae Servientes. Księga Jubileuszowa Profesor Krystyny Kwaśniewskiej,* Bydgoszcz 2015, s. 39 i n.

[214] A. Rogacka-Łukasik, *op. cit.*, s. 68.

[215] Na temat zagrożeń w Internecie takich jak *phishing, pharming,* zob. pkt 3.6. Współczesne zagrożenia prywatności i danych osobowych w Internecie.

– „możliwość utraty otrzymanych wiadomości e-mail poprzez blokowanie skrzynki odbiorczej;
– wyłudzenie danych adresowych, adresu e-mail, a nawet numeru konta bankowego;
– zagrażanie bezpieczeństwu komputera oraz emisja materiałów niepożądanych przez użytkownika;
– zagrożenie zarażeniem szkodliwym wirusem”[216].

Aby skutecznie chronić się więc przed spamem, internauci powinni korzystać z programów antywirusowych i antyspamowych. Czasami jednak i one mogą okazać się niewystarczające, w sytuacji gdy będziemy mieli do czynienia z działaniem hakera, który umiejętnie ominie filtry antyspamowe. „Chodzi o przesyłanie spamu w postaci tzw. map bitowych, a więc obrazka zawierającego ukrytą treść reklamy. Tego rodzaju wiadomości nie zawierają załączników, co może być odczytane przez zabezpieczenia jako zwykła wiadomość”[217]. Dlatego każdy powinien pamiętać, aby usuwać e-maile nieznanego pochodzenia. Świadomość i ostrożność użytkownika sieci okazuje się zatem niezmiernie ważna, ponieważ to dzięki nim możemy chronić granice naszej prywatności i danych osobowych.

We współczesnym świecie Internet stał się narzędziem, które wykorzystywane jest do „tworzenia, przechowywania i przekazywania danych o zróżnicowanym charakterze”[218]. Stanowi więc cenne źródło informacji o jednostce, które pozyskiwane są przez wiele podmiotów do różnych celów. W przypadku organów państwa służą one do walki z przestępczością, jednak mimo to funkcjonariusze służb, gromadząc informacje o jednostce, nie powinni przekraczać granic jej prywatności, które wyznaczone zostały przez Trybunał Konstytucyjny. Trudno

[216] https://poradnikprzedsiebiorcy.pl/-spam-definicja-rodzaje-historia-powstania-oraz-sposoby-ochrony/3 [dostęp: 10.09.2021].
[217] https://poradnikprzedsiebiorcy.pl/-spam-definicja-rodzaje-historia-powstania-oraz-sposoby-ochrony/2 [dostęp: 10.09.2021].
[218] Wyrok TK z dnia 30 lipca 2014 r., K 23/11.

powiedzieć, jak sytuacja wygląda w praktyce, skoro pozyskiwanie informacji na nasz temat odbywa się w niezauważalny dla nas sposób. Aby upewnić się, jakie dane znajdują się w dyspozycji służb państwa, moglibyśmy skorzystać z przysługującego nam konstytucyjnego prawa dostępu do dotyczących nas dokumentów urzędowych i zbiorów danych, jednak trzeba mieć na uwadze, że prawo to może zostać ograniczone w drodze ustawy, np. ze względu na objęcie informacji określoną klauzulą tajności. W przypadku podmiotów prywatnych, pozyskiwanie informacji o jednostce służy przede wszystkim do osiągnięcia zysku przez co granice prywatności i danych osobowych internautów są często przekraczane, czego potwierdzeniem są wskazane wyżej przykłady. W świecie wirtualnym trudno mieć więc kontrolę nad własnymi danymi, zwłaszcza gdy użytkownicy sieci udostępniają je – najczęściej na portalach społecznościowych. Dla niektórych osób nie stanowi to jednak żadnego problemu, ponieważ bezgranicznie ufają dostawcom e-usług, nie zdając sobie przy tym sprawy, co dzieje się z ich danymi. W konsekwencji to sami użytkownicy pozwalają na przekraczanie granic własnej prywatności i danych osobowych, zapominając o kierowaniu się zdrowym rozsądkiem, co może doprowadzić do negatywnych dla nich skutków.

Rozdział II

Prawo do bycia zapomnianym w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej i polskich sądów

1. Standardy ochrony prawa do bycia zapomnianym w orzecznictwie TSUE

Nie ulega wątpliwości, że wraz z wydaniem przez TSUE wyroku w sprawie *Google Spain*[219], prawo do bycia zapomnianym stało się

[219] Wyrok TSUE z dnia 13 maja 2014 r. w sprawie C-131/12 *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja Gonzâlez*. Sprawa, o której mowa, dotyczyła obywatela Hiszpanii *Mario Costeja Gonzâleza*, który wniósł do AEPD (hiszpańskiej agencji ochrony danych) skargę przeciwko hiszpańskiemu dziennikowi „La Vanguardia" oraz przeciwko *Google Spain i Google Inc*. Skarga opierała się na tym, że po wpisaniu do wyszukiwarki internetowej *Google* imienia i nazwiska skarżącego pojawił się link do dwóch stron dziennika „La Vanguardia" z 1998 r., na których widniało ogłoszenie w przedmiocie licytacji z nieruchomości związanej z jej zajęciem wynikającym z niezapłaconej przez *M. Costeja Gonzâleza* należności na rzecz zakładu zabezpieczeń społecznych. *M. Costeja Gonzâlez* zwrócił się o nakazanie „La Vanguardii" usunięcia lub zmiany tych stron internetowych w taki sposób, aby nie pojawiły się na nich jego dane osobowe. Ponadto, domagał się zobowiązania *Google Spain* lub *Google Inc.* do usunięcia lub ukrycia jego danych osobowych w taki sposób, aby nie były one ujawniane w wynikach wyszukiwania i powiązane z linkami do artykułów znajdującymi się w „La Vanguardia". W dniu 30 lipca 2010 r. AEPD oddaliła skargę w zakresie dotyczącym dziennika „La Vanguardia", uznając, że publikacja przedmiotowych artykułów była prawnie uzasadniona, gdyż nastąpiła na żądanie ministerstwa pracy i polityki społecznej. Celem publikacji było jak najszersze rozpowszechnienie informacji o licytacji, tak aby miała

przedmiotem szczególnego zainteresowania. Na mocy tego wyroku operatorzy wyszukiwarek internetowych zostali uznani za administratorów. Uruchomiło to lawinę wniosków kierowanych przez osobę, której dane dotyczą, do operatora wyszukiwarki internetowej z żądaniem usunięcia z listy wyników wyszukiwania – przeprowadzonego na podstawie imienia i nazwiska danej osoby – linków zawierających dotyczące tej osoby informacje. Skutkiem realizacji wniesionego żądania nie jest jednak całkowite usunięcie linku z wyszukiwarki. Informacje na temat danej osoby wciąż bowiem pozostają dostępne w sieci, tyle że przy użyciu innych terminów wyszukiwania aniżeli imię i nazwisko. Należy przy tym zauważyć, że Trybunał uzależnił realizację prawa do bycia zapomnianym od statusu osoby, której dane dotyczą. Poza kręgiem uprawnionych pozostawił bowiem osoby odgrywające rolę w życiu publicznym, co uzasadnił nadrzędnym interesem odbiorców polegającym na otrzymaniu w ramach wyszukiwania na podstawie imienia i nazwiska informacji dotyczących tych osób. Świadczy to o przypisaniu szczególnego znaczenia prawu do wolności informacji w procesie rozpatrywania przez administratora wniosku o usunięcie danych. Rów-

ona największą liczbę uczestników. Skarga *M. Costeja Gonzâleza* została jednak uwzględniona w zakresie dotyczącym *Google Spain i Google Inc*. AEPD uznała, że do operatorów wyszukiwarek internetowych mają zastosowanie przepisy z zakresu ochrony danych, ponieważ podmioty te dokonują przetwarzania danych osobowych, za które ponoszą odpowiedzialność. AEPD uznała, że ma prawo do nakazania usunięcia tych danych i zakazania operatorom wyszukiwarek dostępu do niektórych z nich, jeśli uzna, że ich umiejscowienie i stopień rozpowszechnienia mogą naruszać prawo do ochrony danych i godności osób w szerokim znaczeniu. AEPD uznała także, że obowiązek ten może bezpośrednio spoczywać na operatorach wyszukiwarek bez konieczności usuwania tych danych ze strony internetowej, na której się one znajdują, zwłaszcza gdy zachowanie tych informacji na stronie internetowej jest zgodne z prawem. Na decyzję tę *Google Spain i Google Inc*. wniosły skargi do *Audiencia Nacional* (sąd hiszpański). Zob. M. Wróbel, *Prawo do „bycia zapomnianym" – glosa – C-131/12*, „Monitor Prawniczy" 2017, nr 2, Legalis. H.J. McCarthy, *All the World's a Stage: The European right to be forgotten revisited from a US perspective,* "Journal of Intellectual Property Law and Practice" 2016, Vol. 11, No. 5, s. 360 i n.

nież w wyroku w sprawie *Manni*[220] Trybunał potwierdził, że realizacja prawa do bycia zapomnianym uwarunkowana jest od statusu osoby, której dane dotyczą. Stąd też w niniejszej sprawie uznano, że osoby fizyczne, które zdecydowały się uczestniczyć w wymianie handlowej za pośrednictwem spółki akcyjnej lub spółki z ograniczoną odpowiedzialnością i których dane osobowe znajdują się w rejestrze spółek nie mogą powoływać się na prawo do bycia zapomnianym, ponieważ mają one świadomość obowiązku upublicznienia danych dotyczących ich tożsamości i funkcji, jakie sprawują w spółce, gdy decydują się na podjęcie tego rodzaju działalności. Nie wyłącza to jednak prawa do wniesienia sprzeciwu wobec przetwarzania danych osobowych, bowiem nie można wykluczyć „zaistnienia sytuacji szczególnych, w których przeważające i uzasadnione względy dotyczące konkretnego przypadku osoby, której dane dotyczą, uzasadniają wyjątkowo, aby dostęp do figurujących w rejestrze danych dotyczących tej osoby został ograniczony po upływie wystarczająco długiego okresu od daty likwidacji danej spółki, do kręgu osób trzecich mających konkretny uzasadniony interes w uzyskaniu wglądu do tych danych”[221]. Wymaga to jednak analizy konkretnego przypadku oraz zdecydowania przez państwo

[220] Wyrok TSUE z dnia 9 marca 2017 r. w sprawie C-398/15 *Camera di Commercio, Industrirtigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu.* Sprawa, o której mowa, dotyczyła sporu między przedsiębiorcą *Salvatorem Mannim* a włoską izbą handlową w Lecce prowadzącą rejestr spółek. W dniu 12 grudnia 2007 r. *Manni* pozwał izbę handlową, podnosząc, że nie jest w stanie sprzedać wybudowanych budynków, ponieważ z rejestru spółek wynika, że był on jednoosobowym zarządcą i likwidatorem spółki, której upadłość ogłoszono w 1992 r. i która to spółka została wykreślona z rejestru spółek 7 lipca 2005 r. *Salvatore Manni* wniósł o nakazanie izbie handlowej w Lecce wykreślenia, anonimizacji lub zablokowania danych łączących jego nazwisko z upadłą spółką oraz zasądzenie odszkodowania za szkodę wizerunkową. 1 sierpnia 2011 r. *Tribunale di Lecce* (sąd w Lecce) uwzględnił żądanie *Manniego*. Jednakże *Corte suprema di cassazione* (trybunał kasacyjny), rozpatrując skargę kasacyjną wniesioną od tego wyroku przez izbę handlową, zawiesił postępowanie i skierował do TSUE pytania prejudycjalne.

[221] *Ibidem*.

członkowskie, czy zostaną wprowadzone do krajowego porządku prawnego regulacje ograniczające taki dostęp.

Na tle wskazanych powyżej wyroków wyraźnie widać, że Trybunał wyłączył prawo do bycia zapomnianym względem osób pełniących rolę w życiu publicznym z uwagi na uzasadniony interes internautów w dysponowaniu informacjami na temat tych osób. Ten sam argument został powtórzony w wyroku w sprawie *GC i in./CNIL*[222] dotyczącej

[222] Wyrok TSUE z dnia 24 września 2019 r. w sprawie C-136/17 *GC, AF, BH, ED przeciwko Commission nationale de I'informatique et des libertés (CNIL, krajowa komisja ds. informatyki i swobód).* W niniejszej sprawie GC, AF, BH i ED zwrócili się do spółki *Google* o usunięcie z wyników wyszukiwania – mającego za punkt wyjścia imię i nazwisko – linków kierujących do prowadzonych przez osoby trzecie stron internetowych. GC zażądała usunięcia linku, który odsyła do zamieszczonego 18 lutego 2011 r. pod pseudonimem na *YouTubie* satyrycznego fotomontażu przedstawiającego GC u boku burmistrza gminy, w którego biurze była ona kierownikiem i wyraźnie odwołującego się do łączącej ich intymnej relacji oraz wpływu tej relacji na jej własną karierę polityczną. Fotomontaż został zamieszczony w Internecie w związku z kampanią wyborczą w ramach wyborów kantonalnych, w których GC wówczas kandydowała. W dniu, w którym odmówiono uwzględnienia jej żądania usunięcia linku, GC ani nie była wybrana, ani nie kandydowała w wyborach lokalnych, nie pełniła też już funkcji kierownika biura burmistrza gminy.

AF zażądał usunięcia linków, które odsyłają do artykułu w dzienniku „Libération" z dnia 9 września 2008 r., zamieszczonego na stronie internetowej *Centre contre les manipulations mentales* (centrum zwalczania manipulacji mentalnej, CCMM, Francja), dotyczącego samobójstwa popełnionego przez wyznawcę kościoła scjentologicznego w grudniu 2006 r. AF wymieniono w tym artykule jako osobę odpowiedzialną za tworzenie i utrzymywanie wizerunku kościoła scjentologicznego, której to funkcji osoba ta już wówczas nie wykonywała. Ponadto autor wspomnianego artykułu stwierdza, że skontaktował się z AF w celu uzyskania jego wersji wydarzeń i relacjonuje zebrane przy tej okazji wypowiedzi.

BH zażądał usunięcia linków prowadzących do artykułów, głównie prasowych, dotyczących wszczętego w czerwcu 1995 r. dochodzenia w sprawie finansowania partii republikańskiej (PR), w ramach którego, wraz z kilkoma innymi biznesmenami i politykami, został postawiony w stan oskarżenia. Wszczęte przeciwko niemu postępowanie zostało umorzone w drodze postanowienia z dnia 26 lutego 2010 r. Większość spornych linków prowadzi do artykułów opublikowanych wtedy, gdy wszczęto śledztwo, i które, co za tym idzie, nie relacjonują wyniku postępowania.

ED zażądał usunięcia linków prowadzących do dwóch opublikowanych w „Nice-Matin" i „Le Figaro" artykułów relacjonujących rozprawę w sprawie karnej, na której został on skazany na karę siedmiu lat pozbawienia wolności oraz dodatkową karę dziesięciu lat dozoru kuratora za napaści na tle seksualnym na osoby małoletnie

przetwarzania danych osobowych przez operatorów wyszukiwarek internetowych. W niniejszej sprawie Trybunał zauważył jednak, 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”[223]. Dlatego też w razie wniesionego do operatora wyszukiwarki żądania usunięcia linku do strony internetowej zawierającej dane wrażliwe, „operator musi na podstawie wszystkich istotnych elementów danego przypadku i uwzględniając powagę ingerencji w […] prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych przysługujące osobie, której dane dotyczą, sprawdzić, czy […] umieszczenie linku do danej strony internetowej na wyświetlanej liście wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko osoby, której dane dotyczą, jest ściśle niezbędne do ochrony prawa do wolności informacji przysługującego internautom potencjalnie zainteresowanym uzyskaniem, dzięki takiemu wyszukiwaniu, dostępu do tej strony internetowej”[224]. Przetwarzanie przez operatora wyszukiwarki danych wrażliwych nie będzie jednak podstawą do realizacji żądania usunięcia linków, gdy stwierdzi on, że wskazanego rodzaju dane zostały podane do wiadomości publicznej

w wieku 15 lat. Jedna z tych kronik sądowych przytacza poza tym wiele intymnych szczegółów dotyczących ED, które zostały ujawnione w toku procesu.

Spółka *Google* nie uwzględniła powyższych żądań, dlatego też skarżący zwrócili się do CNIL ze skargami zmierzającymi do nakazania tej spółce usunięcia linków. CNIL umorzyła jednak postępowanie w sprawie tych skarg. Skarżący wnieśli zatem skargi do *Conseil d'État* (rady stanu, Francja) przeciwko wydanym przez CNIL decyzjom odmawiającym wezwania spółki *Google* do usunięcia linków. Z uwagi na liczne wątpliwości pojawiające się z wykładnią dyrektywy 95/46, *Conseil d'État* zawiesiła postępowanie i zwróciła się do TSUE z pytaniami prejudycjalnymi.

[223] *Ibidem.*

[224] *Ibidem.*

przez osobę, której dane dotyczą, oraz pod warunkiem, że przetwarzanie to spełnia wszystkie inne warunki zgodności przetwarzania z prawem ustanowione w dyrektywie 95/46 i o ile osobie, której dane dotyczą, nie przysługuje prawo sprzeciwu wobec takiego przetwarzania z ważnych i uzasadnionych przyczyn związanych z jej szczególną sytuacją[225]. Poza powyższymi elementami treści prawa do bycia zapomnianym, Trybunał uznał, że rozpatrywanie żądania usunięcia linków stron internetowych zawierających informacje dotyczące postępowania sądowego w sprawie karnej przeciwko osobie, której dane dotyczą, a które związane są z wcześniejszym etapem takiego postępowania i nie odpowiadają już aktualnej sytuacji, należy do operatora wyszukiwarki. Dokonanie przez operatora wyszukiwarki oceny, czy osoba, której dane dotyczą, uprawniona jest do tego, by rozpatrywane informacje nie były już aktualnie wiązane z jej imieniem i nazwiskiem za pomocą wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia to imię i nazwisko – wymaga wzięcia pod uwagę wszystkich okoliczności sprawy, takich jak w szczególności „charakter i waga rozpatrywanego przestępstwa (czynu zabronionego), przebieg i wynik tego postępowania, czas, jaki upłynął, rola odgrywana przez tę osobę w życiu publicznym i jej zachowanie w przeszłości, interes publiczny istniejący w chwili skierowania żądania, treść i formę publikacji oraz skutki tej publikacji dla wspomnianej osoby”[226]. Jeżeli na podstawie wszystkich okoliczności sprawy administrator stwierdzi nadrzędność praw podstawowych osoby, której dane dotyczą, wobec praw przysługujących potencjalnie zainteresowanym internautom, nastąpi realizacja przedmiotowego żądania. Jeżeli zaś administrator uzna, że umieszczenie danego linku jest niezbędne do pogodzenia podstawowych praw (tj. prawa do poszanowania życia prywatnego i ochrony danych osobowych) osoby, której dane dotyczą, z prawem do wolności informacji

[225] *Ibidem.*
[226] *Ibidem.*

przysługującym potencjalnie zainteresowanym internautom, zobowiązany jest „najpóźniej w momencie skierowania żądania usunięcia linków do uporządkowania listy wyników w taki sposób, aby wynikający z niej dla internauty ogólny obraz odzwierciedlał aktualną sytuację prawną, co wymaga w szczególności, aby linki do stron internetowych zawierających informacje na ten temat znajdowały się na pierwszym miejscu na tej liście”[227].

Patrząc przez pryzmat orzecznictwa TSUE, dotyczącego prawa do bycia zapomnianym, można dostrzec wyodrębnione przez Trybunał elementy treści tego prawa, które na kanwie danej sprawy były przez niego doprecyzowywane. Odnośnie do wyszukiwarek internetowych uznanych za administratorów, Trybunał w wyroku w sprawie *Google LLC/CNIL*[228] zmodyfikował stanowisko co do zakresu terytorialnego

[227] *Ibidem.*

[228] Wyrok TSUE z dnia 24 września 2019 r. w sprawie C-507/17 *Google LLC przeciwko Commission nationale de I'informatique et des libertés (CNIL).* Sprawa dotyczyła sporu między francuską komisją ds. informatyki i swobód a *Google*. 21 maja 2015 r. przewodnicząca CNIL wezwała *Google* do tego, aby w sytuacji, gdy spółka ta uwzględnia wniosek osoby fizycznej o usunięcie z listy wyników, wyświetlanej w następstwie wyszukiwania według jej imienia i nazwiska, linków prowadzących do stron internetowych, zastosowała owo usunięcie do wszystkich rozszerzeń nazwy domeny swej wyszukiwarki. Spółka *Google* nie zastosowała się do tego wezwania, ograniczając się do usunięcia tych linków jedynie z rezultatów wyświetlanych jako odpowiedź na wyszukiwania prowadzone z nazw domen odpowiadających wersjom jej wyszukiwarki w państwach członkowskich. CNIL uznał też za niewystarczającą złożoną przez spółkę *Google* po upływie terminu do usunięcia uchybienia dodatkową propozycję „geoblokowania”, polegającą na uniemożliwieniu dostępu z adresu IP (Internet Protocol) uważanego za zlokalizowany w państwie miejsca zamieszkania osoby, której ma przysługiwać to „prawo do usunięcia linków”, do spornych wyników uzyskanych w następstwie wyszukiwania według jej imienia i nazwiska, niezależnie od wersji wyszukiwarki, z której internauta skorzystał. Stwierdziwszy, że spółka *Google* nie zastosowała się do tego wezwania w wyznaczonym na to terminie, CNIL – uchwałą z dnia 10 marca 2016 r. – nałożył na tę spółkę podaną do publicznej wiadomości karę w wysokości 100 000 EUR. We wniesionej do *Conseil d'État* (rady stanu, Francja) skardze spółka *Google* żąda uchylenia tej uchwały. Z uwagi jednak na powstałe wątpliwości związane z wykładnią dyrektywy 95/46, *Conseil d'État* zawiesiła postępowanie i zwróciła się do TSUE z pytaniami prejudycjalnymi.

wniesionego – przez osobę, której dane dotyczą – żądania usunięcia danych. O ile w wyroku *Google Spain* stwierdził on, że usunięcie z listy wyników wyszukiwania dotyczy także pozaeuropejskich wyszukiwarek internetowych[229], to już kilka lat później ograniczył ten zasięg do wyszukiwarek państw członkowskich UE. Zaznaczył jednak, że prawo do usunięcia linków może obejmować wszystkie wersje danej wyszukiwarki, przy czym to „organ nadzorczy lub sąd państwa członkowskiego pozostaje właściwy w świetle krajowych standardów ochrony praw podstawowych do wyważenia przysługującego osobie, której dane dotyczą, prawa do poszanowania życia prywatnego i ochrony danych osobowych z prawem do wolności informacji, a po dokonaniu takiego wyważenia – do nakazania w stosownym wypadku operatorowi tej wyszukiwarki usunięcia linków w odniesieniu do wszystkich wersji owej wyszukiwarki"[230]. Ponadto, Trybunał zobowiązał operatorów wyszukiwarek internetowych do stosowania geoblokad, aby uniemożliwić internautom w państwach członkowskich dostęp do linków lub przynajmniej poważnie ich do nich zniechęcić – w wyniku wyszukiwania przeprowadzonego na bazie imienia i nazwiska – które wyświetlane są w wersjach tej wyszukiwarki poza Unią.

Z przedstawionych powyżej wyroków TSUE wynika, że prawo do bycia zapomnianym stało się przedmiotem szczegółowych analiz w kontekście żądań kierowanych do operatora wyszukiwarki internetowej przez osobę, której dane dotyczą. Na tle rozpatrywanych przez Trybunał spraw można dostrzec, że realizacja tego prawa uzależniona została od statusu osoby występującej z żądaniem. Organ ten uczynił bowiem „wyjątek w przypadku wniosków o usunięcie linków z listy wyników wyszukiwania od osób, których dane dotyczą, które odgry-

[229] Zob. M. Rojszczak, *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE*, „Prawo Mediów Elektronicznych" 2017, nr 3, s. 33 i n.

[230] Wyrok TSUE z dnia 24 września 2019 r. w sprawie C-507/17 *Google LLC przeciwko Commission nationale de I'informatique et des libertés (CNIL).*

wają rolę w życiu publicznym, gdy istnieje interes ogółu społeczeństwa w posiadaniu dostępu do tych informacji"[231]. Pewne wątpliwości co do skutecznej realizacji tego prawa pojawiły się na kanwie wskazanego wyżej wyroku *Google LLC/CNIL*, w którym Trybunał ograniczył zakres terytorialny żądania usunięcia danych z listy wyników wyszukiwania do wyszukiwarek internetowych państw członkowskich UE. Wynika to przede wszystkim z tego, że instytucja prawa do usunięcia linków w państwach trzecich nie jest znana lub stosowane jest inne podejście do tego prawa. Należy przy tym mieć na uwadze, że prawo do ochrony danych osobowych nie ma charakteru absolutnego. W związku z tym należy na nie spojrzeć przez pryzmat przypisanej mu funkcji społecznej i wyważyć względem innych praw podstawowych zgodnie z zasadą proporcjonalności[232]. Stąd też równowaga między pewnymi wartościami, a mianowicie prawem do poszanowania życia prywatnego i ochroną danych osobowych z jednej strony a wolnością informacji internautów z drugiej strony może w znacznym stopniu różnić się na całym świecie[233]. I chociaż prawodawca unijny „w art. 17 ust. 3 lit. a) rozporządzenia 2016/679, wyważył to prawo ze wspomnianą wolnością w odniesieniu do Unii […], to jednak należy stwierdzić, że w obecnym stanie rzeczy nie dokonał on takiego wyważenia w odniesieniu do zakresu usuwania linków poza Unią. W szczególności z treści art. 12 lit. b) i art. 14 akapit pierwszy lit. a) dyrektywy 95/46 ani z art. 17 rozporządzenia 2016/679 nie wynika wcale, że prawodaw-

[231] Wytyczne Grupy Roboczej Art. 29 ds. Ochrony Danych dotyczące wykonania wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie *Google Spain i Inc przeciwko Agencia Española De Protección De Datos (AEPR) i Mario Costeja Gonzâles* C-131/12, przyjęte w dniu 26 listopada 2014 r.

[232] Zob. na ten temat wyrok TSUE z dnia 9 listopada 2010 r. w sprawie C-92/09 i C-93/09 *Volker und Markus Schecke i Eifert.*

[233] Wyrok TSUE z dnia 24 września 2019 r. w sprawie C-507/17 *Google LLC przeciwko Commission nationale de I'informatique et des libertés (CNIL).*

ca Unii, dla zapewnienia osiągnięcia celu niniejszego wyroku[234], postanowił nadać ustanowionym w tych przepisach uprawnieniom zakres, który wykracza poza terytorium państw członkowskich, ani że zamierzał on nałożyć na podmiot, który, podobnie jak Google, jest objęty zakresem stosowania tej dyrektywy lub tego rozporządzenia, obowiązek usunięcia linków odnoszący się również do krajowych wersji jego wyszukiwarki, które nie odpowiadają państwom członkowskim"[235].

Zaaprobowany przez TSUE mechanizm geoblokady spotkał się z głosami krytyki[236], bowiem jego obejście możliwe jest poprzez VPN (*Virtual Private Network*). Narzędzie to umożliwia dostęp do globalnego Internetu, ukrywając lokalizację użytkownika, co oznacza, że zastosowana względem państw członkowskich UE technika geoblokowania wyszukiwania jest fikcją. Należy jednak zaznaczyć, że pomimo wprowadzonych ograniczeń terytorialnych, Trybunał nie wyłączył stosowania prawa do bycia zapomnianym w wymiarze globalnym. Jego realizację w tak szerokim ujęcia uzależnił od wyważenia przez właściwe

[234] Tym celem jest zapewnienie wysokiego poziomu ochrony danych osobowych w całej Unii.

[235] Wyrok TSUE z dnia 24 września 2019 r. w sprawie C-507/17 *Google LLC przeciwko Commission nationale de I'informatique et des libertés (CNIL).*

[236] „Takie podejście to przejaw hipokryzji. Jeśli uznajemy, że jakieś dane powinny zniknąć, to powinny zniknąć z całego Internetu. Nie ma bowiem kilku Internetów, tylko jeden. Zobowiązanie zaś do stosowania geoblokad jest fikcją. Aprobujemy w ten sposób sytuację, że gdy ktoś jest wystarczająco cwany i potrafi je obejść, poprzez VPN, to ma dostęp do informacji, które uznano za naruszające prawo – ocenia Maciej Gawroński.

W praktyce oznacza to, że w UE jakiekolwiek ograniczenia geograficzne wyszukiwania nie będą skuteczne. I nie jest ważne, ile osób rzeczywiście korzysta z VPN, ważne jest to, że geoblokadę każdy może bez problemów obejść […]. W sprawie Google Spain trybunał uznał, że operator wyszukiwarki podlega prawu Unii Europejskiej jako administrator danych**.** Teraz zaś doszedł do wniosku, że nie ciąży na nim obowiązek usunięcia linków w odniesieniu do wszystkich wersji wyszukiwarki. Tymczasem zarówno obowiązująca wcześniej dyrektywa 95/46, jak i dzisiaj RODO nie różnicują poziomu ochrony danych osobowych w zależności od kraju, w jakim dane się przetwarza. Jeżeli jakiś podmiot podlega unijnemu prawu ochrony danych, to ma je stosować i już" – podkreśla Paweł Litwiński, https://forsal.pl/artykuly/1431643,niewidocznosc-w-internecie-wyrok-tsue-ws-google.html [dostęp: 10.10.2021].

organy krajowe „przysługującego osobie, której dane dotyczą, prawa do poszanowania życia prywatnego i ochrony danych osobowych z prawem do wolności informacji”[237].

Mając powyższe na względzie, należy uznać, że usankcjonowane przez TSUE prawo do bycia zapomnianym w kontekście jego realizacji przez operatorów wyszukiwarek internetowych nie gwarantuje osobie, której dane dotyczą, całkowitego usunięcia linków z listy wyszukiwania, to jednak wyłącza możliwość dotarcia do informacji na temat danej osoby przy użyciu imienia i nazwiska jako kryterium wyszukiwania, o ile ma zastosowanie do wszystkich wersji wyszukiwarki internetowej. Wprowadzony w ramach niniejszego wyroku mechanizm geoblokady spowodował odejście od uniwersalnej do regionalnej opcji prawa do bycia zapomnianym[238]. Zwolennicy tego rozwiązania argumentują to tym, że „pomiędzy zbyt daleko idącym terytorialnym zastosowaniem do wszystkich domen a zastosowaniem tylko do domen UE pozostaje bardziej rozsądna opcja. Geofiltrowanie wydaje się najbardziej odpowiednim podejściem umożliwiającym skuteczną ochronę prawa do prywatności przy jednoczesnym poszanowaniu zasady terytorialności”[239]. Wprowadzone rozwiązanie (geoblokada), jak już wyżej wspomnieliśmy, można skutecznie obejść, a to oznacza, że skuteczność prawa do bycia zapomnianym staje się ograniczona. Skoro efektem prawa do bycia zapomnianym nie jest całkowite usunięcie linku z wyszukiwarki, a zatem dostęp do informacji na temat danej osoby jest wciąż możliwy, tyle że opiera się na innych hasłach wyszukiwania

[237] Wyrok TSUE z dnia 24 września 2019 r. w sprawie C-507/17 *Google LLC przeciwko Commission nationale de I'informatique et des libertés (CNIL).*

[238] Zob. na ten temat Y. Padova, *Is the right to be forgotten a universal, regional, or 'glocal' right?,* “International Data Privacy Law” 2019, Vol. 9, No. 1.

[239] A.F. Rivero, *Right to be forgotten in the European Court of Justice Google Spain Case: The right balance of privacy rights, procedurę, and extraterritoriality,* “European Union Law Working Papers” 2017, No. 19, Stanford-Vienna Transatlantic Technology Law Forum, s. 44.

niż imię i nazwisko, uważamy, że realizacja prawa do bycia zapomnianym powinna mieć zasięg uniwersalny.

2. Identyfikacja zakresu i charakteru prawa do bycia zapomnianym w ocenie krajowego organu ochrony oraz orzecznictwie sądów w Polsce

Weryfikacja zasadności realizacji prawa do bycia zapomnianym w dotychczasowym orzecznictwie sądów polskich nie jest zbyt rozbudowana. Z jednej strony, jak się wydaje, jest to skutek niewielkiej jeszcze liczby żądań, które są dochodzone przez uprawnione osoby, z drugiej zaś szeroko zdefiniowanego zakresu przesłanek, które wyłączają możliwość skutecznej jego realizacji. Już dawno zauważono bowiem, że „[…] prawo to może być zrealizowane tylko tam, gdzie brak jest jakiejkolwiek przesłanki uprawniającej administratora lub podmiot przetwarzający do przetwarzania danych. Artykuł 6 RODO zawiera jednak bardzo pojemną przesłankę prawnie uzasadnionego celu, która może okazać się tutaj furtką, legalizując duży zakres przetwarzanych danych, np. gdy jest to konieczne do ochrony przed przyszłymi roszczeniami powstałymi po rozwiązaniu umowy, w tym umowy zawieranej poprzez akceptację regulaminu świadczenia usług drogą elektroniczną”[240]. Choć więc samo potoczne pojmowanie „prawa do bycia zapomnianym” brzmi obiecująco i „zdaje się” zapewniać konkretnej osobie możliwość skutecznego wyeliminowania (ograniczenia) z obrotu danych jej dotyczących i funkcjonujących już w informatycznej przestrzeni publicznej[241], to rozumienie takie można uznać jedynie za

[240] 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*, P. Litwiński (red.), Warszawa 2018, s. 410.

[241] Informacyjna przestrzeń publiczna obejmuje swym zakresem określonego rodzaju „obszar”, identyfikowany ze wszystkimi istniejącymi w aktualnej rzeczywistości mechanizmami, płaszczyznami i platformami służącymi pozyskiwaniu, przekazy-

uproszczoną formułę, która tylko w pewien sposób zdaje się służyć sprecyzowaniu rzeczywistej treści i istoty tego prawa i to z wielu względów.

Istotne problemy wiążą się ze zdefiniowaniem zobowiązanego do usunięcia danych. Dotychczasowa praktyka dostarcza dowodów na możliwość różnej interpretacji rozstrzygnięć TSUE, szczególnie tego, które za administratora uznaje operatora wyszukiwarki.

Podobna sytuacja dotyczy interpretacji przesłanek wyłączających możliwość skutecznego powołania się na prawo do bycia zapomnianym. Dobrym przykładem obrazującym różnicę między „pożądanym" pojmowaniem treści prawa do bycia zapomnianym a jego faktycznym charakterem jest ocena praktyki publikacji prasowych dotyczących różnych osób, tak tych pełniących funkcje publiczne[242], jak i osób prywatnych niezwiązanych z funkcjonowaniem szeroko rozumianej sfery publicznej[243], a także wykorzystywania w praktyce funkcjonowania

waniu i utrwalaniu informacji. Obejmuje więc swym zakresem klasyczne postaci i środki pozyskiwania, gromadzenia, przetwarzania i przekazu informacji, jak również te, które wykorzystują nowoczesne technologie informatyczne i informacyjne.

[242] Jak wskazuje się w orzecznictwie, pełnienie funkcji publicznej niesie ze sobą określone konsekwencje prawne, a w przypadku ochrony prywatności i danych osobowych pewne ograniczenia tej ochrony. Z jednej strony informacje o takiej osobie, dotycząc jej aktywności zawodowej, z istoty swej nie tylko będą jawne, ale w szerokim zakresie dotyczyć mogą różnego rodzaju informacji wkraczających w sferę jej prywatności. Podnosi się jednocześnie, że „zaprzestanie pełnienia funkcji publicznej nie oznacza, że informacje z okresu, gdy funkcja ta była pełniona, przestają podlegać udostępnieniu z ograniczeniem prywatności jednostki, bowiem wciąż będą one udostępniane osobom zainteresowanym w odniesieniu do okresu pełnienia funkcji" – por. wyrok Naczelnego Sądu Administracyjnego z dnia 8 lipca 2015 r., I OSK 1530/14.

[243] Np. por. decyzja GIODO z dnia 17 kwietnia 2017 r., DOLiS/DEC-465/17 z odwołaniem się do wyroku WSA w Gorzowie Wielkopolskim z 6 maja 2010 r., II SAB/Go 10/2010, w którym podkreślono, iż: „Cechą prawa do prywatności jest to, że ochroną tą objęta jest dziedzina życia osobistego (prywatnego), rodzinnego i towarzyskiego człowieka. Ochrona ta nie obejmuje działalności publicznej osoby ani też sfery działań i zachowań, które ogólnie są pojmowane jako osobiste lub prywatne, jeżeli działania te lub zachowania wiążą się ściśle z działalnością publiczną." oraz wyroku Trybunału Konstytucyjnego z dnia 20 marca 2006 r., K. 17/2005.

konkretnych administratorów danych pozyskiwanych z rejestrów i informatorów publicznych[244].

Wreszcie warto też zwrócić uwagę na kwestie i zakres oceny przez krajowy organ ochrony danych wywiązania się przez administratora z wdrożenia odpowiednich środków technicznych zapewniających możliwość skorzystania przez uprawnionego z prawa do bycia zapomnianym.

2.1. Identyfikacja zobowiązanego do niezwłocznego usunięcia danych

Mając na względzie fakt, że to właśnie administrator danych[245], a nie inny podmiot, zobligowany zostaje do realizacji żądania osoby kierowanego na podstawie art. 17 ust. 1 i 2 RODO, szereg problemów związanych było (i jest) z ustaleniem, kto (jaki podmiot) w konkretnej sytuacji faktycznej jest do tego zobowiązany.

Ciekawe sprawy dotyczyły przede wszystkim ustalenia tego, czy prawidłowy jest adresat żądania zaprzestania przetwarzania danych osobowych w wynikach wyszukiwania w Internecie. Problem koncen-

[244] Jednocześnie warto zwrócić uwagę, że wiele przepisów nie określa, przez jak długi okres w celach archiwizacyjnych i związanych z dostępem do informacji publicznej mogą być przechowywane dane osoby, która pełniła w przeszłości funkcję publiczną. Nie zwalnia to administratorów od realizacji obowiązku wskazanego w art. 30 ust. 1 lit. f) RODO, co pozwala na odmowę usunięcia danych, z uwagi na potrzebę ich dalszego przetwarzania. W każdym jednak przypadku usunięte powinny zostać dane, które nie służą takim celom lub upłynął czas, przez jaki administrator może lub musi przechowywać określone dane (np. 6 lat w stosunku do oświadczeń majątkowych upublicznianych w BIP), por. decyzja PUODO z dnia 18 października 2019 r., ZSPU.421.3.2019.

[245] Istotne jest więc ustalenie, czy posiada on środki prawne, techniczne oraz organizacyjne, aby zaprzestać przetwarzania danych osobowych. Istotne staje się ustalenie czy adresat żądania posiada środki techniczne i/lub organizacyjne do spełnienia żądania oraz wykonania np. decyzji nakazującej usunięcie danych osobowych z wyszukiwarki internetowej. Na temat elementów definiujących ADO zob.: K. Wygoda, *Administrator danych w administracji publicznej*, [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018, s. 15 i n.

trował się na zweryfikowaniu tego, czy zarówno żądanie, jak i rozstrzygnięcie krajowego organu ochrony skierowane były do administratora danych, a nie innego podmiotu, który statusu takiego nie posiadał.

W kilku sprawach GIODO uznał spółkę zależną, posiadającą odrębną osobowość prawną i wykonującą działalność gospodarczą na terytorium Rzeczypospolitej Polskiej za podmiot ustanowiony przez operatora wyszukiwarki internetowej, a w związku z tym właściwy do uznania go za odpowiedniego adresata żądania zaprzestania przetwarzania danych[246]. Pozwoliło mu ta na potwierdzenie, iż w sprawach dotyczących skarg osób fizycznych zamieszkujących na terytorium Polski na odmowę usunięcia ich danych osobowych udostępnionych w wynikach wyszukiwania w wyszukiwarce internetowej będzie spółka zależna, której celem jest promocja i sprzedaż powierzchni reklamowych, a co jest nierozerwalnie związane z funkcjonowaniem samej wyszukiwarki[247]. Jednocześnie podkreślona – w ślad za orzecznictwem TSUE – została klasyczna ścieżka postępowania osoby, której dane dotyczą w zakresie realizacji przysługujących jej praw. Przyjmują one postać:

– skierowania wniosku o zaprzestanie przetwarzania danych osobowych do operatora wyszukiwarki internetowej[248];

[246] Sprawy takie miały miejsce jeszcze w okresie obowiązywania art. 18 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922).

[247] GIODO uznał, że w badanych sprawach „przetwarzanie danych osobowych ma miejsce w ramach działalności gospodarczej prowadzonej przez zakład administratora danych odpowiedzialnego za to przetwarzanie na terytorium danego państwa w rozumieniu tego przepisu, jeśli operator wyszukiwarki internetowej ustanawia w danym państwie członkowskim oddział lub spółkę zależną, których celem jest promocja i sprzedaż powierzchni reklamowych oferowanych za pośrednictwem tej wyszukiwarki, a działalność tego oddziału lub tej spółki zależnej jest skierowana do osób zamieszkujących to państwo". Oceniając „przedmiot, sposób oraz formę działalności gospodarczej" konkretnego podmiotu „(tj. promowanie usług reklamowych wśród podmiotów m.in. z terytorium Rzeczypospolitej Polskiej, które mogą być realizowane z wykorzystaniem wyszukiwarki internetowej" uznał go „za podmiot ustanowiony przez operatora" przedmiotowej wyszukiwarki internetowej.

[248] „Zgodnie z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Espanola de Proteccion de Datos*

– w przypadku braku właściwej reakcji po stronie operatora, wystąpienie do krajowego organu ds. ochrony danych osobowych.

Krajowy organ ochrony jest uprawniony do nakazania usunięcia danych osobowych jedynie wtedy, gdy przetwarzanie danych w wynikach wyszukiwania nie znajduje oparcia w obowiązujących przepisach prawa i dokonywane jest z naruszeniem obowiązujących przepisów[249].

W orzecznictwie sądowym podkreślono, że krajowy organ ochrony zobligowany jest do wnikliwej oceny, który z podmiotów rzeczywiście decyduje o celach i środkach przetwarzania danych osobowych, a zatem „który podmiot ma kontrolę nad tym, jakie dane wymienionego przetwarzane są (we wskazanym przez niego zakresie) w wyszukiwarce internetowej […] i ma możliwość techniczną i organizacyjną usuwania danych osobowych wnioskodawcy (zablokowania wyników

i Mario Costeja Gonzalez (C-131/12), uznano, iż operatorzy wyszukiwarek internetowych przetwarzają dane osobowe jako administratorzy danych. W związku z powyższym, w celu umożliwienia wyegzekwowania praw osób, których dane dotyczą, żądania usunięcia ich danych osobowych z wyświetlanej listy wyników wyszukiwania, powinny być kierowane do operatorów wyszukiwarek internetowych, a nie do właścicieli stron internetowych. W związku z powyższym jeżeli Skarżący kwestionuje przetwarzanie jego danych osobowych w wyszukiwarce internetowej www.[...].com, winien wystąpić do operatora ww. wyszukiwarki z wnioskiem o zablokowanie wyników wyszukiwania wyszukiwarki B. i usunięcie z listy wyników wyszukiwana określonych linków do informacji naruszających jego prawa" – decyzja GIODO z dnia 22 grudnia 2015 r., DOLiS/DEC-971/15/107373,107392.

[249] Przy tej okazji ciekawa była również kwestia badania istnienia w sprawie prawnie usprawiedliwionego celu przetwarzania danych osobowych. GIODO podkreślił, że fakt uniemożliwienia uzyskania dostępu do danych osobowych wcześniej upublicznionych w BIP (dokumenty zawierające dane osobowe konkretnej osoby ujęto w archiwalnych zasobach BIP, do których nie miały dostępu osoby korzystające z teleinformatora), świadczy o tym, że podjęto działania zmierzające do uniemożliwienia osobom trzecim, zapoznania się z treścią określonych dokumentów. W ocenie GIODO, oznaczało to, że „dalsze przetwarzanie danych osobowych skarżącego w wynikach wyszukiwania […] jest obecnie nieuzasadnione, ponieważ prawnie usprawiedliwiony cel przetwarzania danych osobowych wygasł w chwili podjęcia przez Starostę działań skutkujących usunięciem danych osobowych Skarżącego z BIP Powiatu […]", zob.: wyrok WSA w Warszawie z dnia 29 sierpnia 2017, II SA/Wa 2015/16.

wyszukiwania) […]"[250]. W sytuacji, w której badanie takie nie zostało wyczerpująco przeprowadzone, wydawanie decyzji przez krajowy organ ochrony może być przedwczesne[251].

Mając na względzie, że od 25 maja 2018 r. stosujemy już bezpośrednio postanowienia RODO, warto zwrócić jednak uwagę na pewnego rodzaju zmianę podejścia ustawodawcy unijnego do sposobu definiowania pojęcia administratora[252]. Przede wszystkim trzeba zauważyć, że za wystarczający warunek wpływający na przyznanie statusu administratora uznano zatem wspólne z innymi (współadministratorami) ustalanie celów i sposobów przetwarzania. W tej sytuacji, jak słusznie zauważa K. Witkowska-Nowakowska[253], należy brać pod uwagę konsekwencje wynikające z art. 26 RODO[254], który obejmuje zjawisko współ-

[250] Zob.: wyrok WSA w Warszawie z dnia 29 sierpnia 2017, II SA/Wa 2015/16; wyrok WSA w Warszawie z dnia 16 stycznia 2018 r., II SA/Wa 503/17.

[251] W istotnym zakresie rozstrzygnięcie takie nawiązywało do wcześniejszych por.: wyrok WSA w Warszawie z dnia 29 stycznia 2014 r., II SA/Wa 1819/13; wyrok NSA z dnia 21 kwietnia 2015 r., I OSK 1480/14.

[252] Warto też podkreślić, że już wcześniej GIODO podkreślał, iż sam fakt dostarczania narzędzi pozwalających na dostęp do danych osobowych konkretnej osoby „upublicznionych w serwisie internetowym prowadzonym przez podmiot trzeci, nie jest wystarczający do stwierdzenia, że ma ona decydujący wpływ na cele i środki przetwarzania tych danych. W przeciwnym wypadku za administratorów danych osobowych dostępnych w Internecie należałoby uznać także producentów przeglądarek internetowych, czy czytników RSS (oprogramowania komputerowego umożliwiającego czytanie wiadomości publikowanych w kanałach informacyjnych dostępnych w Internecie)" – decyzja GIODO z dnia 12 listopada 2012 r., DOLiS/DEC – 1180/12/72653,72655.

[253] Zob. szerzej K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 215-217; konieczność łącznego odczytywania definicji administratora i art. 26 RODO wskazują również P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych…*, s. 225.

[254] Art. 26 Współadministratorzy 1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkow-

administrowania, zwłaszcza „[...] że ten współudział przy decydowaniu może przybierać różne formy, w tym formę bardzo ścisłej współpracy lub wprost przeciwnie – jedynie częściowego wspólnego działania. Może zachodzić zatem wówczas, gdy administratorzy wspólnie określają i dzielą wszystkie cele oraz sposoby przetwarzania w równych proporcjach, jak i wtedy, kiedy podział jest niesymetryczny”[255].

Oznacza to zatem, że badanie względnej samodzielności administratora wymaga szczegółowego ustalania zagadnień technicznych i organizacyjnych wiążących się z procesem przetwarzania – co istotne, w spektrum tego działania mieści się też podjęcie decyzji o powierzeniu przetwarzania danych osobowych, gdyż trudno przyjąć założenie, że RODO wymusza, by wszystkie czynności administrator musiał wykonywać samodzielnie. W praktyce rozstrzygnięcie o sposobie przetwarzania danych może zatem sprowadzać się do decyzji o powierzeniu przetwarzania danych zewnętrznemu podmiotowi oraz o tym, że podmiot ten (podmiot przetwarzający) może korzystać z podwykonawcy[256].

skiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

2. Uzgodnienia, o których mowa w ust. 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.

[255] K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 215.

[256] Zbieżne poglądy w tej kwestii wyraża np. M. Sakowska-Baryła, która zauważa że administrator „[…] nie musi bowiem fizycznie posiadać danych, dla których ustala cele i sposoby przetwarzania ani wykonywać samodzielnie wszystkich czynności potrzebnych dla osiągnięcia konkretnego celu; najistotniejsze jest to, że to podejmuje decyzje w procesie przetwarzania danych”, M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 103.

2.2. Publikacje prasowe

W jednej z rozpatrywanych spraw chodziło o usunięcie zamieszczonych w Internecie, na stronie czasopisma, danych osobowych dotyczących stanu zdrowia, leczenia oraz okresu zwolnienia lekarskiego konkretnej, imiennie wskazanej, osoby. Uprawniony, występując do krajowego organu ochrony, zażądał wydania rozstrzygnięcia, w którym nakazano by wydawcy zaprzestania łamania prawa i ujawniania jego danych wrażliwych, a także nałożenia na niego kary pieniężnej.

Prezes Urzędu Ochrony Danych Osobowych rozstrzygnięcia takiego nie wydał, powołując się na obowiązujące przepisy RODO i ustawy o ochronie danych osobowych[257], wskazując jednocześnie właściwą drogę prawną, która w zakresie dochodzenia gwarantowanych praw przysługuje zainteresowanemu[258].

Wyłączenie zasadności powoływania się na treść art. 17 RODO uzasadnione zostało przez odwołanie się wprost do jednego z jego postanowień, zgodnie z którym przetwarzanie danych osobowych jest niezbędne do korzystania z praw do wolności wypowiedzi i informacji przez podmioty uprawnione (ust. 3 lit a)[259]. Organ ochrony uznał jednocześnie, że redaktor gazety czy programu telewizyjnego taki właśnie

[257] Prezes UODO stwierdził, że jeżeli do działalności polegającej m.in. na publikowaniu materiałów prasowych nie stosuje się przepisów RODO wskazanych w art. 2 ust. 1 ustawy o ochronie danych osobowych z 2018 r. w związku z art. 85 ust. 2 RODO. Podkreślił jednocześnie, że m.in. art. 6 stanowiącego o przesłankach legalności przetwarzania danych osobowych, to Prezes UODO nie ma podstaw prawnych do badania tych przesłanek w celu spełnienia żądania skarżącego w zakresie nakazania wydawcy [...] usunięcia jego danych osobowych.

[258] Wskazał, że w zakresie nakazania wydawcy usunięcia danych osobowych uprawnionego ujętych w publikacji prasowej odpowiednie przepisy dotyczące ochrony prywatności oraz dóbr osobistych zdefiniowane zostały w postanowieniach ustawy – Prawo prasowe (art. 37) i Kodeksu cywilnego oraz ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 1360 z późn. zm.).

[259] Na temat wyjątku dziennikarskiego zob.: P. Litwiński, *Komentarz do art. 2*, [w:] P. Litwiński (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 13-17; K. Kozieł, *Komentarz do art. 2*, [w:] M. Gomulewicz, K. Kozieł, P. Kozik (red.), *Ustawa o ochronie danych osobowych. Przepisy wprowadzające Rozporzą-*

charakter „uprawnionego podmiotu" posiadają, a w konsekwencji o ewentualnym naruszeniu przysługujących konkretnej osobie praw i dóbr osobistych powinien decydować nie krajowy organ ochrony danych, ale sąd powszechny, w postępowaniu opartym na przepisach procedury cywilnej[260].

W szerszym ujęciu stanowisko PUODO uzasadnione zostało przez odwołanie się do treści art. 85 RODO[261] i art. 2 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. W przepisach ustawy konkretyzuje się, że do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów praso-

dzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Komentarz, Warszawa 2018, s. 52-53.

[260] Prezes UODO stwierdził, że zgodnie z treścią art. 17 ust. 3 k.p.c. do właściwości sądów okręgowych należą sprawy o roszczenia wynikające z prawa prasowego. W konsekwencji powyższego, w ocenie PUODO w niniejszej sprawie zaistniała uzasadniona przyczyna odmowy wszczęcia postępowania, o której mowa w art. 61 a § 1 k.p.a.

[261] Zgodnie z motywem 153 preambuły RODO „Prawo państw członkowskich powinno godzić przepisy regulujące wolność wypowiedzi i informacji, w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia. Przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, przewidzianymi w art. 11 Karty praw podstawowych. Powinno mieć to zastosowanie w szczególności do przetwarzania danych osobowych w dziedzinie audiowizualnej oraz w archiwach i bibliotekach prasowych. Państwa członkowskie powinny więc przyjąć akty prawne określające odstępstwa i wyjątki niezbędne do zapewnienia równowagi między tymi prawami podstawowymi. Państwa członkowskie powinny przyjąć takie odstępstwa i wyjątki w odniesieniu do zasad ogólnych, praw przysługujących osobie, której dane dotyczą, administratora i podmiotu przetwarzającego, przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, niezależnych organów nadzorczych, współpracy i spójności oraz szczególnych sytuacji przetwarzania danych. Jeżeli odstępstwa i wyjątki różnią się zależnie od państwa członkowskiego, zastosowanie powinno mieć prawo państwa członkowskiego, któremu podlega administrator. Aby uwzględnić, jak ważna dla każdego demokratycznego społeczeństwa jest wolność wypowiedzi, pojęcia dotyczące tej wolności, takie jak dziennikarstwo, należy interpretować szeroko".

wych w rozumieniu ustawy – Prawo prasowe, a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5–9, art. 11, art. 13–16, art. 18–22, art. 27, art. 28 ust. 2–10 oraz art. 30 RODO.

Jak podkreślił to sąd, który rozpatrywał skargę od rozstrzygnięcia PUODO – w żadnym razie wyłączenie takie nie oznacza oczywiście, „[…] że dziennikarze, pisarze i artyści nie mają obowiązku chronić osoby, których dane przetwarzają, a jedynie, że ochrona została ukształtowana inaczej. Działalność prasowa podlega regulacji prawa prasowego i tam ukształtowane są odmienne konstrukcje mające służyć ochronie osób, których dane są przetwarzane […]. Zdaniem Sądu, nie ulega wątpliwości, że uwzględnienie w art. 2 ust. 1 ustawy o ochronie danych osobowych tzw. «wyjątku dziennikarskiego» (czy też tzw. «klauzuli prasowej») stanowi realizację art. 85 RODO regulującego przetwarzanie danych osobowych w kontekście wolność wypowiedzi i informacji”[262].

Zakres zdefiniowanego przez ustawodawcę krajowego ograniczenia jest więc szeroki, ale nie obejmuje prawa określonego w art. 17 RODO, w którym jednak, jak wskazaliśmy wyżej, podkreśla się, że istnieje skuteczna możliwość powołania się na jego wyłączenie w zakresie, w jakim przetwarzanie jest niezbędne do korzystania z praw do wolności wypowiedzi i informacji przez podmioty uprawnione (ust. 3 lit a). Pozwoliło to sądowi na stwierdzenie (w kontekście pozytywnego zweryfikowania strony podmiotowej i przedmiotowej uprawnionej do powołania się na treść art. 17 ust. 3 lit. a), że podstawa oraz zasady przetwarzania danych osobowych przez dziennikarzy w ramach działalności dziennikarskiej (publikacji materiału prasowego) wynikają z ustawy – Prawo prasowe[263]. Oczywiście powołany został również art. 58 ust. 2 RODO ze wskazaniem na brak możliwości merytorycznej oceny przez PUODO

[262] Wyrok WSA w Warszawie z dnia 23 października 2020 r., II SA/Wa 2581/19.
[263] *Ibidem.*

udostępnienia danych osobowych żądającego na łamach czasopisma w oparciu o obowiązujące przepisy o ochronie danych osobowych, i w konsekwencji brak możliwości wykorzystania uprawnień, pozwalających na przywrócenie stanu zgodnego z prawem.

Warto jednak przy tej okazji zauważyć, że interpretacja treści art. 7 ust. 1[264] i 2 ustawy – Prawo prasowe nie jest prosta. Zauważa się, że „[…] ustawodawca definiując w tym przepisie prasę zdawał sobie sprawę z faktu, że postęp techniczny w zakresie form tworzenia i przekazywania publikacji periodycznych jest niezwykle szybki, a możliwości techniczne, w jakich prasa będzie mogła powstawać, trudne do przewidzenia i odgadnięcia"[265]. W konsekwencji przyjmuje się, że „prasą są także wszelkie istniejące i powstające w wyniku postępu technicznego środki masowego przekazywania"[266]. W takim ujęciu „przekaz za pośrednictwem Internetu, jeżeli spełnia wymogi określone w treści art. 7 ust. 2 pkt 1 pr. pr., jest prasą, a interwał czasowy, w jakim się pojawia, determinuje to, czy jest to dziennik w rozumieniu art. 7 ust. 2 pkt 2 pr. pr., czy też czasopismo w rozumieniu art. 7 ust. 2 pkt 2 pr. pr. […]. W tej sytuacji jest rzeczą bezsporną, że dzienniki i czasopisma przez to, że ukazują się w formie przekazu internetowego nie tracą znamion tytułu prasowego, i to zarówno wówczas, gdy przekaz internetowy towarzyszy przekazowi utrwalonemu na papierze, drukowanemu, stanowiąc inną, elektroniczną jego postać w systemie *on line*, jak

[264] Zgodnie z art. 7 ust. 1 ustawy – Prawo prasowe, prasa oznacza publikacje periodyczne, które nie tworzą zamkniętej, jednorodnej całości, ukazujące się nie rzadziej niż raz do roku, opatrzone stałym tytułem albo nazwą, numerem bieżącym i datą, a w szczególności: dzienniki i czasopisma, serwisy agencyjne, stałe przekazy teleksowe, biuletyny, programy radiowe i telewizyjne oraz kroniki filmowe; prasą są także wszelkie istniejące i powstające w wyniku postępu technicznego środki masowego przekazywania, w tym także rozgłośnie oraz tele- i radiowęzły zakładowe, upowszechniające publikacje periodyczne za pomocą druku, wizji, fonii lub innej techniki rozpowszechniania; prasa obejmuje również zespoły ludzi i poszczególne osoby zajmujące się działalnością dziennikarską.

[265] Postanowienie SN z dnia 15 grudnia 2010 r., III KK 250/10.

[266] *Ibidem.*

i wówczas, gdy przekaz istnieje tylko w formie elektronicznej w Internecie, ale ukazuje się tylko periodycznie, spełniając wymogi, o których mowa w art. 7 ust. 2 pr. pr."[267].

Przy takim ujęciu, nawet jeżeli uwzględnimy istotne kwestie badania częstotliwości i charakteru prowadzonej przez konkretny podmiot działalności (periodyczność, stały tytuł)[268] pojawiać się będzie coraz więcej kwestii spornych w odniesieniu do definiowania różnic między pojęciami: prasy (wydawaniem dziennika lub czasopisma) i dziennikarza[269] a jednostką realizującą swoje konstytucyjnie (i ustawowo) gwarantowane uprawnienia w sferze wolności wypowiedzi, a także pozyskiwania i rozpowszechniania informacji. Obecnie bowiem obok pojęcia „prasa, dziennik, czasopismo" funkcjonuje wiele innych, zasadniczo równoważnych względem prasy pojęć, takich jak:

[267] *Ibidem.* Warto też zauważyć, że: W rozumieniu art. 7 ust. 2 pkt 1 ustawy Prawo prasowe „obejmuje również zespoły ludzi i poszczególne osoby zajmujące się działalnością dziennikarską, zaś dziennikarzem jest osoba zajmująca się redagowaniem, tworzeniem lub przygotowywaniem materiałów prasowych, pozostająca w stosunku pracy z redakcją albo zajmująca się taką działalnością na rzecz i z upoważnienia redakcji" – por. wyrok NSA z dnia 4 lutego 2016 r., I OSK 881/15.

[268] W wyroku SN z dnia 28 października 2016 r., I CSK 695/15, wskazano, że: „[…] podstawowe znaczenie w definicji prasy mają jednak periodyczność oraz to, aby publikacje zamieszczane w środkach masowego przekazywania nie tworzyły jednorodnej, zamkniętej całości i przez to nie miały charakteru okazjonalnego. Jeżeli publikacje zamieszczone w Internecie spełniają zasadnicze kryteria prasy, ale nie wskazują jedynie bieżącego numeru, nie tracą przez to statusu prasy. Definicja prasy jest do tego stopnia otwarta, że pozwala nią objąć także te nowe środki masowego przekazywania, którym ze względu na swoją specyfikę, w szczególności możliwość ich ciągłej aktualizacji, trudno byłoby spełnić to kryterium formalne. Odmienna ocena prowadzi do tego, że kryteriów prasy nie spełniałyby nawet publikacje na stronach internetowych będące wiernymi kopiami publikacji w formie drukowanej, a więc spełniających wszystkie kryteria prasy, które następnie, do czasu zamieszczenia kolejnego numeru (kopii wersji drukowanych), ulegałaby zmianie na skutek ich aktualizacji".

[269] Na temat pojęć użytych w przepisach prawa prasowego zob. szerzej: J. Sieńczyło-Chlabicz, M. Nowikowska, Z. Zawadzka, *Rozdział I*, [w:] *Prawo mediów*, red. J. Sieńczyło-Chlabicz, Warszawa 2015, s. 20 i n.; M. Brzozowska-Pasieka, M. Olszyński, J. Pasieka, *Prawo prasowe. Komentarz*, Warszawa 2013, s. 81 i n.; E. Ferenc-Szydełko, *Prawo prasowe. Komentarz*, Warszawa 2010, s. 77 i n.; J. Sobczak, *Prawo prasowe. Komentarz (komentarz do art. 7)*, System informacji prawnej LEX 2008.

portale plotkarskie, prasa obywatelska, moderowane forum internetowe czy nawet blogi[270]. Również pojęcie dziennikarza identyfikowane jest bardzo szeroko. Może to być bowiem nawet taka osoba, która zbiera materiały samodzielnie jedynie z przeznaczeniem (i to niekiedy tylko potencjalnym) przekazania ich konkretnej redakcji (w przeszłości już incydentalnie przyjmującej taki materiał i w szerokim tego słowa znaczeniu pozostająca we współpracy z konkretną osobą). Dziennikarzem będzie też np.: student odbywający praktykę w redakcji[271], jak i początkujący reporter (tzw. wolny strzelec) dopiero starający się o nawiązanie stałej współpracy[272].

Mając powyższe na uwadze, warto byłoby w tym miejscu postulować nieco odmienne spojrzenie na rolę i znaczenie PUODO w kontekście oceny zasadności realizacji przez uprawnionych prawa do bycia zapomnianym. Nie budzi wątpliwości, że przeprowadzona z formalnego punktu widzenia ocena zasadności powołania się w analizowanym przypadku na klauzulę prasową i obowiązujące postanowienia ustawy – Prawo prasowe z perspektywy postanowień RODO i ustawy o ochronie danych osobowych jest co do zasady prawidłowe. Z drugiej jednak stro-

[270] A. Brzostek, *Kiedy blog może zostać uznany za prasę*, z 19 marca 2014, opracowanie zamieszczone na stronie http://prawo.gazetaprawna.pl/artykuly/784760,kiedy-blog-jest-uznawany-za-prase.html z odwołaniem się do zamieszczonego tam orzecznictwa sądów.

[271] J. Sobczak, *Komentarz…*, s. 328; M. Siwicki, *Dziennikarz w ujęciu ustawy Prawo prasowe – problematyka terminologiczna*, „Monitor Prawniczy" 2012, nr 20.

[272] Podkreśla się przy tym jednocześnie, że elementem różnicującym dziennikarza od każdej innej osoby prowadzącej działalność informacyjną jest brak elementu działania z upoważnienia i na rzecz konkretnej redakcji. W praktyce identyfikacja taka jest wyłącznie iluzoryczna ze względu na stopniowe rozluźnianie form i zasad owej współpracy. Szeroko na ten temat z gruntownym omówieniem literatury przedmiotu i wnikliwą analizą K. Siezieniewska, *Zawód dziennikarza w obliczu konwergencji mediów*, praca doktorska, Warszawa 2014, s. 33 i n., zamieszczona na stronie: https://depotuw.ceon.pl/bitstream/handle/item/892/K.%20SIEZIENIEWSKA%20-%20PRACA%20DOKTORSKA.pdf?sequence=1. Na temat praw i obowiązków zob.: L. Garlicki, *Wolność wypowiedzi dziennikarza – przywileje i odpowiedzialność*, „Europejski Przegląd Sądowy" 2010, nr 1, s. 12 i n.

ny pożądana byłaby systemowa modyfikacja kompetencji krajowego organu ochrony w zakresie oceny konkretnej sytuacji przez pryzmat tego, czy rzeczywiście nie dochodzi do naruszenia praw i wolności osoby, której dane dotyczą (są przetwarzane), a nie tylko identyfikacji podmiotu uprawnionego do skutecznego powołania się na treść art. 17 ust. 3 lit. a) RODO i charakteru wykonywanej działalności z perspektywy ustalenia naruszenia (możliwości) przez zobowiązanego przepisów RODO. Oczywiście znane są nam z przeszłości rozstrzygnięcia, które definiowały, że „[…] wśród kompetencji GIODO nie ma uprawnień do badania istotności naruszeń praw i wolności, stąd zgodnie z zasadą wyrażoną w art. 7 Konstytucji RP tak zakreślonej kompetencji nie można domniemywać”[273], co pozostaje oczywiście aktualne, ale nie wykluczalibyśmy zasadności modyfikacji tego stanowiska w następstwie wprowadzenia zmian systemowych. Do tego potrzebna byłaby jednak kolejna reforma kompetencji PUODO.

Mając powyższe na względzie konieczne staje się podkreślenie, że dotychczasowe orzecznictwo sądowe koncentrujące się na zagadnieniu skutecznej realizacji prawa do bycia zapomnianym nie jest jednolite. W innym bowiem rozstrzygnięciu ocena możliwości zapewnienia wnioskodawcy skutecznej ochrony przez PUODO została zweryfikowana zupełnie inaczej. Sprawa dotyczyła skargi skierowanej przez uprawnioną osobę do krajowego organu ochrony danych osobowych ze wskazaniem na nieprawidłowości w przetwarzaniu jej danych osobowych przez redaktora naczelnego czasopisma w zakresie imienia, nazwiska, afiliacji akademickiej oraz szczegółów dotyczących postępowania zakończonego jej ukaraniem (ograniczenie prawa do wykonywania zawodu) w artykule prasowym zamieszczonym na stronie internetowej. Skarga została wniesiona po uprzednim i bezskutecznym

[273] Wyrok WSA w Warszawie z 21 stycznia 2020 r., II SA/Wa 1924/17. Por. też wyrok NSA z 7 września 2021 r., III OSK 2883/21, w którym odrzucono kasację PUODO od rozstrzygnięcia WSA.

wezwaniu do usunięcia danych skarżącego i po upłynięciu wymierzonej kary, co w ocenie skarżącego uzasadniało w pełni jego żądania, także z perspektywy treści art. 10 RODO. PUODO, podobnie jak miało to miejsce we wcześniej omawianym przypadku, umorzył postępowanie w sprawie, odwołując się do braku możliwości merytorycznej oceny udostępnienia danych osobowych.

Również w tej sprawie przeprowadzona została analiza pozwalająca na stwierdzenie, że publikacja miała charakter publikacji prasowej w rozumieniu przepisów – Prawo prasowe, co z perspektywy art. 85 ust. 1 RODO i postanowień ustawy o ochronie danych osobowych uzasadniało podjęcie takiego właśnie rozstrzygnięcia przez PUODO.

Oceniając przesłanki uzasadniające odmowę skutecznej realizacji prawa do bycia zapomnianym, PUODO wskazał, że ze względu na wyłączenie mocą art. 2 ust. 1 ustawy o ochronie danych osobowych art. 5-9 oraz 18-22 RODO do przetwarzania danych osobowych w celu prowadzenia działalności prasowej nie pozwala na ocenę prawidłowości przetwarzania danych osobowych skarżącego, w tym legalności przetwarzania danych osobowych. Nie istnieje bowiem możliwość dokonania merytorycznej oceny bez zweryfikowania legalności, prawidłowości oraz niezbędności w procesie przetwarzania danych (analiza z punktu widzenia postanowień art. 5, 6 oraz 9 RODO oraz zgodność operacji przetwarzania ze wszystkimi ogólnymi zasadami ustanowionymi w art. 5 ust. 1 RODO).

Sąd uznał jednak, że skarżący zasadnie wykazał naruszenie przepisów prawa materialnego, zakreślających kompetencje PUODO. Uznał on bowiem, że choć ustawodawca krajowy skorzystał z upoważnienia zawartego w art. 85 ust. 1 RODO, to w katalogu wyartykułowanych ograniczeń nie uwzględnił art. 17 RODO. Pozwoliło mu to na stwierdzenie, iż „[…] przepisy RODO w danym zakresie – a dotyczące tzw. prawa bycia zapomnianym – odnoszą się także do działalności prasowej, o której mowa w art. 2 ust. 1 ustawy z 2018 r. Nie

można z kolei podzielić stanowiska organu, jakoby przeszkodą dla stosowania danej regulacji mógł być brak odniesienia do innych reguł RODO, w kwestii samego gromadzenia i przetwarzania danych osobowych […]. Art. 17 RODO stanowi spójny kompleks regulacji, dotyczących określonego zagadnienia materialnoprawnego – tu przesłanek możliwości skutecznego żądania usunięcie danych osobowych, także przetwarzanych uprzednio legalnie. Określono tam przesłanki pozytywne sformułowania żądania (tak ust. 1) jak i warunki, gdy nie musi być uwzględnione (tak ust. 2)", odwołując się jednocześnie do sformułowanego w literaturze przedmiotu poglądu uzasadniającego jego stanowisko[274].

W ocenie sądu stanowisko PUODO, który stwierdził, że nie jest on właściwy w sprawie, a obowiązujące przepisy nie pozwalają na merytoryczną ocenę zasadności powoływania się konkretnej osoby na prawo do bycia zapomnianym nie może być uznane za prawidłowe. Uzasadniając swoje rozstrzygnięcie, wskazał, iż zarzut bezpodstawnego przetwarzania danych osobowych wnioskodawcy „w kontekście ich publicznej dostępności – w ramach poszukiwania w sieci Internet, w materiale prasowym", po upływie znacznego czasu od ich publikacji obliguje krajowy organ ochrony „do rozważenia – w granicach własnej kompetencji", czy rzeczywiście wnioskodawca nie ma możliwości skutecznego skorzystania z prawa do bycia zapomnianym. Uznał on jednocześnie – analizując zakres wyłączeń zdefiniowanych przez krajowego ustawodawcę – że PUODO posiada stosowne kompetencje do merytorycznego zbadania, czy „wnioskodawca mógł skutecznie żądać zaprzestania przetwarzania – przez upublicznienie na stosownej stronie internetowej – swoich danych osobowych w mate-

[274] Sąd odwołał się do opracowania M. Gawrońskiego, K. Kloc, K. Kundy, *„Wyjątek dziennikarski" wypowiedzi literackie i artystyczne oraz wypowiedzi akademickie w świetle nowej polskiej ustawy o ochronie danych osobowych cz. II* (opubl. w Lex/el. 2018 jako przypis do art. 2 ustawy z 2018 r.).

riale prasowym, opublikowanym w czasopiśmie", a w konsekwencji umorzenie postępowania w tym właśnie zakresie było bezpodstawne.

Z drugiej strony sąd potwierdził, że krajowy organ ochrony odpowiednio wyjaśnił, że:

- „upublicznianie danego tekstu na stronie internetowej stanowi publikację materiału prasowego, w rozumieniu ustawy – Prawo prasowe, wobec treści art. 2 ust. 1 ustawy z 2018 r. oraz art. 7 w ust. 2 pkt 1 ustawy – Prawo prasowe";
- podmiot, do którego wpłynęło żądanie, spełnia wymagania stawiane prasie;
- zamieszczenie konkretnego materiału prasowego w Internecie „do wglądu w sposób ciągły nie niweczy tego, że chodzi tu publikacje w rozumieniu ustawy – Prawo prasowe; rozpowszechnienie materiału prasowego – jego publikacja – może bowiem nastąpić w formie każdego dostępnego środka technicznego"[275];
- rozumienie „archiwum" zdefiniowanego w zakładce na stronie internetowej czasopisma w żaden sposób nie może być identyfikowane z odrębnymi przepisami definiującymi administracyjnoprawny obowiązek archiwizacyjny[276];
- kwestia naruszenia dóbr osobistych wnioskodawcy „wykracza poza problematykę przepisów dotyczących *stricte* ochrony danych osobowych – nie dotyczą one kwestii praw osobistych w kontekście ochrony dobrego imienia; roszczenia o zaprze-

[275] Wyrok WSA z dnia 21 stycznia 2020 r., II SA/Wa 1924/19.

[276] „Pojęcie archiwizacji – w rozumieniu przepisów odrębnych – dotyczy obowiązku administracyjnoprawnego, co do gromadzenia stosownych dokumentów w odpowiedniej formie i ich zabezpieczenia; sama organizacja strony internetowej – poprzez wydzielenie informacji bieżących od wcześniejszych i określenie danego zbioru mianem «archiwum»" – nie stanowi podstawy do oceny, że zastosowanie do nich znajdą przepisy, dotyczące obowiązku archiwizowania stosownych dokumentów w określonej formie, nie zaś reguły publikacji materiałów prasowych".

stanie bezprawnego naruszenia tych dóbr, o ile do tego faktycznie doszło, mogą być realizowane jedynie w drodze stosownego powództwa przed sądem powszechnym; jako delikt cywilny bądź karny; tylko w danym trybie możliwa jest ocena, czy nie doszło do nadużycia wolności wypowiedzi w materiale prasowym";

– PUODO nie może merytorycznie „oceniać, czy sama publikacja określonych informacji była dopuszczalna; z mocy stosownej regulacji bowiem – wobec jednoznacznie wyrażonej woli prawodawcy – sama kwestia przetwarzania danych osobowych w ramach publikacji prasowych nie jest kompleksowo normowana przepisami w zakresie ochrony danych osobowych; zagadnienie ewentualnej nielegalności w kontekście granic wolności wypowiedzi, wyjęte jest więc z kompetencji organu administracji publicznej, gdy dotyczy publikacji materiału prasowego"[277].

Reasumując, sąd stwierdził, że obowiązkiem krajowego organu ochrony – przy uwzględnieniu charakteru i specyfiki obowiązujących rozwiązań, a w szczególności zakresu zdefiniowanych przez ustawodawcę krajowego wyłączeń – jest zbadanie każdej konkretnej sprawy „w kontekście jej uwarunkowań, z perspektywy sytuacji faktycznej Wnioskodawcy. Okoliczności te mogą mieć wyłącznie znaczenie w kontekście żądania bycie zapomnianym, gdy chodzi o granice przesłanek negatywnych skuteczności jego realizacji"[278].

[277] Wyrok WSA z dnia 21 stycznia 2020 r., II SA/Wa 1924/19.

[278] Podkreślił jednocześnie, że: „Ponieważ sprawa nie była w ogóle badana w tym kontekście przez organ, przedwczesnym byłoby zajmowanie stanowiska w tym aspekcie przez Sąd. Jego zadaniem jest wyłącznie kontrola legalności aktów administracyjnych, gdy sprawa została już rozpoznana w jej istotnych aspektach, w tym poczyniono konieczne w sprawie ustalenia, co do faktów" – wyrok WSA z dnia 21 stycznia 2020 r., II SA/Wa 1924/19.

Stanowisko takie[279] jest niewątpliwie dowodem na poszukiwanie nowego wzorca interpretacji przyczyn i skutków braku wyłączenia stosowania art. 17 RODO do działalności prasowej, a także do wypowiedzi w ramach działalności literackiej lub artystycznej. Opiera się ono na założeniu racjonalności ustawodawcy krajowego, który – definiując konkretne rozwiązania – kierował się przecież wytycznymi sprecyzowanymi przez ustawodawcę unijnego. Jak podkreślano w uzasadnieniu do projektu ustawy o ochronie danych osobowych „[…] w przepisach rozporządzenia 2016/679 wprowadza dwa rodzaje testów, których przeprowadzenie warunkuje możliwość skorzystania przez państwa członkowskie z ograniczeń w stosowaniu rozporządzenia 2016/679 w określonych celach. Pierwszym z nich jest przewidziany w art. 23 rozporządzenia 2016/679 test «niezbędności i proporcjonalności», a drugim jest przewidziany chociażby w art. 85 rozporządzenia test «niezbędności». O ile, jak zostało to wskazane w art. 23 rozporządzenia i odnoszącym się do niego motywie 73 preambuły do rozporządzenia 2016/679 «w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz praw […] o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym»; wymogu proporcjonalności nie przewiduje już ustawodawca unijny w art. 85 rozporządzenia. Zgodnie z odnoszącym się do art. 85 motywem 153 preambuły do rozporządzenia 2016/679 «przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji». Powołanie się na art. 85 rozporządzenia 2016/679 i skorzystanie z przewidzianej w nim swobody regulacyjnej państwa członkowskiego nie

[279] Wyrok nie jest prawomocny. Na dzień oddawania opracowania nie zostało jeszcze wydane orzeczenie przez NSA.

wymaga dokonania więc oceny proporcjonalności proponowanych ograniczeń, a jedynie ich niezbędność”[280].

Oczywiście istotne jest zweryfikowanie, dlaczego ustawodawca nie uznał za niezbędne dokonania wyłączenia tego właśnie przepisu – tu jednak pomocna jest konkretyzacja zawarta wprost w treści art. 17 ust. 3 lit. a) RODO – a także dlaczego nie zdecydował się na dodatkowe uszczegółowienie kompetencji PUODO tylko w zakresie specyfiki realizacji prawa do zapomnienia – i tu z perspektywy wyłączeń określonych w art. 2 ust. 1 ustawy o ochronie danych osobowych sprawa wydaje się również oczywista. Obecnie można mieć bowiem daleko idące wątpliwości, czy w granicach systemowo zdefiniowanego modelu krajowy organ ochrony rzeczywiście posiada kompetencje pozwalające mu skutecznie na podjęcie działań w stosunku do zobowiązanego będącego adresatem żądania kierowanego przez uprawnioną osobę na podstawie art. 17 RODO przy jednoczesnym wyłączeniu stosowania przepisów art. 5–9, art. 11, art. 13–16, art. 18–22, art. 27, art. 28 ust. 2–10 oraz art. 30 RODO.

[280] W uzupełnieniu wskazano, iż: „Dodatkowo należy wskazać, że ustawodawca unijny w art. 85 nie wskazuje konkretnych przepisów podlegających możliwemu ograniczeniu, jak zrobił to w art. 23, wskazując jedynie rozdziały. Tym samym ustawodawca unijny przyznał w art. 85 bardzo szeroki zakres swobody regulacyjnej państwom członkowskim, dostrzegając szczególną wartość działań dziennikarskich oraz artystycznych i akademickich. Dokonując wykładni testu niezbędności, Trybunał Konstytucyjny w wyroku z 5 lutego 2008 r., K 34/06 wskazał, że nakłada on na ustawodawcę «wymóg stwierdzenia rzeczywistej potrzeby dokonania w danym stanie faktycznym ingerencji w zakres prawa bądź wolności jednostki. Z drugiej zaś, winna ona być rozumiana jako wymóg stosowania takich środków prawnych, które będą skuteczne, a więc rzeczywiście służące realizacji zamierzonych przez prawodawcę celów. Ponadto chodzi tu o środki niezbędne, w tym sensie, że chronić będą określone wartości w sposób bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków. Niezbędność to również skorzystanie ze środków jak najmniej uciążliwych dla podmiotów, których prawa lub wolności ulegną ograniczeniu». W ocenie projektodawcy każde z projektowanych ograniczeń w obszarze działalności literackiej, działalności artystycznej, wypowiedzi akademickiej oraz działaniach związanych z tworzeniem materiałów prasowych spełnia powyższe wymogi” – uzasadnienie do projektu ustawy o ochronie danych osobowych, Druk nr 2410, s. 8-9, https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2410.

Szczególną uwagę należy też zwrócić na fakt wyłączenia art. 5 RODO, co w konsekwencji oznacza, że wydawcy prasowi zwolnieni są ze szczegółowego wykazywania niezbędności przetwarzania. Zatem w sytuacji pierwotnej legalności takiego działania brak jest możliwości odwołania się do zasady ograniczenia czasowego procesu przetwarzania w ramach działalności prasowej. W połączeniu ze wskazaną wcześniej przesłanką wyłączającą możliwość skutecznego skorzystania z prawa do bycia zapomnianym (art. 17 ust. 3 lit. a) organ ochrony danych nie dysponuje wzorcem porównawczym, na bazie którego mógłby kwestionować legalność długotrwałego udostępniania informacji na stronie internetowej.

Specyfika systemowej różnorodności podstaw legalizujących przetwarzanie danych osobowych, w tym także ich upublicznienie, staje się widoczna w innej jeszcze sprawie, dotyczącej publikacji danych osobowych (w tym szczególnych) identyfikujących występującego ze skargą konstytucyjną do Trybunału Konstytucyjnego.

2.3. Publikacja danych osobowych w orzeczeniach Trybunału Konstytucyjnego

Trybunał Konstytucyjny w następstwie rozpatrzenia skargi konstytucyjnej wydał wyrok, a następnie wyrok ten z danymi skarżącej (w zakresie imienia i nazwiska, a także informacjami m.in. na temat stanu jej zdrowia, przebytych chorób oraz metod leczenia, postępowań sądowych w sprawie, które znajdowały się w uzasadnieniu) został opublikowany na stronie internetowej organu powołanego do kontroli konstytucyjności prawa. Skarżąca wystąpiła o nakazanie usunięcia jej danych osobowych z sentencji i uzasadnienia opublikowanego wyroku, podkreślając, iż publikowane na stronie internetowej przez Trybunał w tej sprawie dokumenty (skarga konstytucyjna oraz stanowiska uczestników postępowania) były przed ich publikacją anonimizowane. Przed wystąpieniem do

GIODO wniosła do administratora o usunięcie jej danych osobowych z opublikowanego na stronie internetowej orzeczenia.

Prezes Trybunału Konstytucyjnego w odpowiedzi wskazał, że podstawą zamieszczenia danych osobowych w postaci imienia i nazwiska skarżącej był art. 71 ust. 1 pkt 3 ustawy z dnia 1 sierpnia 1997 r. o Trybunale Konstytucyjnym (Dz. U. Nr 102, poz. 643 ze zm.), który stanowi, że orzeczenie Trybunału Konstytucyjnego zawiera wymienienie wnioskodawcy i innych uczestników postępowania; art. 9 ust. 1 pkt 6 ustawy, art. 190 ust. 2 Konstytucji Rzeczypospolitej Polskiej i art. 79 ust. 1 ustawy o Trybunale Konstytucyjnym, które obligowały do publikacji orzeczenia w Dzienniku Ustaw. Podniesiono również, że w regulacjach tych brak jest podstaw do „modyfikowania (w tym anonimizowania) publikowanych orzeczeń", a strona www.trybunal.gov.pl pełni funkcję Biuletynu Informacji Publicznej w rozumieniu przepisów ustawy o dostępie do informacji publicznej, co oznacza, że publikowane tam orzeczenia stanowią informację w rozumieniu jej art. 1 ust. 1. Dodatkowo odwołano się do obowiązującego w tamtym okresie § 53 ust. 2 Regulaminu Trybunału Konstytucyjnego. W dalszej części argumentacja odwoływała się do treści art. 28b ust. 1 ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (obowiązek udostępniania publikowanych orzeczeń na stronach internetowych Rządowego Centrum Legislacji oraz za pomocą środków komunikacji elektronicznej lub informatycznych nośników danych w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne).

Podkreślono jednocześnie, iż „Specyfika postępowania przed Trybunałem nie pozwala na proste przeniesienie standardów anonimizacji orzeczeń stosowanych przez Sąd Najwyższy, sądy powszechne czy administracyjne. Biorąc pod uwagę chociażby sam skutek wyroku Trybunału oraz powiązaną z nim moc powszechnie obowiązującą, trudno nie zwrócić uwagi, że w interesie publicznym jest kształtowa-

nie postępowania przed Trybunałem w sposób jak najbardziej transparentny, włączając w to określenie podmiotu inicjującego takie postępowanie. Nie sposób w ujawnieniu imienia i nazwiska podmiotu (osoby fizycznej lub prawnej) domagającego się derogacji przepisu ustawy doszukiwać się tak naruszenia przepisów ustawy o ochronie danych osobowych, jak i prawa do prywatności”[281].

Dodatkowo przywołane zostało orzecznictwo sądów uzasadniające ograniczenie prywatności osób prywatnych, których dane znajdują się w dokumentach urzędowych[282].

Pierwotne GIODO odmówił uwzględnienia wniosku, jednak ostatecznie już po wpłynięciu skargi, po powtórnym rozpatrzeniu zgromadzonego w sprawie materiału dowodowego i przeanalizowaniu sprawy, nakazał Prezesowi Trybunału Konstytucyjnego wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych, poprzez usunięcie ze strony internetowej, jej danych osobowych w zakresie imienia i nazwiska, zawartych w wyroku wydanym przez Trybunał Konstytucyjny[283]. W uzasadnieniu stwierdził, że analiza obowiązujących regulacji (art. 27 ustawy o ochronie danych osobowych; art. 1

[281] Wyrok WSA w Warszawie z dnia 19 stycznia 2017 r., II SA/Wa 1434/16.

[282] Podniesiono, że „Ochrona ta nie obejmuje działalności publicznej osoby ani też sfery działań i zachowań, które ogólnie są pojmowane jako osobiste lub prywatne, jeżeli działania te lub zachowania wiążą się ścisłe z działalnością publiczną” (wyrok SN z 24 czerwca 2003 r., sprawa III RN 95/02). W wyroku z 8 listopada 2012 r. w sprawie I CSK 190/12 Sąd Najwyższy stwierdził ponadto, że nie zawsze imiona i nazwiska osoby fizycznej, także wówczas, gdy nie pełni ona funkcji publicznej, będą objęte ochroną życia prywatnego. Według Prezesa TK przywołany przez skarżącą wyrok WSA w Warszawie z 18 listopada 2008 r., II SA/Wa 1177/08 „nie jest adekwatny [...] w zakresie dotyczącym publikacji orzeczeń przez Trybunał Konstytucyjny. [...] jednym z elementów, które sądy administracyjne biorą pod uwagę przy ocenie dopuszczalności publikowania danych osobowych, jest również powiązanie ze sferą publiczną (zob. wyrok NSA z dnia 14 marca 2013 r., sprawa I OSK 620/12). A tak, co oczywiste, jest w przypadku skargi konstytucyjnej oraz wyroku Trybunału wydanego w następstwie takiej skargi”, *ibidem.*

[283] Decyzja GIODO z dnia 16 czerwca 2016 r., DOLiS/DEC-505/16, 54485, 54488. Decyzja ta uchylała dwie wcześniejsze decyzje: z dnia 5 kwietnia 2016 r. (DOLiS/DEC-246/16/25397,25400), oraz poprzedzającą ją decyzję z dnia 5 listopada 2014 r.

ust. 1, 3 ust. 1 pkt 2, art. 5 ust. 2, art. 6 ust. 1 pkt 4 lit. a), art. 8 ust. 3 ustawy o dostępie do informacji publicznej; art. 9 ust. 1 pkt 6 ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych oraz art. 100 ust. 1 pkt 3 i 4 ustawy o Trybunale Konstytucyjnym, pozwala stwierdzić, że przetwarzanie danych osobowych skarżącej przez Trybunał Konstytucyjny poprzez ich publikację na stronie internetowej „odbywa się niezgodnie z art. 27 ust. 2 pkt 2 ustawy (o ochronie danych osobowych), bowiem udostępnione zostało imię i nazwisko skarżącej, a także informacje dotyczące jej osoby, jak stan zdrowia (przebyte choroby, metody leczenia), przebieg i wynik postępowań sądowych”[284].

Fundamentalne w sprawie stało się przeprowadzenie analizy treści art. 5 ust. 2 ustawy o dostępie do informacji publicznej, w którym definiuje się ograniczenia dostępu do takiej informacji, co w analizowanym przypadku powinno przyjąć postać anonimizacji orzeczenia, które w takiej postaci i tak będzie pozwalać wszystkim zainteresowanym na zapoznanie się z istotą rozstrzygnięcia[285]. Wskazano również, że obowiązujący w tamtym okresie przepis art. 100 ust. 1 pkt 4 ustawy o Trybunale Konstytucyjnym nie legalizował publikacji wyroku wraz ze wszystkimi danymi na stronie internetowej BIP. W konsekwencji uznano, że administrator, przetwarzając dane osobowe i uwzględniając

(DOLiS/DEC-1048/14/87035,87037), https://archiwum.giodo.gov.pl/p/decyzje [dostęp: 5.10.2021].

[284] Wyrok WSA w Warszawie z dnia 19 stycznia 2017 r., II SA/Wa 1434/16.

[285] Rozstrzygnięcie takie wielokrotnie były podejmowane przez GIODO; np. w innym stwierdzał on, że: „Organ dysponujący informacjami, które w myśl ustawy o dostępie do informacji publicznej stanowią informację publiczną i jednocześnie są objęte przynajmniej jedną z tajemnic wymienionych w art. 5 ust. 1-3 wskazanej ustawy, jest zobowiązany do nieujawniania tych informacji. Ustawodawca uznał je bowiem za informacje konfidencjonalne. Zlekceważenie tego obowiązku skutkowałoby działaniem organu wbrew przepisom prawa i naruszeniem nie tylko norm powołanej ustawy, lecz także zasad ustanowionych w ustawie zasadniczej z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. z 1997 r., nr 78, poz. 483, z późn. zm.)”, decyzja GIODO z 31 sierpnia 2016 r., DIS/DEC-783/16/77613.

zasadę adekwatności, nie był uprawniony do upublicznienia w wyroku Trybunału Konstytucyjnego danych osobowych skarżącej[286].

Argumentacja skargi, którą administrator skierował do sądu, opierała się na wskazaniu istoty i charakteru orzeczeń Trybunału Konstytucyjnego, ich odrębności systemowej, specyfiki prawnych podstaw publikacji orzeczeń jako informacji publicznej w BIP, a także szerokiemu odwołaniu się do orzecznictwa, które uzasadniało legalność traktowania danych osobowych jako informacji publicznej[287].

Analiza pozwoliła skarżącemu na przedstawienie konkluzji, w myśl której „[…] trudno wyprowadzić z art. 5 ust. 2 ustawy o dostępie do informacji publicznej zakaz publikowania na stronie internetowej Trybunału Konstytucyjnego, imienia i nazwiska osoby fizycznej, która zainicjowała postępowanie zakończone wydaniem wyroku. Tego typu dane osobowe, ze względu na charakter postępowania przed Trybunałem, nie mieszczą się w sferze ochrony prywatności wyznaczonej przez ww. przepis, a ich przetwarzanie na stronie internetowej, w kontekście przytoczenia treści wyroku Trybunału Konstytucyjnego są adekwatne do założonego celu, tym samym odbywa się to zgodne z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Taka wykładnia art. 5 ust. 2 ustawy o dostępie do informacji publicznej koresponduje ze wskazanym we wcześniejszej części skargi art. 9 ust. 1 pkt 6 w zw. z art. 28 b ust. 1 pkt 2 ustawy z 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych w zw. z art. 100

[286] W uzasadnieniu odwołano się też do orzecznictwa sądów administracyjnych i Sądu Najwyższego.

[287] Wskazano np. na orzeczenia SN oraz NSA, w których za prawidłowe uznano udostępnianie imion i nazwisk osób fizycznych, które weszły w formalne relacje z organami władzy publicznej, nawet wówczas, gdy nie uzyskały przez to bezpośredniego wpływu na sprawowanie funkcji publicznych – wyrok SN z dnia 8 listopada 2012 r., I CSK 190/12; wyrok NSA z dnia 9 października 2014 r., I OSK 546/14; wyrok NSA z dnia 12 lutego 2015 r., I OSK 759/14; wyrok NSA z dnia 6 lutego 2015 r., I OSK 650/14; wyrok NSA z dnia 4 lutego 2015 r., I OSK 531/14; wyrok NSA z dnia 11 grudnia 2014 r., I OSK 213/14; wyrok NSA z dnia 8 lipca 2015 r, I OSK 1530/14.

ust. 1 pkt 3 ustawy z 25 czerwca 2015 r. o Trybunale Konstytucyjnym, z których wynika obowiązek publikacji danych inicjatora postępowania w dzienniku urzędowym (jako element składowy orzeczenia). Ustawodawca przewidując podanie tego typu danych do publicznej wiadomości ogranicza jednocześnie zakres prywatności przysługujący osobie fizycznej. Inne założenie przeczyłoby zasadzie racjonalności ustawodawcy"[288].

Sąd, rozpatrując tę sprawę, podtrzymał ostateczną decyzję GIODO[289]. Po przeprowadzeniu analizy obowiązujących przepisów i zakresu przetwarzanych danych osobowych (nie tylko imię i nazwisko, ale również charakter zatrudnienia, niezdolność do pracy z powodu choroby, informacje o zasiłkach chorobowych decyzję Zakładu Ubezpieczeń Społecznych z podaniem daty i znaku sprawy o zwrocie nienależnie pobranego zasiłku chorobowego i uzasadnienie tego stanowiska, argumentację i zarzuty wymienione zawarte w odwołaniu do sądu, datę i sygn. wyroków sądowych wraz z ustaleniami faktycznymi dokonanymi przez sądy) sąd uznał, że link do strony internetowej z zamieszczonym wyrokiem i przytoczonymi w nim opisanymi danymi, jest niezgodny z treścią art. 27 ust. 2 pkt 1) i 2) ustawy o ochronie danych osobowych, ponieważ brak było zgody na piśmie na przetwarzanie danych osoby, której one dotyczą. Zwrócono również uwagę, że art. 5 ust. 2 ustawy o dostępie do informacji publicznej nie legalizuje udostępniania danych osobo-

[288] Wyrok WSA w Warszawie z dnia 19 stycznia 2017 r., II SA/Wa 1434/16.

[289] W decyzji wyraźnie podkreślono, że „prywatność Skarżącej, jako dobro chronione prawem powinno mieć pierwszeństwo przed innym dobrem prawem chronionym – dostępnością do informacji publicznej. Udostępniając, bowiem informację publiczną w sposób ingerujący w prywatność osoby fizycznej administrator danych obowiązany jest ustalić czy zakres przekazywanych danych jest niezbędny dla potrzeb takiego udostępnienia. Jak wynika z poczynionych w tym zakresie ustaleń, w przedmiotowym przypadku doszło do przekroczenia niezbędnego zakresu danych przekazywanych celem ich udostępnienia", decyzja GIODO z dnia 16 czerwca 2016 r., DOLiS/DEC-505/16, 54485, 54488, s. 8.

wych osoby niepełniącej funkcji publicznej[290]. W tym zakresie „Udostępniając, […] informację publiczną w sposób ingerujący w prywat-

[290] W uzasadnieniu wniosku I Prezesa SN z 16 lutego 2021 r. do Trybunału Konstytucyjnego (o sygnaturze K 1/21) podniesiono, że „art. 5 ust. 1, ust. 2 i ust. 3 oraz art. 2 ust. 2 u.d.i.p. w zakresie, w jakim przepisy te, nakładając na władze publiczne oraz inne podmioty wykonujące zadania publiczne obowiązek udostępniania informacji publicznej nie regulują zarazem kwestii anonimizacji danych osobowych lub innych danych ze sfery prywatności oraz wyłączają możliwość weryfikacji interesu prawnego lub faktycznego w pozyskaniu tych danych celem nadużycia prawa podmiotowego – są niezgodne z art. 47, art. 51 ust. 2, art. 51 ust. 5, art. 61 ust. 1, art. 61 ust. 2 i art. 61 ust. 4 Konstytucji RP oraz z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm). Przede wszystkim należy zauważyć, że anonimizacja (utajnienie) określonych danych osobowych wchodzących w skład udostępnianej informacji publicznej jest narzędziem kompromisowym, jakie zostało wypracowane w judykaturze. Anonimizacja jest czynnością o charakterze technicznym, dokonywaną na dokumencie stanowiącym informację publiczną, polegającą na zasłonięciu części tego dokumentu, zawierającej dane niepodlegające udostępnieniu. Jest to niewątpliwie sposób pozwalający na ujawnienie informacji i publicznych z wyłączeniem szczególnie istotnych informacji podlegających ochronie, np. ze względu na prywatność. Anonimizacja nie może jednak prowadzić do udostępnienia tylko części wnioskowanych dokumentów, a jedynie do utajnienia tzw. „wrażliwych danych" (zob. wyrok Wojewódzkiego Sądu Administracyjnego w Olsztynie z dnia 21 listopada 2019 r., SAB/Ol 75/19, LEX nr 2750054). W ocenie wnioskodawcy trudno uznać, aby rozwiązanie problemu i obowiązku konstytucyjnego wynikającego z konieczności ważenia zasad zawartych w art. 47 i art. 51 ust. 2 Konstytucji RP oraz w art. 61 Konstytucji RP, które w praktyce polega na anonimizacji określonych danych powinno być, w demokratycznym państwie prawnym, rozwiązywane na płaszczyźnie stosowania prawa (nawet sądowego), co dodatkowo jest ograniczone naturalnymi właściwościami procesu stosowania prawa narażonego na wystąpienie braku jednolitości orzecznictwa. Tymczasem brak ustawowo normowanych zasad anonimizacji jest istotnym mankamentem, który pozostawia ustalenie granic ochrony prawa do prywatności podmiotom udostępniającym określone dane (informacje). Działanie organu może bowiem powodować przekroczenie granic i zakresu prawa do informacji publicznej, wynikającego z art. 61 ust. 1 i ust. 2 Konstytucji RP. Podjęcie zaś samodzielnej decyzji o anonimizacji danych w przypadku braku regulacji prawno-materialnej może narazić podmiot udostępniający na zarzut odpowiedzialności karnej z art. 23 u.d.i.p (s. 25). Warto w tym miejscu podkreślić, że klasyczny test szkody, ważenia interesów i proporcjonalności także sprowadza się do oceny, co i kiedy w odniesieniu do konkretnej osoby może być ujawnione. Zawsze więc tego rodzaju mechanizm będzie musiał towarzyszyć udostępnianiu informacji publicznej dotyczącej osoby pełniącej funkcję publiczną.

ność osoby fizycznej administrator danych obowiązany jest ustalić, czy zakres przekazywanych danych jest niezbędny dla potrzeb takiego udostępnienia. Jak wynika z poczynionych w tym zakresie ustaleń, w przedmiotowym przypadku doszło do przekroczenia niezbędnego zakresu danych przekazywanych celem ich udostępnienia", co miało fundamentalne znaczenie w kontekście potwierdzenia konieczności odróżnienia wykonania obowiązku wynikającego z treści art. 100 ust. 1 pkt 4 ustawy z dnia 25 czerwca 2015 r. o Trybunale Konstytucyjnym, a legalności i dopuszczalności publikacji pełnej treści tego rozstrzygnięcia na stronie internetowej Biuletynu Informacji Publicznej. W konsekwencji sąd uznał, że prawidłowe upublicznienie rozstrzygnięć Trybunału na stronie internetowej powinno każdorazowo uwzględniać zasadę adekwatności, co w praktyce oznacza konieczność odpowiedniego przetworzenia danych osobowych w nich zawartych[291].

Niejako na poboczu głównych rozważań pojawiła się też kwestia prawa do bycia zapomnianym (art. 17 RODO). W dacie orzekania przepisy tego aktu już obowiązywały, choć nie były jeszcze bezpośrednio stosowane. Podkreślono jednak, że uprawniona osoba ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe. Zwrócono jednocześnie uwagę, że „Ze względu na specyfikę funkcjonowania sieci Internet, dane te będą dostępne dla podmiotów z całego świata oraz będą mogły być pozyskiwane bez żadnych ograniczeń przez osoby fizyczne i podmioty gospodarcze, a następnie wykorzystywane przez te osoby i podmioty w dowolnych celach i w dowolny sposób np. do celów profilowania. Publikując dane osobowe w Internecie administrator danych osobowych powinien mieć świadomość powyższych konsekwencji"[292]. Argumentacja ta służyć

[291] Wyrok WSA w Warszawie z dnia 19 stycznia 2017 r., II SA/Wa 1434/16.
[292] *Ibidem.*

miała podkreśleniu istoty i charakteru prawa do bycia zapomnianym z jednoczesnym wskazaniem potencjalnych skutków, jakie mogą zostać wywołane w następstwie takiego właśnie upublicznienia.

2.4. Przetwarzanie danych upublicznionych w jawnych rejestrach w ramach wykonywanej działalności serwisu internetowego

Bardzo istotną sprawą, która w pełnym zakresie zdaje się obrazować problemy ze zrozumieniem prawa do zapomnienia, jest ta dotycząca skargi na przetwarzanie danych osobowych przez konkretny podmiot dla potrzeb związanych z funkcjonowaniem prowadzonego w ramach wykonywanej działalności serwisu internetowego. W ocenie skarżącego działanie takie było nieuprawnione, co uzasadniało w pełnym zakresie wystąpienie z żądaniem ich usunięcia z serwisu, a także zaprzestania ich przetwarzania przez administratora.

W tym konkretnym przypadku okazało się jednak, że „realizacja celów Fundacji jest zarazem uwarunkowana przetwarzaniem danych osobowych ujawnionych w publicznie dostępnych rejestrach, w tym danych osobowych skarżącego, jako osoby pełniącej określone funkcje w podmiotach podlegających wpisowi do Rejestru", co znajduje umocowanie w art. 6 ust. 1 lit. f) RODO[293], jak i to, że ponowne wykorzystywanie tego rodzaju danych (informacji pochodzących z KRS) nie zostało w tym zakresie warunkami takimi ograniczone. Jednocześnie przeprowadzona została analiza wszystkich przesłanek wskazanych przez ustawodawcę unijnego w art. 17 ust. 1 RODO w powiązaniu z prawem do sprzeciwu (art. 21 ust. 2 RODO)[294].

[293] Na temat przesłanek legalizujących zob.: M. Jabłoński, K. Wygoda, *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej. Aspekty praktyczne*, Warszawa 2021, s. 50-93.

[294] „Organ wskazał, że w rozpoznawanej sprawie, dane osobowe skarżącego w dalszym ciągu są niezbędne w kontekście celów realizowanych przez Fundację (brak przesłanki z art. 17 ust. 1 lit. a) RODO), podstawą ich przetwarzania jest prawnie usprawie-

Sąd, rozstrzygając skargę na rozstrzygniecie krajowego organu ochrony, stwierdził, że „przetwarzanie przez Fundację publicznie dostępnych danych osobowych skarżącego, jako osoby pełniącej określone funkcje w podmiotach podlegających wpisowi do KRS, w tym ich publikacja, znajduje oparcie w art. 6 ust. 1 lit. f RODO". Uznał ponad-

dliwiony interes realizowany przez administratora (art. 6 ust. 1 lit. f) RODO) a nie zgoda skarżącego (brak przesłanki z art. 17 ust. 1 lit. b), kwestionowany proces przetwarzania danych osobowych skarżącego jest realizowany w sposób legalny (brak przesłanki z art. 17 ust. 1 lit. d) RODO), nie istnieje przepis, który obligowałby Fundację do usunięcia kwestionowanych danych osobowych skarżącego (brak przesłanki z art. 17 ust. 1 lit. e) RODO), dane osobowe skarżącego nie zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO (brak przesłanki z art. 17 ust. 1 lit. f) RODO). W rozpoznawanej sprawie nie można również przyjąć istnienia przesłanki do skutecznego żądania usunięcia danych określonej w art. 17 ust. 1 lit. c) RODO. Powołany przepis nakazuje usunąć dane w sytuacji wniesienia przez osobę, której one dotyczą sprzeciwu na mocy art. 21 ust. 1 i ust. 2 RODO – te z kolei regulacje dotyczą sprzeciwu wobec przetwarzania danych osobowych odpowiednio w sytuacji: gdy przetwarzanie to jest realizowane na podstawie art. 6 ust. 1 lit. e) lub f) RODO oraz gdy celem przetwarzania danych jest cel marketingowy. W niniejszej sprawie dane osobowe skarżącego są przetwarzane w celach niezwiązanych z marketingiem. Organ wskazał jednocześnie, że art. 21 ust. 1 RODO przyznaje osobie, której dane dotyczą, prawo do tego, by w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów wskazując zarazem, że administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. W sytuacji, gdy żądanie przewidziane w art. 21 ust. 1 RODO jest zasadne, osoba, której dane dotyczą, ma prawo domagać się realizacji prawa do bycia zapomnianym (art. 17 ust. 1 lit. c) RODO). Organ wskazał, że w przedmiotowej sprawie w istocie skarżący nie wniósł sprzeciwu wobec przetwarzania jego danych osobowych – nie twierdzi on bowiem, że Fundacja dysponuje przesłanką przetwarzania jego danych osobowych przewidzianą w art. 6 ust. 1 lit. e) lub lit. f) RODO, lecz nie może danych tych przetwarzać z uwagi na jego szczególną sytuację. Skarżący twierdzi natomiast, że Fundacja nie ma w ogóle podstaw prawnych do przetwarzania jego danych – wobec niespełnienia którejkolwiek z przesłanek z art. 6 ust. 1 RODO. W tej sytuacji, posłużenie się przez pełnomocnika skarżącego w inicjującej przedmiotowe postępowanie skardze formułą cyt.: «wyrażam sprzeciw wobec przetwarzania danych osobowych Mojego Mocodawcy» organ uznał za błędne i nie odnoszące się w istocie do instytucji sprzeciwu z art. 17 ust. 1 RODO", wyrok WSA w Warszawie z dnia 19 października 2020, II SA/Wa 2837/19.

to, że w analizowanym zakresie zgoda osoby, której dane były przetwarzane nie była wymagana, wątpliwości nie budziła legalność i adekwatność przetwarzanych danych, nie doszło też do naruszenia przepisów ustawy o ponownym wykorzystywaniu informacji sektora publicznego. Co istotne, uznano również, że skarżący skutecznie nie wniósł sprzeciwu wobec przetwarzania danych (art. 21 ust. 1 RODO), albowiem „nie powoływał się na przyczyny związane ze swoją szczególną sytuacją, o czym jest mowa w tym przepisie, a kwestionował zgodność z prawem ich przetwarzania na podstawie art. 6 ust. 1 lit. f RODO”[295].

Podobne rozstrzygnięcia podejmowane były przez GIODO już w przeszłości, a dotyczyły legalności funkcjonowania stron internetowych, które zawierały np. dane osobowe lekarzy[296], także z określeniem bezzasadności zgłoszenia sprzeciwu[297].

Należy mieć na uwadze, że skuteczne wniesienie sprzeciwu daje dopiero podstawę do wystąpienia przez osobę, której dane dotyczą z żądaniem usunięcia danych tzw. prawem do bycia zapomnianym. W takiej sytuacji administrator zobowiązany jest żądanie przyjąć i podjąć działania zmierzające do jego realizacji, zachowując przy tym wymogi określone w art. 12 RODO (o czym szerzej piszemy w rozdziale III pkt 4.2). Pozytywne rozpatrzenie żądania usunięcia danych nakłada na administratora obowiązek poinformowania o tym każdego odbiorcy[298],

[295] Wyrok WSA w Warszawie z dnia 19 października 2020, II SA/Wa 2837/19.

[296] „Mając zatem na uwadze, iż dane osobowe Skarżącej udostępnione na ww. stronie internetowej dotyczą wyłącznie jej życia zawodowego, jak również to, że są one tożsame z danymi, dotyczącymi Skarżącej, dostępnymi w CEIDG oraz Centralnym Rejestrze Lekarzy w zakresie imienia, nazwiska i specjalizacji lekarskiej, nie sposób uznać, iż doszło do naruszenia jej prawa do ochrony prawnej życia prywatnego, rodzinnego czy też prawa do decydowania o swoim życiu osobistym” – decyzja GIODO z dnia 11 sierpnia 2017 r., DOLiS/DEC-977/17.

[297] Decyzja GIODO z dnia 11 sierpnia 2017 r., DOLiS/DEC-977/17.

[298] „Odbiorca – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie do tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkret-

któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku[299]. Poza tym, administrator informuje osobę, której dane dotyczą, o tych odbiorach, jeżeli wystąpi ona z takim żądaniem (art. 19 RODO)[300].

Przyjęte na tle art. 19 RODO rozwiązanie zasługuje na aprobatę, bowiem ma ono charakter gwarancyjny względem osoby, której dane dotyczą[301]. Daje ono możliwość „osobie fizycznej kontroli nad dotyczącymi jej informacjami"[302]. Poza tym nic nie stoi na przeszkodzie, aby osoba korzystająca z przyznanego jej na mocy art. 19 *in fine* żądania mogła wystąpić z nim w momencie składania administratorowi wniosku o usunięcie danych[303]. „Realizacja takiego prawa do poinformowania ma wówczas charakter warunkowy – będzie ono realizowane wówczas, gdy administrator stwierdzi podstawy do wykonania uprawnień określonych w art. 16–18 RODO (w tym przypadku prawa do usunięcia danych – art. 17 RODO, przyp. M.J. i J.W.) i faktycznie je wykona"[304].

---

nego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosowanie do celów przetwarzania" – art. 4 pkt 9 RODO.

[299] Na temat tego pojęcia zob.: M. Jabłoński, K. Wygoda, *Praktyczne znaczenie podstawowych pojęć RODO – wybrane zagadnienia*, Wrocław 2019, s. 113–114; M. Jabłoński, D. Kuźnicka-Błaszkowska, *The meaning of the concept of „disproportionate effort" as a refund not specified in art. 14 GDPR*, „Przegląd Prawa Konstytucyjnego" 2021, nr 6 (w druku).

[300] Zob. na ten temat J. Kurek, *Prawo do uzyskania powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,* [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą, na podstawie rodo,* Wrocław 2017, s. 251 i n.

[301] M. Sakowska-Baryła, *Komentarz do art. 19,* [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 251.

[302] M. Czerniawski, *Komentarz do art. 19,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 540.

[303] M. Sakowska-Baryła, *Komentarz do art. 19…,* s. 252.

[304] *Ibidem.*

2.5. Kwestie związane z rzeczywistym zagwarantowaniem przez administratora środków technicznych zapewniających możliwość skorzystania przez uprawnionego z prawa do bycia zapomnianym

Nieco inne problemy wiążą się z wdrożeniem takich rozwiązań proceduralnych w tym technicznych, które zapewniają uprawnionemu skuteczną realizację prawa do bycia zapomnianym. W jednej ze spraw krajowy organ ochrony uznał, że naruszenie art. 17 RODO przybrało postać wdrożenia przez administratora takiego procesu, który *de facto* utrudniał skuteczne odwołanie zgody (wprowadzał też w błąd) na przetwarzanie danych osobowych, uniemożliwiając tym samym faktyczne doprowadzenie do skorzystania z gwarantowanego prawa[305].

Przy tej okazji PUODO wyraźnie podkreślił, że na administratorze ciąży obowiązek opracowania i wdrożenia nie tylko takich środków technicznych i organizacyjnych, które w rzeczywisty i efektywny sposób zapewnią osobie, której dane dotyczą, w formie łatwo dostępnej, zwięzłej, przejrzystej i zrozumiałej informacje na temat, możliwość skutecznego odwołania drogą elektroniczną zgody na przetwarzanie danych osobowych[306], ale równolegle stworzenie mechanizmów wnoszenia skutecznych żądań w każdej formie (oczywiście także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną). Ocena sumy rozwiązań dokonywana jest więc

[305] PUODO stwierdzał naruszenie art. 5 ust. 1 lit. a) w związku z art. 5 ust. 2 oraz art. 7 ust. 3, art. 12 ust. 2, art. 17 ust. 1 lit. b) i art. 24 ust. 1 RODO poprzez niewdrożenie przez administratora odpowiednich środków technicznych i organizacyjnych, które umożliwiałyby osobie, której dane dotyczą, łatwe i skuteczne wycofanie zgody na przetwarzanie swoich danych osobowych oraz realizację prawa do żądania niezwłocznego usunięcia swoich danych osobowych, czyli prawa do bycia zapomnianym.

[306] Na temat odpowiedniego zapewnienia osobom w procesie rejestracji w serwisie internetowym możliwości wyboru w kwestii wyrażenia zgody na przetwarzanie danych w zakresie adresu e-mail odrębnie dla poszczególnych celów przetwarzania danych osobowych zob.: decyzja GIODO z dnia 2 października 2015 r., DIS/DEC-796/15/89140.

także ze względu na kryterium łatwości i dostępności wycofania zgody i realizacji praw, o których mowa w art. 15–22 RODO.

Zarówno PUODO, jak i sąd orzekający potwierdzili, że każdy administrator danych jest odpowiedzialny za przestrzeganie wszystkich zasad przy przetwarzaniu danych osobowych (wymienionych w art. 5 RODO). Podkreślone jednocześnie zostało znaczenie poszanowania zasady rozliczalności, której prawidłowe uwzględnienie wiąże się z koniecznością wykazania przez administratora dowodów na przestrzeganie wszystkich obowiązujących zasad przetwarzania danych. W ocenie organów rozstrzygających istotne jest więc każdorazowo przeprowadzenie wszechstronnej oceny istnienia podstawy przetwarzania danych osobowych przez administratora. Jak podkreślił to sąd, „Jeżeli osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych, to ma prawo w dowolnym momencie wycofać zgodę, jak stanowi art. 7 ust. 3 rozporządzenia. Wycofanie zgody powinno skutkować zaprzestaniem przetwarzania danych w zakresie, w jakim przetwarzanie opiera się na zgodzie. Jeżeli administrator, pomimo wycofania zgody, nie zaprzestał przetwarzania danych, to osoba, której dane dotyczą, może żądać dopełnienia tego obowiązku, a administrator ma obowiązek niezwłocznie usunąć dane”[307]. Jednocześnie naruszeniem prawa gwarantowanego w art. 17 ust. 1 lit. b) będzie takie zachowanie administratora, które przyjmuje postać stworzenia tak skomplikowanych i wprowadzających w błąd mechanizmów, które *de facto* uniemożliwiają szybkie i proste odwołanie wyrażonej zgody[308].

[307] W tym też zakresie przyjęto, że dochodzi do naruszenia prawa do usunięcia danych (prawo do bycia zapomnianym), w sytuacji, w której administrator stosuje taki proces odwołania zgody, który utrudnia skuteczne odwołanie zgody, wyrok WSA w Warszawie z dnia 10 lutego 2021 r., II SA/Wa 2378/20.

[308] Wyrok WSA w Warszawie z dnia 10 lutego 2021 r., II SA/Wa 2378/20.

Rozdział III

Specyfika prawa do bycia zapomnianym

Szybki postęp techniczny stwarza jednostce wiele możliwości, ale także i wiele zagrożeń m.in. w zakresie przepływu danych osobowych. Zapewnienie więc wysokiego poziomu ochrony danych osobowych, a także przyznanie jednostce kontroli nad jej danymi wiąże się z potrzebą aktualizacji przepisów prawnych. Wyzwaniom, które pojawiły się w dziedzinie ochrony danych osobowych, stawił czoło prawodawca unijny, czego efektem jest wejście w życie w dniu 24 maja 2016 r. rozporządzenia Parlamentu Europejskiego i Rady 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 osobowych), które zaczęło być stosowane od 25 maja 2018 r.

W rozporządzeniu, o którym mowa odniesiono się m.in. do:

- warunków wyrażania zgody przez dziecko w przypadku usług społeczeństwa informacyjnego;
- przejrzystego informowania i komunikowania oraz trybu wykonywania praw przez osobę, której dane dotyczą;
- zasad profilowania;
- obowiązku uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych;

– ogólnych warunków nakładania administracyjnych kar pieniężnych[309], a także prawa do bycia zapomnianym[310], które stanowi przedmiot niniejszych rozważań.

1. Zakres podmiotowy prawa do bycia zapomnianym

1.1. Podmiot uprawniony

Prawo do bycia zapomnianym uregulowane zostało w art. 17 RODO. Zgodnie z tym przepisem, podmiotem uprawnionym jest „osoba, której dane dotyczą", a więc tylko osoba fizyczna, bowiem „niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz da-

[309] Por. P. Kowalik, D. Wociór, *Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego,* [w:] *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem ogólnego rozporządzenia unijnego,* Warszawa 2016, s. 4; D. Wociór, *Informacje wstępne,* [w:] D. Wociór (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego,* Warszawa 2016, s. 3 i n.

[310] Zob. np. D. McGoldrick, *Developments in the Right to be Forgotten,* "Human Rights Law Review" 2013, Vol. 12, No. 3, s. 761 i n.; G. Sartor, *The right to be forgotten in the Draft Data Protection Regulation,* "International Data Privacy Law" 2015, Vol. 5, No. 1, s. 64 i n.; J. Żak, *Koncepcja „prawa do bycia zapomnianym",* [w:] M. Jabłoński, S. Jarosz-Żukowska (red.), *Aktualne wyzwania ochrony…*, s. 141 i n.; B. Baran, K. Poglodniak-Gierz, *Perspektywa regulacji prawa do bycia zapomnianym w Internecie. Zarys problematyki,* „Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego. Nauki Społeczne" 2017, nr 17(2), s. 144 i n.; B. Wysocki, *Prawo do bycia zapomnianym – prawem cyfrowej rzeczywistości,* „Ars Educandi" 2016, nr 13, s. 107 i n.; L. Szot, *Prawo do bycia zapomnianym w sieci,* [w:] W. Kitler, J. Taczkowska-Olszewska (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne,* Warszawa 2017, s. 183 i n.; A.A. Sławiński, *„Prawo do bycia zapomnianym" w świetle ogólnego rozporządzenia o ochronie danych osobowych i orzecznictwa TSUE,* [w:] M. Wiązek (red.), *Prawo do prywatności – współczesne wyzwania,* Warszawa 2019, s. 82 i n.; O. Karczewska, *RODO w Internecie – prawo do bycia zapomnianym,* [w:] A. Surma, E. Chodźko (red.), *Współczesne wyzwania cyfryzacji – przegląd i badania,* Lublin 2019, s. 80 i n.; P. Rutkowska, *Prawo do bycia zapomnianym w cyfrowym świecie. Wybrane zagadnienia*, „Społeczeństwo i Polityka" 2019, nr 1.

nych kontaktowych osoby prawnej”[311]. Należy przy tym zaznaczyć, że zawężenie zakresu podmiotowego prawa do bycia zapomnianym wyłącznie do osoby fizycznej nie jest jednoznaczne z tym, że w ramach wskazanej kategorii osób nie można dokonać pewnego zróżnicowania. Powyższy wniosek można wyciągnąć już nie tylko z – omówionego w poprzednim rozdziale – wyroku TS w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González,* w którym Trybunał dokonał rozróżnienia[312] „osób prywatnych od tych jednostek, które znajdują się w sferze publicznej, i w związku z tym informacje ich dotyczące stanowią wartość wyższą dla interesu ogółu niż dla jednostkowego prawa podmiotowego tych osób fizycznych”[313], ale przede wszystkim z treści art. 17 RODO, w którym określono przesłanki warunkujące korzysta-

[311] Motyw 14 RODO.

[312] Zgodnie ze wskazanym wyrokiem TSUE „art. 12 lit. b) i art. 14 akapit pierwszy lit. a) dyrektywy 95/46 należy interpretować w taki sposób, iż w ramach oceny tego, czy spełnione zostały warunki zastosowania tych przepisów, należy w szczególności przeanalizować kwestię, czy osoba, której dotyczą dane, ma prawo do tego, aby dana 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, przy czym stwierdzenie, iż takie prawo przysługuje, pozostaje bez związku z tym, czy zawarcie na tej liście wyników wyszukiwania danej informacji wyrządza szkodę tej osobie. Ponieważ osoba ta może, ze względu na przysługujące jej i przewidziane w art. 7 i 8 karty prawa podstawowe, zażądać, aby dana informacja nie była już podawana do wiadomości szerokiego kręgu odbiorców poprzez zawarcie jej na takiej liście wyników wyszukiwania, prawa te są co do zasady nadrzędne nie tylko wobec interesu gospodarczego operatora wyszukiwarki internetowej, lecz również wobec interesu, jaki ten krąg odbiorców może mieć w znalezieniu rzeczonej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby. Taka sytuacja nie ma jednak miejsca, jeśli ze szczególnych powodów, takich jak rola odgrywana przez tę osobę w życiu publicznym, należałoby uznać, że ingerencja w prawa podstawowe tej osoby jest uzasadniona nadrzędnym interesem tego kręgu odbiorców, polegającym na posiadaniu, dzięki temu zawarciu na liście, dostępu do danej informacji”.

[313] E. Michałkiewicz, E. Milczarek, *Prawo do prywatności w dobie Internetu,* „Prawo Mediów Elektronicznych” 2015, nr 2, s. 59.

nie z prawa do bycia zapomnianym oraz przesłanki wyłączające to prawo, o czym szerzej w dalszej części opracowania.

Niewątpliwie pojęcie uprawnionego ma jeszcze o wiele bardziej złożony charakter. Ze względu na to, że w praktyce przetwarzanie danych i ich upublicznianie dotyczyć będzie również osób, które nie posiadają pełnej zdolności do czynności prawnych, pojawia się bowiem kwestia ustalenia, czy i w jakim zakresie osoby takie skutecznie będą je mogły samodzielnie dochodzić[314].

W tym zakresie za właściwe widzielibyśmy odróżnienie dwóch płaszczyzn. Pierwsza dotyczyłaby sytuacji, w której osoba taka wyrażałaby zgodę na przetwarzanie jej danych przez administratora, a dotyczyłoby to czynności, które można byłoby zaliczyć do nieprzekraczających zakres czynności, tzn. takich, które mieszczą się kategorii drobnych bieżących sprawach życia codziennego (np. w zakresie akceptacji regulaminów bezpłatnego dostępu do wyszukiwarki internetowej). W tym przypadku, biorąc również pod uwagę, że mają one charakter cywilnoprawny, uznajemy za zasadne przyjęcie, iż osoba taka sama będzie mogła, powołując się na treść art. 17 RODO, żądać od administratora niezwłocznego usunięcia jej danych osobowych (art. 17 ust. 1), jak również tego, aby poinformował on innych administratorów danych, przetwarzających te dane (w ramach rozsądnych działań, w tym środków technicznych), że takie zasadne wystąpienie nastąpiło, co wiąże się również z obowiązkiem usunięcia przez nich wszelkich

[314] Oczywiście w tym zakresie uwzględniamy fakt, że w sprawach nieuregulowanych w ustawie do postępowań administracyjnych przed PUODO, o których mowa w rozdziałach 4-7 i 11 ustawy o ochronie danych osobowych, stosuje się ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, oczywiście przy uwzględnieniu postanowień art. 62 i n. ustawy o ochronie danych osobowych, w których wprowadzono modyfikacje reguł kodeksowych – zob. szerzej: P. Gorzko, *Komentarz do art. 7*, [w:] *Ustawa o ochronie danych osobowych. Przepisy wdrażające*…, s. 93-95.

łącz do tych danych, kopii tych danych osobowych lub ich replikacji (art. 17 ust. 2 RODO).

Sytuacja ta ulega jednak zmianie w razie odmowy przez administratora spełnienia żądania i zaistnienia potrzeby wystąpienia do organu ochrony danych, a być może, i sądu administracyjnego.

Pomocna w tym zakresie staje się przeprowadzona już przez sąd ocena zdolności procesowej takiej osoby w odniesieniu do realizacji konstytucyjnego prawa dostępu do informacji publicznej (art. 61 Konstytucji RP).

Sąd stwierdził – oceniając w konkretnej sprawie zdolność siedemnastolatka – że „W sprawach sądowoadministracyjnych zdolność procesową posiadają osoby fizyczne mające pełną zdolność do czynności prawnych (art. 26 § 1 P.p.s.a.)”[315]. Oznacza to, że z punktu widzenia realizacji praw w jakimkolwiek postępowaniu sądowym (tu przed sądem administracyjnym) osoba taka nie będzie mogła zostać uznana za uprawnioną (posiadającą zdolność procesową) w zakresie dochodzenia swoich praw. Nie budzi przy tym wątpliwości, że ustawa o ochronie danych osobowych nie precyzuje konkretnego wyjątku, który osobom takim gwarantowałby możliwość skutecznego realizowania praw skonkretyzowanych w RODO, w tym oczywiście prawa do bycia zapomnianym. NSA w swoim postanowieniu podkreślił wprost, że „zakres uprawnień w sferze materialnej ma decydujący wpływ na ocenę zakresu zdolności procesowej, bo jasno na to wskazuje art. 26 § 2 P.p.s.a.”[316].

[315] Postanowienie NSA z dnia 21 marca 2017 r., I OSK 2500/16.

[316] Podkreślił jednocześnie, że „Wyjątkowo dokonywanie czynności prawnych przez osoby małoletnie dopuszcza ustawa z dnia 2 kwietnia 2009 r. o obywatelstwie polskim […] przewidująca uprawnienie osoby, która ukończyła szesnasty rok życia, do wyrażania zgody na nabycie lub zrzeczenie się przez rodziców obywatelstwa polskiego, rozciągającego się na nią, jak również składania oświadczenia przez taką osobę o powrocie do obywatelstwa polskiego, jeśli jedno z jej rodziców jest obywatelem polskim, a obywatelstwo obce zostało dla niej wybrane przez rodziców po urodzeniu (art. 6 ust. 2, art. 7 ust. 1 i 2, art. 8). We wskazanych wyżej wypadkach osoby małolet-

Mając na względzie powyższe, przy uwzględnieniu zakresu i charakteru obowiązujących aktualnie w polskim porządku prawnym regulacji (przepisów prawa materialnego) nie sposób uznać, że twierdzenie, zgodnie z którym 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 (tu obejmującym postępowanie przed PUODO i sądem administracyjnym) jest błędne. Przyjąć w związku z tym trzeba, że dopóki nie zostaną wprowadzone konkretne zmiany, dopóty konieczne staje się podjęcie za małoletniego odpowiednich działań przez przedstawiciela ustawowego tak w odniesieniu wystąpienia ze skargą do krajowego organu ochrony, jak i późniejszego do sądu administracyjnego.

1.2. Podmiot zobowiązany

Zgodnie z art. 17 ust. 1 RODO adresatem wyrażonego w przepisie tym obowiązku jest administrator. Przez termin ten 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”[317]. Posiadania statusu admini-

nie będą posiadały zdolność do czynności w postępowaniu sądowoadministracyjnym, jeżeli działanie lub bezczynność organów administracji stanie się przedmiotem sądowej kontroli, co jedynie w ograniczonym zakresie dopuszcza art. 10 tej ustawy […]. Podobna regulacja występuje również w art. 8 ust. 2, 3, 4 ustawy z dnia 17 października 2008 r. o zmianie imienia i nazwiska […] przewidującym zgodę małoletniego, który ukończył trzynaście lat, na zmianę nazwiska, w przypadku gdy takiej zmiany dokonują jego rodzice”.

Istotne stało się również wskazanie przez sąd, iż osoba posiadająca ograniczoną zdolność do czynności prawnych nie dysponuje samodzielnym uprawnieniem do dokonywania czynności w sprawach z zakresu informacji publicznej, a w związku z tym „[…] wystąpienie z wnioskiem o udostępnienie informacji publicznej przez osobę małoletnią wymaga działania przedstawiciela ustawowego. W konsekwencji czego osoby te nie mają uprawnienia do samodzielnego dokonywania czynności również w postępowaniu sądowo-administracyjnym dotyczącym tego przedmiotu”, *ibidem.*

[317] Art. 4 pkt 7 RODO. Zob. na ten temat M. Jabłoński, K. Wygoda, *Praktyczne znaczenie podstawowych pojęć RODO…*, s. 9 i n.

stratora nie można zatem „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”[318]. Przymioty te – jak podkreślił Trybunał Sprawiedliwości UE – posiada operator wyszukiwarki internetowej, którego działalność polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym ich przechowywaniu i udostępnianiu internautom w sposób uporządkowany zgodnie z określonymi preferencjami, w sytuacji gdy informacje takie zawierają dane osobowe[319].

Z wyjątkiem operatorów wyszukiwarek internetowych, podmiotami zobowiązanymi do realizacji prawa do bycia zapomnianym mogą być np. „inne podmioty świadczące usługi społeczeństwa informacyjnego”[320], a także podmioty dokonujące sprzedaży towarów przez Inter-

[318] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 217.

[319] Wyrok TSUE z dnia 13 maja 2014 r. w sprawie C-131/12 *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González,* pkt 41.

[320] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 401. Por. 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 12, s. 66.

Zgodnie z art. 4 pkt 25 RODO usługa społeczeństwa informacyjnego oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady UE 2015/1535. W rozumieniu tej dyrektywy usługa społeczeństwa informacyjnego to każda usługa normalnie świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Do celów niniejszej definicji:

– „na odległość” oznacza, że usługa świadczona jest bez równoczesnej obecności stron;
– „drogą elektroniczną” oznacza, iż **usługa jest wysłana i odbierana** [podkr. M.J. i J.W.] w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (wyłącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą

net, które dostarczane są drogą tradycyjną, a nie elektroniczną – pod warunkiem, że będzie można im przyznać status administratora i znajdzie zastosowanie jedna z przesłanek, o której mowa w art. 17 ust. 1 lub przesłanki wyrażone w ust. 1 i 2 RODO. Wydaje się, że nie będą to podmioty świadczące usługi hostingowe, do których zaliczyć można serwisy społecznościowe (np. Nasza klasa[321], Facebook), ponieważ nie mają one statusu administratora „w stosunku do danych osobowych będących przedmiotem hostingu"[322]. Podmioty, o których mowa, udostępniają „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)"[323]. W związku z tym nie podejmują one 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 będących przedmiotem hostingu […]"[324]. W każdym więc przypadku cele „określane są nie przez podmiot, który faktycz-

kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych;

– „na indywidualne żądanie odbiorcy usług" oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie.

Przykładowy wykaz usług nieobjętych niniejszą definicją został określony w załączniku I dyrektywy.

[321] Zob. http://prawo.vagla.pl/node/7900 [dostęp: 10.09.2021].

[322] P. Litwiński, P. Barta, M. Kawecki, *op. cit.*, s. 401.

[323] P. Litwiński, *Hosting danych osobowych. Zagadnienia podstawowe*, „Monitor Prawniczy" 2008, 23, s. 1258.

[324] *Ibidem*, s. 1261.

nie dane przechowuje (dostawca usług hostingowych), lecz przez podmiot, który z usług hostingowych korzysta”[325].

Wobec powyższego wydaje się, że administratorem jest użytkownik korzystający z usługi hostingowej, natomiast dostawca usług hostingowych jest administratorem tylko danych osoby, korzystającej z jego usług. Na tym tle pojawia się jednak pytanie, czy użytkownik usługi hostingowej będzie mógł być uznany za administratora w świetle rozwiązań przyjętych w RODO?

Jak wynika z art. 2 ust. 2 lit. c) w związku z motywem 18 RODO, „niniejsze rozporządzenie nie ma 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 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”.

Przyjęcie wskazanego wyżej rozwiązania oznacza, że w przypadku serwisów społecznościowych służących do kontaktów zawodowo-biznesowych (np. LinkedIn) jego użytkownik w razie zamieszczenia w takim serwisie np. danych osobowych współpracowników będzie mógł być uznany za administratora. Na kwestię tę zwróciła uwagę Grupa Robocza Art. 29, podkreślając „Wśród SNS (sieciowe serwisy społecznościowe – przyp. M.J. i J.W.) obserwuje się narastającą tendencję do przechodzenia od «Web 2.0 dla zabawy» do «Web 2.0 na potrzeby zwiększenia wydajności i świadczenia usług», wskutek czego czynności niektórych użytkowników SNS mogą wykraczać poza dzia-

[325] *Ibidem.*

łania o czysto osobistym lub domowym charakterze, na przykład gdy SNS jest stosowane jako platforma współpracy w ramach stowarzyszenia lub przedsiębiorstwa. Jeżeli użytkownik SNS działa w imieniu przedsiębiorstwa lub stowarzyszenia lub wykorzystuje SNS głównie jako platformę służącą osiąganiu celów komercyjnych, politycznych lub charytatywnych, wspomniane wyłączenie nie ma zastosowania. W tym przypadku użytkownik przyjmuje pełnię obowiązków administratora danych ujawniającego dane osobowe innemu administratorowi danych (SNS) lub osobom trzecim (innym użytkownikom SNS lub potencjalnie nawet innym administratorom danych mającym dostęp do danych). W takich okolicznościach użytkownik musi uzyskać zgodę osób zainteresowanych lub wskazać inną podstawę prawną przewidzianą w dyrektywie o ochronie danych"[326], a obecnie w RODO.

Nie jest jednak przesądzone, że korzystanie z serwisu społecznościowego, które nie służy wymienionym wyżej celom będzie zawsze miało charakter osobisty lub domowy. Jak podkreśla bowiem Grupa Robocza Art. 29 „zazwyczaj dostęp do danych (danych ujętych w profilu, wpisów, opowiadań itp.) przekazanych przez użytkownika jest ograniczony do samodzielnie wybranych kontaktów. Jednakże w niektórych przypadkach użytkownicy mogą mieć wiele kontaktów z osobami trzecimi, z których nie wszystkich mogą faktycznie znać. Duża ilość kontaktów mogłaby wskazywać, że «wyłączenie do celów domowych» nie obowiązuje, a więc użytkownika można byłoby uznać za administratora danych"[327]. Idąc tym tokiem rozumowania, można byłoby także przyjąć, że wyłączenie, o którym mowa we wskazanym wcześniej art. 2 ust. 2 lit. c) w związku z motywem 18 RODO, nie będzie miało zastosowania w sytuacji, gdy użytkownik serwisu społecznościowego, zamieszczając w nim dane innych osób, zmienił usta-

[326] Grupa Robocza Art. 29, Opinia 5/2009 w sprawie portali społecznościowych przyjęta w dniu 12 czerwca 2009 r., s. 7.

[327] *Ibidem*.

wienia prywatności – na opcję publiczne (co wynika z zasady *privacy by default*) – wskutek czego stały się one dostępne dla nieograniczonej liczby osób. Niewykluczone zatem jest, że i w tej kwestii mogą pojawić się odmienne stanowiska. Naszym zdaniem upublicznienie danych przez użytkownika serwisu społecznościowego będzie mieściło się w pojęciu działalności czysto osobistej pod warunkiem, że nie będzie związane z celem zarobkowym[328].

Biorąc pod uwagę powyższe kryteria, a także orzecznictwo TSUE, warto odnieść się do wyroku z dnia 5 czerwca 2018 r. w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* przeciwko *Wirtschaftsakademie Schleswing-Holstein GmbH,* w którym Trybunał uznał – *Wirtschaftsakademie,* tj. spółkę prawa prywatnego świadczącą usługi kształcenia przy użyciu fanpage'a prowadzonego na Facebooku – za administratora. W niniejszej sprawie podmiot prowadzący fanpage'a za pomocą funkcji „Facebook Insights" udostępnionej bezpłatnie przez Facebooka uzyskał anonimowe dane statystyczne dotyczące osób odwiedzających te strony. Jak się okazało, dane tych osób gromadzone były dzięki plikom szpiegującym, tj. plikom cookies, z których każdy zawiera niepowtarzalny kod użytkownika. Pliki te pozostawały aktywne przez dwa lata (jeśli nie zostały usunięte) i zapisywane przez Facebooka na twardym dysku komputera lub innym nośniku osób odwiedzających fanpage'a. „Takie przetwarzanie danych osobowych ma w szczególności pozwolić, po pierwsze, Facebookowi na poprawę jego systemu reklam, jakie emituje on za pośrednictwem swego portalu, a po drugie, administratorowi fanpage'a na uzyskanie statystyk sporządzonych przez Facebook w oparciu o liczbę odwiedzających tę stronę, do celów zarządzania promocją jego działalności, które to statystyki umożliwiają temu administratorowi poznanie na przykład profilu odwiedzających, którzy oceniają jego fanpage'a lub

[328] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 149.

korzystają z jego aplikacji, tak aby mógł im zaproponować bardziej odpowiednie treści i rozwinąć funkcje, które mogłyby ich zainteresować w większym stopniu”[329]. Należy przy tym zaznaczyć, że „utworzenie fanpage’a na Facebooku wiąże się z podjęciem przez jego administratora działań polegających na ustaleniu parametrów zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakresie zarządzania lub promocji jego działalności, co wpływa na przetwarzanie danych osobowych na potrzeby statystyk sporządzonych na podstawie liczby odwiedzających fanpage’a. Ów administrator może za pomocą filtrów udostępnionych przez Facebook zdefiniować kryteria, na podstawie których statystyki te muszą być sporządzane, a nawet określić kategorie osób, których dane osobowe będą wykorzystywane przez Facebook. W konsekwencji administrator fanpage’a prowadzonego na Facebooku przyczynia się do przetwarzania danych osobowych osób odwiedzających jego stronę. W szczególności administrator fanpage’a może zwrócić się o udzielenie – a zatem o przetworzenie – danych demograficznych dotyczących jego użytkowników docelowych, a w szczególności tendencji w zakresie wieku, płci, stanu cywilnego i statusu zawodowego; informacji na temat stylu życia i zainteresowań jego użytkowników docelowych, a także informacji dotyczących zakupów i zachowań w zakresie zakupów w sieci osób odwiedzających jego stronę, kategorii produktów lub usług, które najbardziej ich interesują, jak również danych geograficznych, które pozwalają administratorowi fanpage’a ustalić, gdzie należy przeprowadzić specjalne promocje lub zorganizować wydarzenia, a bardziej ogólnie, jak najlepiej ukierunkować swą ofertę informacyjną”[330]. I choć statystyki dotyczące osób odwiedzających fanpage’a sporządzone

[329] Wyrok TSUE z dnia 5 czerwca 2018 r. w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* przeciwko *Wirtschaftsakademie Schleswing-Holstein GmbH*.

[330] *Ibidem.*

przez Facebooka są w zanonimizowanej formie przekazywane jedynie administratorowi fanpage'a, to nie zmienia to faktu, że administrator fanpage'a – w tym przypadku *Wirtschaftsakademie* – „uczestniczy, podejmując działania polegające na ustaleniu parametrów zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakresie zarządzania lub promocji jego działalności, w określeniu celów i sposobów przetwarzania danych osobowych osób odwiedzających jego fanpage'a"[331]. Z tego względu w niniejszym przypadku Trybunał uznał, że administratorem danych w rozumieniu art. 2 lit. d) dyrektywy 95/46 jest administrator fanpage'a. Wyrok ten, mimo że został wydany na tle dyrektywy 95/46, pozostaje aktualny, ponieważ definicja administratora przyjęta w art. 4 pkt 7 RODO „nie uległa istotnej zmianie w relacji do definicji"[332] administratora danych, która obowiązywała pod rządami dyrektywy 95/46.

Jak wynika z powyższych ustaleń, określenie podmiotu zobowiązanego do realizacji prawa do bycia zapomnianym nie jest wcale zadaniem łatwym, zwłaszcza gdy idzie o działalność portali społecznościowych. Słusznie zwraca się więc uwagę w doktrynie zagranicznej, że RODO będące przedmiotem wielu dyskusji, niektóre pytania pozostawia bez odpowiedzi. Na przykład nie jest jasne, czy portale społecznościowe takie jak Facebook i Twitter uznaje się za administratorów i czy zobowiązane one są do usunięcia treści zamieszczonych przez użytkownika na temat innej osoby, gdy wystąpi ona z żądaniem usunięcia dotyczących jej danych[333]. Naszym zdaniem bezsprzeczne jest, że portale społecznościowe są administratorami danych osobowych ich użytkowników. Wątpliwości pojawiają się natomiast, gdy idzie o dane osób, które zostały umieszczone przez użytkownika portalu w ramach

[331] *Ibidem.*

[332] M. Górski, *„Właściciel" fanpage'a na portalu społecznościowym jako administrator,* „ABI Expert" 2018, nr 3, s. 52.

[333] Zob. http://communication.oxfordre.com/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189 [dostęp: 10.09.2021].

czynności o czysto osobistym lub domowych charakterze. W takim przypadku uważamy, że portale społecznościowe, tj. Facebook i Twitter nie mają statusu administratora, a to oznacza, że w świetle art. 14 ustawy o świadczeniu usług drogą elektroniczną[334], wskazane w przepisie tym wyłączenie ma zastosowanie względem tych podmiotów. Jak się okazuje, problem z prawidłowym określeniem administratora dotyczy także sfery publicznej. Mając bowiem na względzie treść art. 4 pkt 7 RODO należy pamiętać, że „cele przetwarzania w sferze publicznej wynikają bezpośrednio z przepisów prawa, zgodnie z regułą działania administracji publicznej na podstawie i w graniach prawa (zasada legalizmu). Trudno zatem przyjąć, że organy i podmioty publiczne samodzielnie oraz w każdej sytuacji wskazują (czy ustalają) cele przetwarzania"[335]. Zasadnicza różnica w przyznaniu statusu administratora w sferze publicznej przejawia się więc w samodzielnym decydowaniu przez podmiot o sposobach przetwarzania m.in. o środkach technicznych i organizacyjnych wiążących się z przetwarzaniem danych. Nato-

[334] Art. 14 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2017 r. poz. 1219 ze zm.) stanowi:

Ust. 1. 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.

Ust. 2. Usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych.

Ust. 3. Usługodawca, który uzyskał wiarygodną wiadomość o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych, jeżeli niezwłocznie zawiadomił usługobiorcę o zamiarze uniemożliwienia do nich dostępu.

Ust. 4. Przepisów ust. 1-3 nie stosuje się, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów o ochronie konkurencji i konsumentów.

[335] M. Jabłoński, K. Wygoda, *Praktyczne znaczenie podstawowych pojęć RODO*…, s. 11.

miast cele powinny być określone przez ustawodawcę. Warto przy tym zwrócić uwagę, że art. 4 pkt 7 RODO dopuszcza, aby przepisy państwa członkowskiego określały wprost administratora lub konkretne kryteria jego wyznaczenia. Praktyka pokazuje, że polski ustawodawca skorzystał z pierwszego rozwiązania co nie oznacza rozwiania wątpliwości pojawiających się na tym tle. W doktrynie dostrzega się potrzebę ustalenia konkretnych kryteriów co do określenia statusu administratora[336], co z pewnością nie jest zadaniem łatwym. Nie budzi jednak wątpliwości, że przyjęcie modelowego schematu ustalenia statusu administratora stanowiłoby duże ułatwienie w praktyce stosowania przepisów z zakresu ochrony danych osobowych.

1.3. Zakres i charakter uprawnień

Uwzględniając treść art. 17 RODO, jesteśmy w stanie wskazać, że w praktyce mamy do czynienia z dwoma uprawnieniami, które realizować będzie osoba, której dane dotyczą, a które definiować będą treść prawa do bycia zapomnianym.

Pierwszym z nich jest żądanie „niezwłocznego usunięcia dotyczących jej danych osobowych" (art. 17 ust. 1), drugim zaś w razie upublicznienia jej danych przez administratora żądanie, aby obok ich usunięcia – biorąc pod uwagę dostępną technologię i koszt realizacji – podjął rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że uprawniony zasadnie żąda, by usunęli oni wszelkie łącza do tych danych, ich kopie lub replikacje (art. 17 ust. 2)[337].

[336] *Ibidem*, s. 11 i n.

[337] Kopia – duplikaty plików tworzone na różnych nośnikach w celu ochrony danych, http://www.i-slownik.pl/157,kopia-bezpieczenstwa-lub-kopia-zapasowa-backup/ [dostęp: 5.10.2021]. Natomiast „Replikacja danych jest procesem kopiowania informacji pomiędzy różnymi serwerami baz danych, w celu utrzymania ich spójności. Można powiedzieć, że jest to tworzenie kopii bezpieczeństwa, zaawansowany back up danych, ich archiwizacja, w celu stworzenia efektywnie działającego, zdublowanego systemu

Nie budzi wątpliwości, że zarówno pierwsze, jak i drugie uprawnienie jest bardzo istotne dla osoby, której dane dotyczą. Należy jednak mieć na uwadze, że o ile w ramach uprawnienia, o którym mowa w art. 17 ust. 1 RODO, administrator kategorycznie musi ustosunkować się do żądania podmiotu danych, tj. usunąć bądź odmówić usunięcia dotyczących danej osoby danych, to w przypadku uprawnienia wynikającego z ust. 2 wskazanego wyżej przepisu prawodawca unijny nie nałożył na administratora bezwzględnego obowiązku poinformowania administratorów o żądaniu przez osobę, której dane dotyczą usunięcia dotyczących jej danych, „ponieważ z punktu widzenia technicznego może okazać się to niezwykle trudne, a niekiedy nawet niemożliwe”[338]. Wątpliwości, jakie mogą pojawić się jednak przy realizacji tych uprawnień, związane są z użytymi w art. 17 ust. 1 i 2 RODO zwrotami niedookreślonymi. Jak wynika z treści art. 17 ust. 1 RODO, „Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe […]”, co w praktyce

informatycznego firmy. W przypadku awarii systemu głównego uruchomi się kopia zapasowa, czyli powielony w wyniku replikacji system”, https://www.iphbms.pl/replikacja-danych/ [dostęp: 5.10.2021].

W najprostszym ujęciu: Łącze – to odnośnik do danych np. hiperłącze.

Słusznie zauważa Paweł Fajgielski, że „wątpliwości budzi określenie «replikacje danych» i jego relacja do pojęcia «kopie danych», gdyż *prima facie* wydaje się, że są to określenia tożsame. Jednak w znaczeniu technicznym pojęcia te są od siebie odróżniane. O kopii danych mówimy zwykle w odniesieniu do dokładnego odwzorowania danych, przy czym po sporządzeniu kopii (np. kopii zapasowej) jest ona niezależna od skopiowanych danych, które mogą ulec zmianie bez wpływu na dane, które zostały powielone (skopiowane). Replikacja w znaczeniu technicznym oznacza podwajanie – tworzenie dokładnej kopii danych pomiędzy miejscem źródłowym składowania danych a docelowym miejscem, do którego one trafiają, i stanowi mechanizm wykorzystywany do poprawy bezpieczeństwa przetwarzanych danych. Prawodawca wymaga usunięcia zarówno danych, jak i odnośników do danych, kopii danych, a także replikacji danych, a więc wymaga usunięcia wszystkich danych i informacji, które pozwalają na dotarcie do treści danych”, P. Fajgielski, *Ogólne rozporządzenie…,* s. 274-275.

[338] P. Fajgielski, *Komentarz do art. 17,* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Lex.

nie będzie oznaczać natychmiastowej realizacji przez administratora przedmiotowego żądania, to znaczy w tym samym czasie, w którym osoba je wniosła. Spełnienie żądania „niezwłocznie", tj. bez zbędnej zwłoki, wydaje się, że należy oceniać w ramach okoliczności charakterystycznych dla danego przypadku. Trzeba zatem mieć na uwadze czas potrzebny administratorowi do należytej realizacji konkretnego żądania, który określony został w art. 12 ust. 3 RODO. Mowa w nim o terminie miesiąca od otrzymania żądania, ale w razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Wówczas w terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Mając powyższe na względzie, nie budzi wątpliwości, że pomimo posłużenia się przez prawodawcę unijnego w art. 17 ust. 1 RODO zwrotem niedookreślonym, rozpatrzenie wniesionego przez osobę, której dane dotyczą, żądania musi obligatoryjnie nastąpić. Realizacja natomiast uprawnienia wynikającego z art. 17 ust. 2 RODO jest bardziej problematyczna, ponieważ uzależniona jest od podjęcia przez administratora rozsądnych działań, w tym środków technicznych, za pomocą których administratorzy zostaną poinformowani o żądaniu osoby, której dane dotyczą. Przy czym działania, o których mowa wymagają wzięcia pod uwagę dostępnej technologii i kosztów ich realizacji, co świadczy o tym, że zobowiązanie ciążące na administratorze nie ma charakteru „rezultatu, a wyłącznie starannego działania"[339]. W praktyce dla osoby, której dane dotyczą, oznacza to, że jej żądanie w ramach uprawnienia z art. 17 ust. 2 RODO uzależnione jest od stopnia rzetelności administratora.

Pojęcie „rozsądnych działań" pojawia się w wielu różnych regulacjach prawnych i rozstrzygnięć, także międzynarodowych organów

[339] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 407.

ochrony prawnej[340]. Nie budzi wątpliwości, że jest to sformułowanie w istotnym zakresie odwołujące się do anglosaskiej kultury prawnej[341]. W polskim systemie prawa, w zasadzie, odwoływanie się do tego pojęcia nie jest praktykowane. Najlepszym tego przykładem niech będzie dyskusja prowadzona w zakresie implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego *know-how* i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskaniem, wykorzystaniem i ujawnianiem[342]. W trakcie przygotowywania odpowiednich rozwiązań wskazywano, że „posługuje się terminologią («rozsądne działania»), która w tym kontekście nie jest używana w języku polskich aktów normatywnych – stanowiących raczej o działaniach z należytą starannością, czy starannością wymaganą w stosunkach danego rodzaju (art. 355 § 1 i 2 k.c.). W związku z tym projekt, zamiast pojęcia «rozsądnych działań», posługuje się pojęciem działań, które «przy zachowaniu należytej staranności» uprawniony podjął (powinien podjąć) w celu ochrony informacji stanowiących tajemnicę

[340] Wyrok *Fernandes de Oliveira v. Portugalia, 31.01.2019 r., Wielka Izba, skarga nr 78103/14*; Konwencja Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów z dnia 11 kwietnia 1997 r., Dz. U. z 1997 r. Nr 45, poz. 286; dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego *know-how* i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskaniem, wykorzystaniem i ujawnianiem.

[341] Dobrym przykładem jest także ustawa z dnia 17 czerwca 2004 r. o skardze na naruszenie prawa strony do rozpoznania sprawy w postępowaniu sądowym bez nieuzasadnionej zwłoki, t.j. Dz. U. z 2018 r. poz. 75 ze zm., którego pierwotny projekt posługiwał się tytułem: ustawa o skardze na naruszenie prawa strony do rozpoznania w rozsądnym terminie sprawy w postępowaniu sądowym, druk nr 2256 z 17 listopada 2003 r., http://orka.sejm.gov.pl/proc4.nsf/opisy/2256.htm [dostęp: 5.10.2021], a który został ostatecznie dostosowany do terminologii bardziej rozpoznawalnej w praktyce polskiego prawodawcy.

[342] Dz. Urz. UE L 157/1 z 15.06.2016 r.

przedsiębiorstwa przed ich pozyskaniem, ujawnieniem lub wykorzystaniem przez osobę nieuprawnioną”[343].

Na gruncie stosowania RODO taka zamiana nie ma miejsca, a więc konieczne staje się interpretowanie zwrotu „rozsądne działania, w tym środki techniczne” autonomicznie w odniesieniu do charakteru i specyfiki rozwiązań zdefiniowanych przez ustawodawcę unijnego, a które konkretyzowane będą w praktyce działania administratorów, PUODO i sądów rozstrzygających. Nie budzi przy tym wątpliwości, że pojęcie „rozsądnych działań” jest trudniejsze do oceny przez sąd, niż pojęcie działań „niezbędnych”, czy podjętych z zachowaniem „należytej staranności”. Postulować należy więc przyjęcie takiego sposobu ich identyfikacji, które opierając się na znanym naszemu porządkowi prawnemu kryterium „niezbędności” i „należytej staranności” nie będą przybierały postaci działań, które jedynie potencjalnie mogłyby zostać podjęte i zupełnie pomijają np. ich koszty, czy też faktyczne możliwości techniczne, którymi dysponuje. Ocena więc zawsze musi dotyczyć konkretnego przypadku. Nie budzi jednak wątpliwości, że „rozsądne działania” administratora należy rozpatrywać pod kątem racjonalności (możliwości) podejmowanych przedsięwzięć, zarówno od strony ewentualnego powodzenia podejmowanej interakcji, jak i zaangażowanych w jej przeprowadzenie osób, środków i ostatecznie kosztów.

W tym celu administrator powinien wdrożyć odpowiednie procedury wewnętrzne dotyczące zdefiniowania zarówno zakresu i charakteru działań, które podejmuje on w celu realizacji praw, o którym mowa w art. 17 ust. 1 i 2 RODO, jak i osób (pracowników), które za ich wykonanie będą odpowiedzialne. Administrator powinien więc być zdolny do określenia, co ma w jego organizacji kluczowe znaczenie dla wykazania podjęcia rzeczywistych działań, mających na celu wywiązanie się

[343] Druk nr 2549 i dołączone uzasadnienie, a także prace w parlamencie, http://orka.sejm.gov.pl/Druki8ka.nsf/0/624D957922830811C1258291003ED53B/%24File/2549.pdf [dostęp: 05.10.2021]

z tego obowiązku, jakie działania podjął wcześniej, niejako przygotowując się na tego typu żądania, jakie podjął w następstwie uznania ich za zasadne (po wpłynięciu) i wreszcie, jakie w tym zakresie wykorzystał środki (być może również takie, które niezwłocznie wdrożył w celu jak najpełniejszego wywiązania się z tego obowiązku).

Kwestia rozsądnych działań będzie mogła być jednocześnie weryfikowana z perspektywy innego wzorca oceny, jakim potencjalnie może być „brak rozsądnego usprawiedliwienia" dla niepodjęcia określonych działań przez administratora. W takim ujęciu możliwe jest określenie tego, co administrator mógł zrobić, ale wiedząc, że trzeba w tym celu ponieść określone koszty, uznał bezpodstawnie, że nie jest to wymagane, ponieważ przekracza granicę „działań rozsądnych". Ta perspektywa będzie podlegała rozłożonemu w czasie obiektywizowaniu, co musi wiązać się z ukształtowaniem praktyki zarówno w kontekście rozstrzygnięć PUODO, jak i sądów administracyjnych. Ocena w tym zakresie będzie polegała – przynajmniej takie jest nasze zdanie – na zweryfikowaniu tego, czy administrator podjął jedynie typowe działania, czy też jest w stanie wykazać, że ich charakter wykracza poza tak zdefiniowaną sferę. Uważamy, że powinniśmy w tym właśnie zakresie odwoływać się pomocniczo do kryterium „realnie istniejących okoliczności"[344], charakteryzujących ocenę możliwości i działań podjętych przez administratora w konkretnym przypadku, w ramach „dostępnych środków", czyli takich, które są osiągalne w danej sytuacji (nie są trudne lub niemożliwe do zastosowania i nie wymagają nadmiernego trudu, kosztów i starań).

Nie budzi jednak wątpliwości, że „rozsądne działania" należy powiązać z definiowaniem wzorca tzw. rozsądnego administratora, czyli takiego, który nie podejmuje wyłącznie pozornych lub obiektywnie weryfikowalnych minimalistycznych działań, ale włączywszy to w ogólny

[344] Por. wyrok SN z dnia 19 maja 2005 r., V CK 648/04.

kontekst sytuacji i oczekiwań występującego na podstawie art. 17 ust. 2 RODO, jest podmiotem, który z łatwością może wykazać, że podjął takie działania, które były odpowiednie i możliwe do wykonania.

Bez wątpienia definiowanie testów „rozsądnego administratora" i „rozsądnych działań" jest procesem długotrwałym, rozłożonym w czasie i zostanie skonkretyzowane ostatecznie dopiero przez orzecznictwo sądowe. Przyjąć należy, że kryteria weryfikacji nie mogą być kształtowane „biegunowo" jako wyznacznik działań minimalistycznych oraz maksymalnie dostępnych. Przyjąć należy zasadę oceny każdego przypadku z osobna i dopiero całościowa jego analiza powinna prowadzić do uznania, czy administrator rzeczywiście wypełnił ciążący na nim obowiązek, co ma przecież znaczenie także z perspektywy skutków wskazanych w art. 82 i 83 RODO.

Mając powyższe na względzie, nie budzi wątpliwości, że wystąpienie przez osobę, której dane dotyczą, z żądaniem usunięcia dotyczących jej danych czy to na mocy art. 17 ust. 1, czy ust. 1 i 2, wymaga od administratora podjęcia należytych działań. Na tle tych przepisów to właśnie administrator jest odpowiedzialny za „usunięcie danych osobowych, które sam przetwarza, oraz za należyte zrealizowanie obowiązku informacyjnego względem pozostałych administratorów poprzez podjęcie racjonalnych i realnych działań. Administrator nie będzie jednak w żadnym przypadku odpowiedzialny za to, czy oraz w jaki sposób zawiadomieni przez niego administratorzy usuną dane objęte żądaniem. Podmioty te natomiast będą ponosić odpowiedzialność w zakresie, w jakim nie uczyniły zadość żądaniu usunięciu danych"[345].

[345] B. Fischer, *Prawo do usunięcia danych,* [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą, na podstawie RODO,* Wrocław 2017, s. 216.

2. Przesłanki warunkujące korzystanie z prawa do bycia zapomnianym

Prawo do bycia zapomnianym uregulowane zostało w art. 17 ust. 1 i 2 RODO. W ustępie pierwszym prawodawca unijny wymienił katalog zamknięty sytuacji, w których osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć te dane. Następuje to, gdy:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) 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;
c) 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;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

W ustępie drugim zaś prawodawca unijny zobowiązał administratora, który upublicznił dane osobowe, do poinformowania administratorów przetwarzających te dane, że osoba, której one dotyczą, żąda, by usunięte zostały wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

W praktyce mamy tu więc do czynienia z dwoma uprawnieniami, które realizować będzie osoba, której dane dotyczą.

Pierwszym jest żądanie „niezwłocznego usunięcia dotyczących jej danych osobowych", drugim zaś w razie upublicznienia jej danych przez administratora żądanie, aby obok ich usunięcia – biorąc pod uwagę dostępną technologię i koszt realizacji – podjął rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że uprawniony, zasadnie żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, ich kopie lub replikacje.

2.1. Przesłanka „wygaśnięcia" celu przetwarzania danych

Jedną z zasad dotyczących przetwarzania danych osobowych[346] jest zasada czasowego ich przechowywania wyrażona w art. 5 ust. 1 lit. e) RODO. Istotą tej zasady jest przechowywanie danych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez czas nie dłuższy, niż jest to potrzebne do celów, dla których są one przetwarzane. Prawodawca unijny dopuszcza jednak możliwość przechowywania ich przez okres dłuższy wyłącznie do celów archiwalnych w interesie publicznym, badań naukowych lub historycznych lub celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą.

Mając na względzie powyższą zasadę, należy podkreślić, że związane z nią jest prawo do bycia zapomnianym, a dokładnie przesłanka określona w art. 17 ust. 1 lit. a). Przepis ten statuuje bowiem prawo żądania od administratora usunięcia danych, jeżeli nie są już niezbędne do celów, w których zostały zebrane lub następnie przetwarzane. „Co do zasady więc to sam administrator danych, nie czekając na żądanie osoby, której dane dotyczą, powinien przestrzegać zasady ogranicze-

[346] Na temat zasad dotyczących przetwarzania danych osobowych zob. D. Dyjak, *Zasady podstawowe przetwarzania danych osobowych w świetle RODO,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *op. cit.,* s. 45 i n.

nia przetwarzania danych osobowych”[347], bowiem zarówno ona, jak i inne zasady, o których mowa w art. 5 RODO, mają nadrzędną moc „w stosunku do pozostałych przepisów o ochronie danych”[348]. Wyznaczają one obowiązki ciążące na administratorze, za naruszenie których przewidziano administracyjne kary pieniężne, o których piszemy w dalszej części opracowania.

Jak wynika z motywu 65, intencją prawodawcy unijnego jest zapewnienie każdej osobie fizycznej prawa do bycia zapomnianym, jeżeli zatrzymanie dotyczących jej danych narusza rozwiązania przyjęte w RODO, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. Prawo to może budzić jednak pewne wątpliwości, zwłaszcza gdy idzie o wskazaną wyżej przesłankę wyrażoną w art. 17 ust. 1 lit. a), bowiem pojawia się pytanie, czy osoba, której dane dotyczą, dysponuje wiedzą na temat tego, że jej dane osobowe są zbędne do celów, w których zostały zebrane – „poza przypadkami oczywistymi (np. likwidacja konta na portalu społecznościowym)?”[349]. Na pewno nie dla każdego „uzyskanie takiego stanu wiedzy”[350] będzie łatwe i zrozumiałe. Wobec tego, w sytuacji, gdy dana osoba zdecyduje się zawrzeć umowę ze sprzedawcą przez Internet (np. sprzedaż zabawek *on-line*), do której sfinalizowania konieczne jest podanie niezbędnych danych, to po otrzymaniu zamówionego przez nią towaru, nie będzie ona mogła ubiegać się o realizację prawa do bycia zapomnianym, ponieważ jej dane są niezbędne do celu realizacji umowy. Z uwa-

[347] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 402.

[348] P. Drobek, *Komentarz do art. 5 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 324.

[349] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 402. Por. decyzja PUODO z dnia 10 lutego 2020 r., ZKE.440.36.2019 nakazująca spełnienie obowiązku informacyjnego oraz usunięcie danych pozyskanych w związku z założeniem konta w serwisie. Decyzja PUODO z dnia 11 czerwca 2019 r., ZSZZS.440.592.2018 nakazująca usunięcie danych osobowych Skarżącej w zakresie imienia i nazwiska z zarządzenia Kuratora Oświaty, https://uodo.gov.pl/pl/p/decyzje [dostęp: 5.10.2021].

[350] *Ibidem.*

gi na rękojmię za wady fizyczne towaru, administrator – w tym przypadku sprzedawca – może przetwarzać dane osobowe klienta i to nie tylko na czas trwania tego uprawnienia, ale także i po jego upływie. Podstawą do przetwarzania danych także po upływie terminu rękojmi jest wywiązanie się sprzedawcy (administratora) z ciążącego na nim obowiązku prawnego – np. archiwizacji faktur wynikającej z przepisów podatkowych – o czym przesądza art. 17 ust. 3 lit. b) RODO. To z kolei oznacza, że osoba, której dane dotyczą, nie będzie mogła powołać się na prawo do bycia zapomnianym w zakresie, w jakim przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator.

2.2. Przesłanka wycofania zgody

Nie ulega wątpliwości, że przetwarzanie danych zgodnie z prawem następuje na podstawie zgody osoby, której dane dotyczą, lub na innej podstawie prawnej. W przypadku zgody przyjęto, że musi być ona „wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. […]. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczą”[351]. Z wyrażeniem zgody w powyższym ujęciu będziemy mieli do czynienia np. w razie przystąpienia do programu lojalnościowego lub zaznaczenia okienka podczas przeglądania strony

[351] Motyw 32 RODO.

internetowej z klauzulą wyrażenia zgody „na przesyłanie informacji handlowych w zamian za otrzymanie zniżki”[352] lub dostęp do bezpłatnych czasopism.

„Z przetwarzaniem danych osobowych w oparciu o przesłankę zgody skorelowane są niektóre uprawnienia podmiotów danych”[353], takie jak np. prawo do bycia zapomnianym. Mowa tu o art. 17 ust. 1 lit. b) RODO, z którego treści wynika, że prawodawca unijny uzależnił realizację prawa do bycia zapomnianym od wycofania przez osobę, której dane dotyczą, zgody, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) i braku innej podstawy prawnej przetwarzania. Wobec tego, gdy jedyną podstawą przetwarzania danych zwykłych jest zgoda, a w przypadku danych szczególnej kategorii zgoda wyraźna[354], osoba, której dane dotyczą, może żądać od administratora ich usunięcia dopiero po jej wycofaniu.

[352] D. Lubasz, *Komentarz do art. 4 pkt 25 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 248.

[353] D. Lubasz, *Komentarz do art. 6 ust. 1 lit. a) RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 357.

[354] „Termin «wyraźna» odnosi się do sposobu wyrażenia zgody przez osobę, której dane dotyczą. Oznacza to, że osoba, której dane dotyczą, musi złożyć w sposób wyraźny oświadczenie o wyrażeniu zgody. Oczywistym sposobem zapewnienia, aby zgoda była wyraźna, byłoby jej wyraźne potwierdzenie w pisemnym oświadczeniu. W stosowanych przypadkach administrator mógłby zapewnić podpisanie pisemnego oświadczenia przez osobę, której dane dotyczą, aby rozwiać wszelkie możliwe wątpliwości i zapobiec możliwemu brakowi dowodów w przyszłości. Takie podpisane oświadczenie nie jest jednak jedynym sposobem uzyskania wyraźnej zgody i nie można stwierdzić, iż w RODO przewidziano obowiązek uzyskania pisemnych i podpisanych oświadczeń we wszystkich okolicznościach, w których wymagane jest uzyskanie ważnej wyraźnej zgody. Na przykład w kontekście cyfrowym lub online osoba, której dane dotyczą, może być w stanie złożyć wymagane oświadczenie przez wypełnienie formularza elektronicznego, wysyłanie wiadomości e-mail, przesyłanie zeskanowanego dokumentu opatrzonego podpisem osoby, której dane dotyczą, lub złożenia podpisu elektronicznego. W teorii wykorzystanie oświadczeń ustnych również może zostać uznane za wystarczająco wyraźny sposób uzyskania ważnej wyraźnej zgody, jednak administratorowi może być trudno udowodnić, że spełniono wszystkie przesłanki ważnej wyraźnej zgody w chwili, gdy przyjmowano oświadczenie. […]. Innym sposobem upewnienia się, że wyraźna zgoda jest ważna, jest dwuetapowa weryfikacja zgody. Na

Należy jednak podkreślić, że z uwagi na zasadę legalności przetwarzania wyrażoną w art. 5 ust. 1 lit. a) RODO, której doprecyzowaniem jest art. 6 i art. 9 ust. 2, administrator w przypadku cofnięcia przez osobę, której dane dotyczą, zgody na przetwarzanie jej danych powinien te dane „usunąć albo je zanonimizować”[355], jeżeli nie ma innej podstawy prawnej przetwarzania, nie czekając, aż osoba ta wystąpi z żądaniem ich usunięcia (prawo do bycia zapomnianym). Należy jednak wziąć pod uwagę, że w sytuacji, gdy „zgoda została udzielona, administrator danych osobowych ma uzasadniony interes w tym, aby przechowywać dane o udzieleniu zgody, o czynnościach podjętych na podstawie zgody oraz dowody na nie, dla celu obrony przed roszczeniami w szczególności roszczeniami opartymi na twierdzeniu, że zgoda nigdy nie została udzielona. […]. Cofnięcie zgody jest przesłanką do żądania usunięcia swoich danych, ale dopiero po wygaśnięciu okresu przedawnienia roszczeń związanych z działaniami realizowanymi na podstawie zgody”[356].

Mając powyższe na względzie, nie ulega wątpliwości, że w praktyce realizacja przedmiotowego żądania powinna być skierowana do administratorów ze sfery prywatnej, bowiem przetwarzanie danych osobowych oparte na przesłance zgody w sferze publicznej może

przykład osoba, której dane dotyczą, otrzymuje wiadomość e-mail z zawiadomieniem o tym, że administrator danych zamierza przetwarzać rejestr zawierający dane medyczne. Administrator wyjaśnia w wiadomości e-mail, że prosi o zgodę na wykorzystanie określonego zestawu informacji w konkretnym celu. Jeżeli osoba, której dane dotyczą, zgadza się na wykorzystanie tych danych, administrator prosi ją o odpowiedź w formie wiadomości e-mail zawierającej oświadczenie «Wyrażam zgodę». Po wysłaniu odpowiedzi osoba, której dane dotyczą, otrzymuje link weryfikacyjny, który należy kliknąć lub wiadomość SMS z kodem weryfikacyjnym w celu potwierdzenia zgody”, wytyczne EROD 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, przyjęte 4 maja 2020 r.

[355] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 402.

[356] M. Gawroński, K. Kunda, *Prawo do usunięcia danych, prawo do bycia zapomnianym (art. 17 RODO),* [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami,* Warszawa 2018, s. 244.

mieć miejsce w wyjątkowych sytuacjach, np. w celu przygotowania newslettera[357].

2.3. Przesłanka wniesienia sprzeciwu

Zgodnie z art. 17 ust. 1 lit. c) RODO, osoba, której dane dotyczą, ma prawo żądania od administratora usunięcia dotyczących jej danych, jeżeli 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. Jak wynika z treści art. 21 ust. 1, podstawą wniesienia sprzeciwu mogą być przyczyny związane ze szczególną sytuacją osoby, której dane dotyczą, gdy celem przetwarzanie jest:

- wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowanej władzy publicznej powierzonej administratorowi[358] (art. 6 ust. 1 lit. e) RODO) lub
- realizacja prawnie uzasadnionych interesów administratora lub strony trzeciej[359] (art. 6 ust. 1 lit. f) RODO),

[357] Na temat zgody jako przesłanki przetwarzania danych przez podmioty publiczne zob. M. Jabłoński, K. Wygoda, *Legalność pozyskiwania…*, s. 95 i n.

[358] W tym miejscu warto wspomnieć, że „Prawo Unii lub prawo państwa członkowskiego powinno określać […] czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ władzy publicznej czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, na przykład zrzeszenie zawodowe, jeżeli uzasadnia to interes publiczny, w tym cele zdrowotne, takie jak zdrowie publiczne, ochrona socjalna oraz zarządzenie usługami opieki zdrowotnej", motyw 45 RODO. Na temat kryterium zadania publicznego zob. G. Sibiga, *Kryterium „zadania publicznego" w ustawie z 10.5.2018 r. o ochronie danych osobowych oraz jego konsekwencje dla wykonywania obowiązków administratora oraz realizacji praw osoby, której dane dotyczą (dodatek MoP 22/2018),* „Monitor Prawniczy" 2018, nr 22/, Legalis.

[359] Zgodnie z art. 4 pkt 10 RODO, „strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

w tym profilowanie. Ze szczególną sytuacją osoby, która wniosła sprzeciw wobec przetwarzania opartego na drugiej z wymienionych przesłanek, będziemy mieli do czynienia, gdy informacje na jej temat indeksowane przez wyszukiwarkę internetową stanowią pomówienie, przez co wyrządzają tej osobie szkodę[360]. Obowiązek uwzględnienia jednak sprzeciwu i usunięcia danych przez administratora uzależniony jest od wyważenia, „czy rzeczywiście sytuacja, w której znajduje się wnioskodawca, wyróżnia się na tle innych, a także czy nie występują prawnie uzasadnione podstawy przetwarzania nadrzędne wobec prawa do sprzeciwu i interesów wnioskodawcy”[361]. We wskazanym wyżej przykładzie wydaje się, że wszystkie okoliczności zachodzą.

Wymieniona powyżej przesłanka odnosząca się do realizacji prawnie uzasadnionych interesów administratora jest bardzo pojemna,

[360] EROD w wytycznych 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO (część 1), wersja 2.0, przyjętych 7 lipca 2020 r., zwraca uwagę, że „szczególna sytuacja osoby, której dane dotyczą, będzie leżała u podstaw żądania usunięcia z listy wyników wyszukiwania (na przykład wyniki wyszukiwania przynoszą szkodę osobie, której dane dotyczą, gdy ubiega się ona o pracę, lub niszczą jej reputację w życiu publicznym) i zostanie ona uwzględniona przy ustalaniu równowagi między prawami osobistymi i prawem do informacji, poza zwykłymi kryteriami służącymi rozpatrywaniu żądań o usunięcie z listy wyników wyszukiwania, takimi jak:

- osoba nie pełni żadnej roli w życiu publicznym;
- informacje, których dotyczy żądanie, nie są związane z jej życiem zawodowym, lecz mają wpływ na jej prywatność;
- informacje stanowią nawoływanie do nienawiści, pomówienie, zniesławienie w formie pisemnej lub podobne przestępstwo w obszarze wypowiedzi skierowanych przeciwko niej uznane za takie na podstawie orzeczenia sądowego;
- dane wydają się być zweryfikowanymi faktami, lecz w rzeczywistości są nieprawidłowe;
- dane odnoszą się do stosunkowo nieznacznego wykroczenia, które miało miejsce dawno temu i jest powodem uprzedzeń względem osoby, której dane dotyczą”.

[361] M. Krzysztofek, *Ochrona danych osobowych…*, s. 159.

o czym świadczą motywy RODO[362]. Obejmuje ona m.in. przetwarzanie danych osobowych do celów marketingu bezpośredniego[363]. Przetwarzanie we wskazanym celu może jednak wynikać nie tylko z art. 6 ust. 1 lit. f) RODO. Nic nie stoi bowiem na przeszkodzie, aby oparte ono zostało na przesłance zgody wyrażonej w art. 6 ust. 1 lit. a) RODO. Należy jednak pamiętać, że „niezależnie od podstawy prawnej przetwarzania danych, którą w przypadku marketingu bezpośredniego może być art. 6 ust. 1 lit. f) RODO, pewne formy (sposoby) komunikacji będą wymagały uzyskania dodatkowej zgody od ich adresata. Dotyczy to:

– wysyłania informacji o charakterze marketingowym na adres e-mail bądź wiadomości SMS o takim charakterze na numer telefonu (art. 10 ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[364] – przyp. M.J. i J.W.);
– wszelkich form wykorzystania numeru telefonu w celach marketingowych oraz zastosowania systemów IVR (art. 172 ustawy z 16 lipca 2004 r. Prawo telekomunikacyjne[365] – przyp. M.J. i J.W.).

[362] Za prawnie uzasadnione interesy administratora uznaje się m.in. zapewnienie bezpieczeństwa sieci, tj. „zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy. Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu «odmowa usługi», a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej”, motyw 49 RODO. Zob. także motyw 47 i 48.

[363] Motyw 47 RODO.

[364] T.j. Dz. U. z 2020 r. poz. 344.

[365] T.j. Dz. U. z 2021 r. poz. 576.

Nie są to zgody na przetwarzanie danych w rozumieniu RODO, ale (dodatkowe) zgody na wykorzystanie określonych kanałów komunikacji w celach marketingowych”[366]. Bez względu na podstawę prawną przetwarzania danych osobowych w celach marketingowych, tj. art. 6 ust. 1 lit. a) lub f) RODO, przetwarzanie, o którym mowa, ma granice czasowe. Wyznacza je odpowiednio art. 7 ust. 3 RODO, dający możliwość wycofania zgody, oraz art. 21 ust. 2, statuujący prawo do sprzeciwu.

Mając na względzie powyższe odniesienia, a także treść art. 17 ust. 1 lit. c) RODO, nie ulega wątpliwości, że prawo do bycia zapomnianym przysługuje w momencie wnoszenia sprzeciwu, o czym świadczy użyte w tym przepisie słowa „wnosi”. Z sytuacją taką będziemy mieli do czynienia np. wtedy, gdy osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych na potrzeby marketingu bezpośredniego. Należy jednak pamiętać, że jeżeli przetwarzanie danych w tym celu odbywa się w związku z zawartą umową, to zgłaszany sprzeciw i żądanie usunięcia danych dotyczą tylko celu marketingowego, a nie celu związanego z realizacją umowy, co wynika z powyższych rozwiązań oraz z treści art. 17 ust. 3 lit. b) RODO.

2.4. Przesłanka braku legalności przetwarzania danych

Wśród zasad dotyczących przetwarzania danych, prawodawca unijny wymienił zasadę legalności, którą dookreśla w kontekście danych zwykłych art. 6 i danych szczególnej kategorii art. 9 RODO. Istotą tej zasady jest nie tylko konieczność spełnienia wyrażonych w tych przepisach przesłanek, ale także zapewnienie zgodności przetwarzania danych „z pozostałymi przepisami o ochronie danych osobowych”[367]. Nie bez przyczyny więc prawodawca unijny w art. 17 ust. 1 lit. d) RODO przy-

[366] P. Barta, *Prawnie uzasadniony interes w działalności marketingowej,* „ABI Expert” 2018, nr 3, s. 17.

[367] P. Drobek, *Komentarz do art. 5 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…,* s. 326.

znał osobie, której dane dotyczą, prawo żądania od administratora usunięcia dotyczących jej danych, jeżeli były one przetwarzane niezgodnie z prawem[368].

W doktrynie podkreśla się, że „przetwarzanie «nielegalne» ignoruje obowiązek lub zakaz określony w przepisach prawa, a więc w szczególności jest to przetwarzanie danych bez podstawy prawnej lub w celu niezgodnym z prawem"[369]. Z nielegalnym przetwarzaniem danych będziemy mieli np. do czynienia wtedy, gdy osoba, której dane dotyczą, wycofa zgodę, a mimo to jej dane będą dalej przetwarzane przez administratora bez istnienia ku temu innej podstawy prawnej. W takiej sytuacji osoba, której dane dotyczą, może od razu wystąpić ze skargą do organu nadzorczego i czekać na jego rozstrzygnięcie bądź skorzystać z prawa do bycia zapomnianym, które nakłada na administratora obowiązek usunięcia danych bez zbędnej zwłoki.

Żądanie usunięcia danych na podstawie przesłanki wyrażonej w art. 17 ust. 1 lit. d) RODO może budzić jednak pewne wątpliwości, gdy idzie o ustalenie, czy naruszenie obowiązków informacyjnych, o których mowa w art. 13 i 14, skutkuje uznaniem przetwarzania za niezgodne z prawem[370]. Na gruncie ustawy o ochronie danych osobowych z 1997 r. stanowiska w tej kwestii były podzielone. Zdaniem J. Barty, P. Fajgielskiego i R. Markiewicza „niespełnienie przez administratora danych obowiązków informacyjnych przewidzianych w art. 24

[368] Por. decyzja PUODO z dnia 30 kwietnia 2020 r., ZKE.440.13.2019 nakazująca przywrócenie stanu zgodnego z prawem przez usunięcie z serwisu internetowego danych osobowych Skarżącego w zakresie jego imienia i nazwiska, sprawowanej przez niego funkcji, miejscowości zamieszkania oraz podpisu. Decyzja PUODO z dnia 20 listopada 2019 r. ZKE.440.54.20019 nakazująca usunięcie ze strony internetowej danych osobowych Skarżącego pozyskanych bezpośrednio z Monitora Sądowego i Gospodarczego i udostępnionych w serwisie internetowym jako dane osoby fizycznej w upadłości likwidacyjnej, https://uodo.gov.pl/pl/p/decyzje [dostęp: 5.10.2021].

[369] M. Krzysztofek, *Ochrona danych osobowych…*, s. 159.

[370] M. Krzysztofek, *Prawo do bycia zapomnianym i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy" 2012, s. 33.

u.o.d.o. (podobnie art. 25 u.o.d.o.) powoduje, iż przetwarzanie przez niego danych jest sprzeczne z prawem (ma nielegalny charakter)”[371]. Inaczej uważa P. Barta i P. Litwiński, do poglądu których przychylamy się, bowiem podkreślają oni, że „naruszenie obowiązku informacyjnego z art. 24 ust. 1 lub art. 25 ust. 1 OchrDanOsU nie wywiera takiego skutku, by można automatycznie uznać przetwarzanie danych osobowych zebranych z naruszeniem tego obowiązku za nielegalne”[372].

Mając powyższe na względzie, uważamy, że niedopełnienie obowiązków informacyjnych ciążących na administratorze (art. 13 i 14 RODO), mimo że stanowi poważne naruszenie, nie zawsze będzie podstawą do usunięcia danych. Usunięcie danych, a więc skorzystanie z prawa do bycia zapomnianym na podstawie art. 17 ust. 1 lit. d) „może być skutkiem niewykonania lub nieprawidłowego wykonania obowiązku informacyjnego, gdy przetwarzanie danych jest uzależnione od zgody albo braku sprzeciwu osoby, której dotyczą, ponieważ warunkiem ważności oświadczenia o zgodzie jest świadomość co do wszystkich aspektów planowanego przetwarzania”[373].

2.5. Przesłanka obowiązku prawnego

Zgodnie z art. 17 ust. 1 lit. e) RODO, osoba, której dane dotyczą, ma prawo żądania od administratora usunięcia dotyczących jej danych, gdy muszą one zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator. Na przesłankę tę można zatem powołać się, gdy upłynął termin przechowywania faktur sprze-

[371] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 507.

[372] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2016, s. 288 i n.

[373] M. Krzysztofek, *Ochrona danych osobowych…,* s. 160.

daży, tj. 5 lat, licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku[374].

Wskazany wyżej przepis budzi pewne wątpliwości, bowiem uzależnia realizację prawa do bycia zapomnianym od znajomości przez osobę, której dane dotyczą, przepisów prawa zobowiązujących administratora do usunięcia jej danych, o ile żądanie ma być skuteczne. Ponadto nie jest zrozumiałe, dlaczego administrator „miałby czekać z usunięciem danych"[375] aż do momentu wystąpienia z takim żądaniem przez osobę, której dane dotyczą, skoro jest to jego obowiązek wynikający z przepisów prawa[376], za naruszenie którego organ nadzorczy może nałożyć karę pieniężną.

2.6. Przesłanka dotycząca oferowania usług społeczeństwa informacyjnego dziecku

Rozwój nowych technologii oraz powszechny dostęp do sieci spowodowały, że Internet zyskał wielu użytkowników różnej kategorii wiekowej. Wśród nich są dzieci, które bardzo często nie są świadome ryzyka związanego z przetwarzaniem ich danych osobowych, ani przysługujących im z tego tytułu praw. Na kwestię tę zwrócił uwagę prawodawca unijny, podkreślając w motywach RODO konieczność objęcia szczególną ochroną danych osobowych dzieci. „Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich"[377]. Nie bez przyczyny więc przyjęto, że „wszelkie informacje i komunikaty – gdy przetwarzanie doty-

[374] Art. 70 § 1 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, t.j. Dz. U. z 2021 r. poz. 1540 ze zm.

[375] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 403.

[376] *Ibidem.*

[377] Motyw 38 RODO.

czy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć”[378].

Powyższe uwagi nie pozostają bez wpływu na treść prawa do bycia zapomnianym, bowiem zgodnie z art. 17 ust. 1 lit. f) RODO, osoba, której dane dotyczą, ma prawo żądania od administratora usunięcia dotyczących jej danych, gdy zostały one zebrane w związku z oferowaniem usług społeczeństwa informacyjnego[379], o których mowa w art. 8 ust. 1 RODO.

W przepisie tym, tj. w art. 8 ust. 1 RODO, prawodawca unijny określił warunki wyrażenia zgody przez dziecko w przypadku oferowanych mu usług społeczeństwa informacyjnego. Chodzi tu o ukończenie 16 lat przez dziecko, aby udzielona przez nie cyfrowa zgoda była skuteczna. Jeżeli nie ukończyło ono 16 lat, takie przetwarzanie uznane będzie za zgodne z prawem, gdy zgodę wyraziła lub zaaprobowała ją osoba spra-

[378] Motyw 58 RODO.

[379] Zgodnie z art. 4 pkt 25 RODO, usługa społeczeństwa informacyjnego oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady UE 2015/1535. W rozumieniu tej dyrektywy usługa społeczeństwa informacyjnego to każda usługa normalnie świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Do celów niniejszej definicji:

– „na odległość” oznacza, że usługa świadczona jest bez równoczesnej obecności stron;
– „drogą elektroniczną” oznacza, iż usługa jest wysłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (wyłącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomoc kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych;
– „na indywidualne żądanie odbiorcy usług” oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie.

Przykładowy wykaz usług nieobjętych niniejszą definicją został określony w załączniku I dyrektywy.

W tym miejscu warto dodać tytułem uzupełnienia, że przesłanka odpłatności „nie oznacza jednak wymogu opłacenia usługi przez odbiorcę usługi. Zgodnie z ukształtowaną linią orzeczniczą Trybunału Sprawiedliwości do uznania, iż przesłanka odpłatności jest spełniona, wystarczy, że dane świadczenie ma charakter ekonomiczny szeroko rozumiany, np. pozyskane jest z reklamy”, D. Lubasz, *Komentarz do art. 4 pkt 25 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 314.

wująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody. Przy czym państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat. W polskim porządku prawnym wynosi ona 16 lat.

Jak wynika z treści art. 8 ust. 1 RODO, wyrażona przez 16-letnie dziecko zgoda ma zastosowanie do usług społeczeństwa informacyjnego, które są bezpośrednio mu oferowane. Z usługą tą będziemy mieli do czynienia, gdy spełni ona kilka wymogów, a mianowicie będzie: skierowana do dzieci lub dzieci i dorosłych z uwagi na „brak sformułowania przesłanki wyłączności”[380] w art. 8 ust. 1 RODO; świadczona na odległość; drogą elektroniczną i na indywidualne jego żądanie. Przykładem są serwisy z grami, bajkami, „wyszukiwarki treści dla dzieci, magazyny dziecięce *on-line* czy dziecięce kanały streamingowe”[381].

Mając powyższe na względzie, nie ulega wątpliwości, że z realizacją przesłanki, o której mowa w art. 17 ust. 1 lit. f) RODO, będziemy mieli do czynienia, gdy 16-letnie dziecko wyraziło zgodę na przetwarzanie jego danych osobowych w celach marketingowych w związku z przystąpieniem do konkursu internetowego. W takim przypadku usunięcia danych „może domagać się zarówno dziecko, jak i osoba dorosła, jeżeli dotyczą one jej dzieciństwa”[382], co potwierdza również motyw 65 RODO[383]. Przesłanka, o której mowa, nie będzie miała jednak zastosowania, gdy podstawą przetwarzania nie jest zgoda, ale np. umowa, która najczęściej wykorzystywana jest przy zakładaniu konta – w tym przy-

[380] D. Lubasz, *Komentarz do art. 8 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 432.

[381] *Ibidem.*

[382] M. Czerniawski, *Komentarz do art. 17 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 528.

[383] Prawo do bycia zapomnianym „ma znaczenie w przypadkach, gdy osoba, której dane dotyczą wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z Internetu. Osoba, której dane dotyczą, powinna móc wykonywać to prawo, mimo że nie jest dzieckiem”, motyw 65 RODO.

padku – na portalu adresowanym do dzieci. W takiej sytuacji zgoda rodzica na przetwarzanie danych osobowych dziecka w świetle rozwiązań przyjętych w RODO nie jest wymagana, ale biorąc jednak pod uwagę przepisy Kodeksu cywilnego, może okazać się ona (zgoda rodzica) potrzebna w celu zawarcia umowy.

2.7. Przesłanka upublicznienia danych osobowych

W celu wzmocnienia prawa do bycia zapomnianym w Internecie prawodawca unijny zobowiązał administratora, który upublicznił dane osobowe – a które na mocy art. 17 ust. 1 ma obowiązek usunąć – do poinformowania administratorów, którzy przetwarzają takie dane, o usunięciu[384] wszelkich łączy do tych danych, kopii do tych danych lub ich replikacji[385]. Spełniając ten obowiązek, administrator podejmuje rozsądne działania z uwzględnieniem dostępnej technologii i kosztu realizacji, w tym dostępnych środków technicznych, w celu poinformowania administratorów, którzy przetwarzają dane osobowe, o żądaniu osoby, której dane dotyczą[386].

[384] „Usunięcie może następować za pomocą różnych działań, ważne jest natomiast aby przyniosły one jeden efekt, tj. wykluczyły możliwość identyfikacji określonej osoby", wyrok NSA z dnia 11 kwietnia 2017 r., I OSK 2170/15.

[385] Słusznie zauważa Paweł Fajgielski, że „wątpliwości budzi określenie «replikacje danych» i jego relacja do pojęcia «kopie danych», gdyż *prima facie* wydaje się, że są to określenia tożsame. Jednak w znaczeniu technicznym pojęcia te są od siebie odróżniane. O kopii danych mówimy zwykle w odniesieniu do dokładnego odwzorowania danych, przy czym po sporządzeniu kopii (np. kopii zapasowej) jest ona niezależna od skopiowanych danych, które mogą ulec zmianie bez wpływu na dane, które zostały powielone (skopiowane). Replikacja w znaczeniu technicznym oznacza podwajanie – tworzenie dokładnej kopii danych pomiędzy miejscem źródłowym składowania danych a docelowym miejscem, do którego one trafiają, i stanowi mechanizm wykorzystywany do poprawy bezpieczeństwa przetwarzanych danych. Prawodawca wymaga usunięcia zarówno danych, jak i odnośników do danych, kopii danych, a także replikacji danych, a więc wymaga usunięcia wszystkich danych i informacji, które pozwalają na dotarcie do treści danych", P. Fajgielski, *Ogólne rozporządzenie* …

[386] Zob. na ten temat, W.J. Kocot, *Charakter prawa do „bycia zapomnianym" – restytucja reputacji w Internecie*, [w:] I. Matusiak, K. Szczepanowska-Kozłowska, Ł. Żelechowski (red.), *Opus auctorem laudat. Księga jubileuszowa dedykowana Profesor*

Jak wynika z powyższych rozwiązań przyjętych w art. 17 ust. 2 oraz motywie 66 RODO, zakres ciążącego na administratorze obowiązku informacyjnego względem innych administratorów jest ograniczony, na co mają wpływ użyte w tym przepisie sformułowania, takie jak dostępna technologia, koszt realizacji czy rozsądne działania, które mogą być swobodnie interpretowane[387]. W konsekwencji oznacza to, że nałożone na administratora zobowiązanie nie ma charakteru „rezultatu, a wyłącznie starannego działania"[388].

Mając na względzie powyższe rozwiązania, nie wydaje się, aby były one przypadkowe. Prawodawca unijny, gwarantując bowiem prawo do bycia zapomnianym, wziął pod uwagę sytuację osoby, której dane dotyczą, nie zapominając przy tym o podmiocie zobowiązanym, który powinien podjąć racjonalne działania, a więc takie, które dopasowane są do jego możliwości (m.in. finansowych), by „poinformować tych administratorów, co do których wie, że przetwarzają dane objęte żądaniem"[389] osoby, której one dotyczą. W doktrynie odnośnie do tego obowiązku nie wyklucza się sytuacji, w której żądanie osoby uprawnionej będzie ograniczone jedynie do usunięcia dotyczących jej danych przez konkretnego administratora bez informowania o tym fakcie innych administratorów[390]. Ponadto zwraca się także uwagę i na inne sytuacje, w których żądanie osoby, której dane dotyczą, nie będzie skuteczne względem innych administratorów, którzy zostali o tym żądaniu poinformowani, pod warunkiem że dysponują oni „własną podstawą przetwarzania danych, skutecznie umożliwiającą im dalsze przetwa-

Monice Czajkowskiej-Dąbrowskiej, Warszawa 2019, Lex; M. Błażewski, J. Behr, *Środki ochrony danych osobowych,* Wrocław 2018, s. 166 i n.

[387] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 407.

[388] *Ibidem*.

[389] *Ibidem*.

[390] M. Czerniawski, *Komentarz do art. 17 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…,* s. 524 i n.

rzanie danych objętych żądaniem”[391]. Jeżeli natomiast i „w ich przypadku spełnione są przesłanki powstania możliwości żądania usunięcia danych, takie dane powinny zostać przez nich usunięte”[392], w tym wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

W sytuacji więc, gdy pracodawca udostępni na stronie internetowej zdjęcie pracownika wraz z imieniem i nazwiskiem, nie mając jego zgody, to w razie wystąpienia przez pracownika z żądaniem usunięcia tych danych, pracodawca zobowiązany będzie – biorąc pod uwagę wszystkie elementy treści zawarte w art. 17 ust. 2 RODO – do poinformowania innych administratorów przetwarzających te dane (np. operatorów wyszukiwarek internetowych), że osoba, której dane dotyczą, (pracownik) żąda, by usunęli oni linki do tych danych, ich kopie lub replikacje. Powyższe wnioski co do obowiązku informacyjnego wynikającego z art. 17 ust. 2 RODO zostały potwierdzone przez Europejską Radę Ochrony Danych. Organ ten zwrócił bowiem uwagę, że obowiązek, o którym mowa, „nie ma zastosowania do dostawców wyszukiwarek internetowych, gdy znajdują informacje zawierające dane osobowe opublikowane lub zamieszczone w Internecie przez osoby trzecie, indeksując je w sposób automatyczny, czasowo przechowując i udostępniając internautom w sposób uporządkowany zgodnie z określonymi preferencjami. Ponadto nie wymaga się w tym przypadku od dostawców wyszukiwarek internetowych otrzymujących żądanie usunięcia z listy wyników wyszukiwania od osoby, której dane dotyczą, poinformowania osoby trzeciej, która upubliczniła te informacje w Internecie. Zobowiązanie takie ma nałożyć większą odpowiedzialność na pierwotnych administratorów i dążyć do zapobiegania mnożeniu inicjatyw osób, których dane dotyczą”[393].

[391] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 407.

[392] *Ibidem*.

[393] Wytyczne EROD 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO (część 1), wersja 2.0, przyjęte 7 lipca 2020 r.

3. Przesłanki wyłączające korzystanie z prawa do bycia zapomnianym

Zgodnie z treścią art. 17 ust. 3 RODO, prawo do bycia zapomnianym, o którym mowa w ust. 1 i 2, nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
e) do ustalenia, dochodzenia lub obrony roszczeń.

Wymienione wyżej przesłanki zostały omówione w poniższych punktach niniejszego opracowania.

3.1. Przesłanka wolności wypowiedzi i informacji

Prawo do wolności wypowiedzi i informacji[394], w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, to jedno z zagadnień, na które zwrócił uwagę prawodawca unijny w kontekście ochrony danych osobowych. W motywie 153 RODO podkreślił on bo-

[394] Zob. M. Fazlioglu, *Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet,* "International Data Privacy Law" 2013, Vol. 3, No. 3, s. 153 i n.

wiem, że przetwarzanie danych osobowych jedynie do wskazanych wyżej celów „powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, przewidzianymi w art. 11 Karty praw podstawowych. […]. Państwa członkowskie powinny więc przyjąć akty prawne określające odstępstwa i wyjątki niezbędne do zapewnienia równowagi między tymi prawami podstawowymi". Tak też uczynił ustawodawca polski w art. 2 u.o.d.o. 2018, wskazując wyraźnie, które z przepisów RODO nie stosuje się do prasowej działalności dziennikarskiej w rozumieniu ustawy Prawo prasowe, a także do wypowiedzi w ramach działalności literackiej, artystycznej lub akademickiej[395].

Przyjęte wyjątki odnoszą się m.in. do praw przysługujących osobie, której dane dotyczą, wśród których nie ma prawa do bycia zapomnianym z uwagi na treść art. 17 ust. 3 lit. a) RODO. Przepis ten stanowi bowiem, że prawa do bycia zapomnianym, o którym mowa w ust. 1 i 2, nie stosuje się w zakresie, w jakim przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji. Aktualne pozostaje zatem w tej kwestii stanowisko TSUE, który w wyroku *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González* podkreślił, że „usunięcie linków z listy wyników może, w zależności od rodzaju wy-

[395] Art. 2 u.o.d.o. 2018.

Ust. 1. Do działalności polegającej na redagowaniu, przygotowaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. − Prawo prasowe (Dz. U. poz. 24 z późn. zm.), a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5-9, art. 11, art. 13-16, art. 18-22, art. 27, art. 28 ust. 2-10 oraz art. 30 rozporządzenia 2016/679.

Ust. 2. Do wypowiedzi akademickiej nie stosuje się przepisów art. 13, art. 15 ust. 3 i 4, art. 18, art. 27, art. 28 ust. 2-10 oraz art. 30 rozporządzenia 2016/679. Zob. także: W. Wątor, *Prawo do bycia zapomnianym a swoboda wypowiedzi. Glosa do wyroku ETPC z dnia 28 czerwca 2018 r., 60798/10 i 65599/10,* „Europejski Przegląd Sądowy" 2019, nr 5, Lex.

szukiwanej informacji, oddziaływać na uzasadniony interes potencjalnie zainteresowanych uzyskaniem dostępu do tej informacji internautów, […] należy dążyć do znalezienia punktu równowagi pomiędzy tym interesem a prawami podstawowymi, które przysługują tej osobie na podstawie art. 7 i 8 karty. 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”[396]. Nie budzi zatem wątpliwości, że przesłanka wyłączająca prawo do bycia zapomnianym, o której mowa w art. 17 ust. 3 lit. a), będzie miała zastosowanie np. do polityków lub osób pełniących funkcje publiczne zainteresowanych usunięciem niewygodnych dla nich informacji, które są istotne z punktu widzenia interesu publicznego. Nie będzie natomiast miała zastosowania do osoby fizycznej w razie upublicznienia w sieci informacji z jej sfery prywatnej np. kompromitujących zdjęć wraz z imieniem i nazwiskiem.

Innym przykładem potwierdzającym brak możliwości powołania się na prawo do bycia zapomnianym z uwagi na treść art. 17 ust. 3 lit. a) RODO jest udostępnienie *on-line* np. cyfrowej rzeźby przedstawiającej karykaturę polityka czy utworu muzycznego dotyczącego osoby pełniącej funkcję publiczną.

[396] Wyrok TSUE z dnia 13 maja 2014 r. w sprawie C-131/12 *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González,* pkt 81.

3.2. Przesłanka wywiązania się z obowiązku prawnego

Jak wynika z rozwiązań przyjętych w art. 17 ust. 3 lit. b) RODO, prawo do bycia zapomnianym nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Wskazany wyżej przepis jest bardzo pojemny, bowiem odnosi się do trzech kryteriów, w ramach których możliwe jest ograniczenie prawa do bycia zapomnianym[397]. Pierwsze z nich tyczy się wywiązania administratora z obowiązku prawnego. Z sytuacją taką będziemy mieli do czynienia np. gdy sprzedawca przetwarza dane osobowe klienta, który dokonał zakupu towaru przez Internet, w celu archiwizacji faktur, do czego zobowiązują go przepisy podatkowe[398].

Drugie kryterium związane jest z wykonaniem zadania realizowanego w interesie publicznym. Z uwagi na brak dookreślenia przez prawodawcę unijnego klauzuli generalnej, tj. interesu publicznego, należy przyjąć, że musi być ona „w kontekście indywidualnej spra-

[397] Por. decyzja PUODO z dnia 13 września 2019 r., ZSOŚS.440.102.2018 odmawiająca uwzględnienia wniosku w sprawie skargi na przetwarzanie danych osobowych Skarżącego w Krajowym Systemie Informacyjnym Policji (KSIP) przez Komendanta Głównego Policji oraz przetwarzanie i udostępnianie danych osobowych Skarżącego przez Komendanta Miejskiego Policji, https://uodo.gov.pl/pl/p/decyzje [dostęp: 5.10.2021].

[398] Por. decyzja PUODO z 23 grudnia 2019 r., ZKE.440.46.2019. Decyzja PUODO odmawiająca uwzględnienia wniosku dotyczącego usunięcia danych osobowych Skarżącego, ponieważ są one niezbędne do wypełnienia obowiązku prawnego ciążącego na Spółce, jakim jest obowiązek przechowywania danych zawartych na fakturze sprzedaży, gdyż stanowią one dokument księgowy, a Spółka jako podatnik jest zobowiązana do przechowywania ksiąg i związanych z ich prowadzeniem dokumentów do czasu upływu okresu przedawnienia zobowiązania podatkowego, tj. z upływem 5 lat, licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku, https://uodo.gov.pl/pl/p/decyzje [dostęp: 5.10.2021].

wy […] poddana stosownej wykładni”[399]. Na klauzulę tę zwrócił uwagę Trybunał Sprawiedliwości UE, nie tylko w wyroku *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González*, o czym wspomnieliśmy już w poprzednim punkcie tego rozdziału, ale także w sprawie przeciwko *Salvatoremu Manniemu*[400], który domagał się usunięcia z rejestru spółek informacji na temat tego, że był on zarządcą i likwidatorem spółki *Immobiliare Salentina*. W konsekwencji Trybunał, kierując się interesem publicznym, który realizują rejestry spółek, stwierdził brak możliwości „usunięcia bądź anonimizacji danych osobowych z rejestru handlowego, dopuszczając jedynie ograniczenie dostępu do nich osobom trzecim”[401].

Trzecie kryterium dotyczy wykonania zadania realizowanego w ramach sprawowania władzy publicznej powierzonej administratorowi[402]. Wyłączenie prawa do bycia zapomnianym oparte na tym kryterium będzie zatem możliwe, gdy przetwarzanie danych osobowych nastąpi na podstawie i w granicach prawa, a także służyć będzie wykonywaniu władzy publicznej. W sytuacji więc, gdy osoba zostanie wpisana przez starostę właściwego ze względu na jej miejsce zamieszkania do ewidencji instruktorów nauki jazdy, nie będzie ona mogła powołać się na prawo do bycia zapomnianym. Skorzystanie z tego prawa będzie natomiast możliwe, gdy przetwarzanie danych nie będzie mieć związku ze sprawowaniem władzy publicznej, np. „w od-

[399] Wyrok NSA z dnia 2 grudnia 2014 r., II FSK 71/13.

[400] Wyrok TSUE z dnia 9 marca 2017 r. w sprawie C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu.*

[401] M. Czerniawski, *Komentarz do art. 17 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 529.

[402] „Prawo Unii lub prawo państwa członkowskiego powinno określać także, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu […]”, motyw 45 RODO.

niesieniu do danych, które organ przetwarza na potrzeby prowadzenia newslettera"[403].

3.3. Przesłanka interesu publicznego w dziedzinie zdrowia publicznego

Zgodnie z art. 17 ust. 3 lit. c) RODO prawo do bycia zapomnianym, o którym mowa w ust. 1 i 2, nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego[404] zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3, a mianowicie gdy:

1) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia, z zastrzeżeniem, że są one przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej[405] na mocy

[403] M. Czerniawski, *Komentarz do art. 17 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…,* s. 529.

[404] Zgodnie z motywem 54 RODO, „zdrowie publiczne należy interpretować zgodnie z definicją z rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1338/2008, czyli jako wszelkie elementy związane ze zdrowiem, mianowicie stan zdrowia, w tym zachorowalność i niepełnosprawność, czynniki warunkujące stan zdrowia, potrzeby w zakresie opieki zdrowotnej, zasoby opieki zdrowotnej, oferowane usługi opieki zdrowotnej i powszechny dostęp do nich, wydatki na opiekę zdrowotną i sposób jej finansowania oraz przyczyny zgonów".

[405] Generalnie przez tajemnicę zawodową „rozumie się spoczywający na konkretnej osobie obowiązek ochrony przed nieuprawnionym dostępem przez osoby (podmioty) trzecie określonych przedmiotowo (indywidualnie, rodzajowo bądź kompleksowo) informacji pozyskanych lub wytworzonych w związku z wykonywaniem przez tę osobę zawodem (służbą i czynnościami, które w jej ramach są podejmowane). Podkreśla się przy tym jednocześnie, że cechą charakterystyczną takiego zawodu/służby (a tym samym tajemnicy zawodowej) jest ochrona zaufania, co do osoby zawód taki

prawa Unii lub prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe[406];

2) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową[407].

Jak wynika z rozwiązań przyjętych w art. 17 ust. 3 lit. c) RODO, prawodawca unijny uznał za dopuszczalną odmowę usunięcia danych ze względu na interes publiczny w dziedzinie zdrowia publicznego opierając się na wymienionych wyżej przesłankach dotyczących szczególnej kategorii danych osobowych. W konsekwencji oznacza to możliwość przetwarzania wskazanego rodzaju danych do „celów zdrowotnych wyłącznie w przypadkach, gdy jest to niezbędne do realizacji tych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa”[408]. Przy czym przetwarzanie danych w celu określonym w pkt 1 jest możliwe przez **pracownika** (podkr. M.J. i J.W.) podlegającego obowiązkowi zachowania wiążącej go tajemnicy zawodowej lub przez **inną osobę** (podkr. M.J. i J.W.) podlegającą obowiązkowi zachowania tajemnicy zawodowej. Uprawnionymi w tym kontekście są m.in. lekarze, pielęgniarki, położne,

wykonującej, której powierza się (dostarcza) konkretnych informacji i jej źródeł”, M. Jabłoński, J. Węgrzyn, *Ochrona tajemnic…*, s. 95.

[406] Art. 9 ust. 2 lit. h) i art. 9 ust. 3 RODO.

[407] Art. 9 ust. 2 lit i) RODO.

[408] Motyw 53 RODO.

diagności laboratoryjni. Co do przetwarzania danych szczególnej kategorii przez inną osobę podlegającą obowiązkowi zachowania tajemnicy zawodowej, pojawiają się jednak pewne wątpliwości, zwłaszcza gdy sięgniemy do wersji angielskiej art. 9 ust. 3[409] RODO. Wydaje się, że w przepisie tym chodzi o obowiązek zachowania przez inną osobę tajemnicy, a nie tajemnicy zawodowej. Należy bowiem mieć na uwadze, że przetwarzać dane szczególnej kategorii w określonym w pkt 1 celu może przecież osoba, która nie podlega tajemnicy zawodowej, np. pracownik firmy zewnętrznej zajmujący się obsługą serwisową. W takiej sytuacji ochrona tych danych nastąpi na podstawie umownej klauzuli poufności wprowadzonej do umowy powierzenia przetwarzania danych osobowych łączącej jej strony. Wątpliwości mogą pojawić się także w odniesieniu do osoby na stanowisku dyrektora szpitala, która niewykluczone jest, że może przetwarzać dane w celach określonych w pkt 1 w związku z pełnioną funkcją, ale z racji tego, że nie jest lekarzem, nie będzie związana tajemnicą zawodową. Poza tym, dane szczególnej kategorii mogą być przetwarzane do celów określonych w pkt 1 na odpowiedzialność pracownika zobowiązanego do zachowania tajemnicy zawodowej. Z sytuacją taką mielibyśmy do czynienia np. wtedy, gdy lekarz udostępniłby dane przetwarzane do celów, o których mowa w pkt 1 osobie nieuprawnionej.

3.4. Przesłanka dotycząca celów archiwalnych, badań naukowych, historycznych lub statystycznych

W myśl art. 17 ust. 3 lit. d) RODO, prawo do bycia zapomnianym nie ma zastosowania, jeżeli przetwarzanie jest niezbędne do celów ar-

[409] Art. 9 ust. 3 RODO, Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

chiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo do bycia zapomnianym, o którym w art. 17 ust. 1, uniemożliwi lub poważnie utrudni realizację wskazanych wyżej celów przetwarzania.

Jak wynika z rozwiązań przyjętych w art. 17 ust. 3 lit. d) RODO, prawodawca unijny odniósł się do czterech celów przetwarzania. Pierwszy to cel archiwalny w interesie publicznym, który dotyczy informacji np. o „postawie politycznej w dawnych systemach państw totalitarnych, o przypadkach ludobójstwa, zbrodniach przeciwko ludzkości (zwłaszcza holokauście) czy zbrodniach wojennych”[410]. Drugi cel tyczy się badań naukowych i obejmuje m.in. „rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych […]. Wyrażenie «do celów badań naukowych» powinno obejmować także badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego”[411]. W sytuacji więc, gdy lekarz w celach naukowych przetwarza informacje o pacjentach i stosowanych przez niego metodach leczenia, prawo do bycia zapomnianym nie znajdzie zastosowania. Trzeci to cel historyczny. Obejmuje on m.in. badania historyczne i badania do celów genealogicznych[412]. Czwarty jest cel statystyczny, przez który należy rozumieć „każdą operację zbierania i przetwarzania danych osobowych niezbędnych do badań statystycznych lub do opracowywania wyników statystycznych. Z kolei wyniki statystyczne mogą następnie służyć do dalszych celów, m.in. do celów badań naukowych. Wyrażenie «cel statystyczny» sugeruje, że wynikiem przetwarzania do celów statystycznych nie są dane osobowe, lecz dane zbiorcze, i że wynik ten lub

[410] Motyw 158 RODO.
[411] Motyw 159 RODO.
[412] Motyw 160 RODO.

dane osobowe nie służą za podstawę środków czy decyzji dotyczących konkretnych osób fizycznych”[413].

Wymienionym wyżej celom nie bez przyczyny prawodawca unijny przyznał nadrzędną rolę względem prawa do bycia zapomnianym. Wynika to z istoty tego prawa, która przejawia się w usunięciu danych, bez których przetwarzanie czy to do celów archiwalnych w interesie publicznym, czy do celów badań naukowych lub historycznych, czy do celów statystycznych, nie byłoby możliwe.

3.5. Przesłanka dotycząca roszczeń

Ostatnią z wymienionych w art. 17 ust. 3 RODO przesłanek, wyłączających prawo do bycia zapomnianym, jest ta, która odnosi się do ustalenia, dochodzenia lub obrony roszczeń[414]. W praktyce może okazać się, że będzie to jedna z najczęściej wykorzystywanych przesłanek, dająca podstawę administratorowi do dalszego przetwarzania danych osoby, której one dotyczą. Z sytuacją taką będziemy mieli do czynienia np. w razie zawarcia umowy sprzedaży przez Internet. Sprzedawca (administrator) z uwagi na możliwość skorzystania przez klienta z rękojmi za wady fizyczne towaru lub gwarancji będzie mógł odmówić realizacji prawa do bycia zapomnianym. Na tę samą przesłankę mogą powoływać się również firmy windykacyjne, które nabyły wierzytelność. Należy bowiem mieć na uwadze, że zgodnie z art. 6 ust. 1 RODO, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy i w takim zakresie, w jakim spełniony jest jeden ze wskazanych w tym przepisie warunków. W przypadku firm windykacyjnych warunkiem jest „przetwarzanie niezbędne do celów wynikających z prawnie uzasadnionych interesów re-

[413] Motyw 162 RODO.

[414] Art. 17 ust. 3 lit. e) RODO. Por. decyzja PUODO z 20 marca 2019 r., ZSPR.440.493.2019 odmawiająca uwzględnienia wniosku dotyczącego usunięcia danych osobowych Skarżącej z Banku oraz z Biura Informacji Kredytowej, https://uodo.gov.pl/pl/p/decyzje [dostęp: 5.10.2021].

alizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności, osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem" – art. 6 ust. 1 lit. f)[415].

Mając powyższe na względzie, nie budzi wątpliwości, że firmy windykacyjne posiadające wierzytelności (administratorzy danych) mogą skutecznie odmawiać dłużnikom realizacji prawa do bycia zapomnianym, opierając się na przesłance wyrażonej w art. 17 ust. 3 lit. e) RODO. Aktualny pozostaje zatem pogląd Wojewódzkiego Sądu Administracyjnego w Warszawie, który podkreślił, że „zasadą powszechnie akceptowaną, wynikającą nie tylko z przepisów prawa cywilnego, lecz także z norm moralnych, zasad współżycia społecznego oraz dobrych obyczajów jest regulowanie zaciągniętych zobowiązań (zapłata długów). Zasada ta odnosi się w pełni do podmiotów prawa mających status konsumentów. […]. Dłużnik, który nie wywiązuje się ze swoich zobowiązań, musi liczyć się z konsekwencjami wynikającymi z przepisów regulujących obrót gospodarczy. Postawa dłużnika nie może bowiem prowadzić do uprzywilejowania jego sytuacji prawnej. Gdyby generalnie uznać każdy wypadek przetwarzania danych osobowych dłużnika (będącego konsumentem) za godzący w jego prawa i wolności, doszłoby z jednej strony do niczym nieuzasadnionej ochrony osób niewywiązujących się ze swoich zobowiązań, z drugiej natomiast do naruszenia zasady swobody działalności gospodarczej, co z pewnością nie było zamiarem"[416] prawodawcy unijnego.

[415] Por. decyzja PUODO z 4 stycznia 2019 r., ZSPR.440.631.2018 odmawiająca uwzględnienia skargi na udostępnienie na internetowej giełdzie długów danych osobowych dłużnika w zakresie imienia i nazwiska oraz nazwy miejscowości i ulicy, https://uodo.gov.pl/pl/p/decyzje [dostęp: 5.10.2021].

[416] Wyrok WSA w Warszawie z dnia 30 listopada 2004 r., II SA/Wa 1057/04. Wyrok dostępny na: http://orzeczenia.nsa.gov.pl/doc/AE4E8781C7 [dostęp: 10.09.2021].

4. Procedura postępowania w sprawie realizacji prawa do bycia zapomnianym

4.1. Brak normatywnego wzorca wniosku o usunięcie danych osoby, której one dotyczą

Wydany pod rządami nieobowiązującej już dyrektywy 95/46/WE wyrok Trybunału Sprawiedliwości UE w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González* zapewnił możliwość żądania od operatorów wyszukiwarek internetowych usunięcia linków z listy wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby[417]. „Pomimo wielu niejasności oraz braku precyzyjnych wskazówek czy procedur w zakresie sposobu implementacji"[418] tego wyroku przez podmioty zobowiązane, „już 29.5.2014 r. *Google*, operator wyszukiwarki *Google Web Search*, udostępnił formularz internetowy"[419], za pomocą którego osoby, których dane dotyczą, mogą żądać usunięcia treści zindeksowanej przez tę wyszukiwarkę. Do kwestii tej odniosła się także Grupa Robocza Artykułu 29, wskazując, że opracowanie przez operatorów wyszukiwarek internetowych procedur *online* i wniosków elektronicznych, może być dobrym rozwiązaniem ze względu na wygodę, to jednak nie powinien być to wyłączny sposób realizacji prawa do bycia zapomnianym[420].

W praktyce okazuje się, że wniosek elektroniczny pomimo udostępnienia go jedynie przez operatora wyszukiwarki *Google* oraz

[417] Por. pkt 88 wyroku TSUE w sprawie C-131/12 oraz pkt 73 wyroku TSUE w sprawie C-507/17.

[418] T. Grzegory, *op. cit.*, s. 61.

[419] *Ibidem.*

[420] Wytyczne Grupy Roboczej Art. 29 dotyczące wykonania wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González C-131/12,* https://giodo.gov.pl/pl/1520203/8648 [dostęp: 10.09.2021].

Bing[421] stał się wyłącznym środkiem realizacji prawa do bycia zapomnianym. Mimo to, jak wynika z dostępnych statystyk, zainteresowanie tym prawem jest duże. Od maja 2014 r. do 7 grudnia 2015 r. polscy internauci wysłali 9566 zgłoszeń, które dotyczyły 36 061 adresów URL[422]. Łącznie z całego świata, do końca 2015 r., *Google* otrzymało 353 820 zgłoszeń, które dotyczyły 1 253 101 linków[423]. Najnowsze statystyki pokazują, że od 28 maja 2014 do sierpnia 2021 r. polscy internauci wysłali do Google 34 334 zgłoszenia, które dotyczą 148 858 adresów URL[424], co potwierdza, że zainteresowanie prawem do bycia zapomnianym nadal jest duże.

Brak normatywnego wzorca wniosku, na podstawie którego osoba, której dane dotyczą, może żądać ich usunięcia, tyczy się także RODO. Prawodawca unijny w żadnym z przepisów tego aktu nie odniósł się bowiem do elementów treści wniosku, ani do jego formy. W związku z tym, wydaje się, że administrator zobowiązany jest do rozpatrzenia żądania, gdy zawierać ono będzie dane wnioskodawcy i wykazane zostanie, że zachodzi jedna z przesłanek, o których mowa w art. 17 ust. 1 RODO. W niektórych przypadkach wydaje się, że brak uzasadnienia wniosku nie powinien skutkować pozostawieniem go bez rozpoznania, zwłaszcza gdy idzie o przesłankę wyrażoną w art. 17 ust. 1 lit. a) lub b) RODO. Forma jego wniesienia może być dowolna. Ważne natomiast jest, aby na jej podstawie można było ustalić tożsamość osoby składającej żądanie. Administrator powinien więc zapewnić możli-

[421] https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636594911489394651-2718733419&hl=pl&rd=1 [dostęp: 10.09.2021]; https://www.bing.com/webmaster/tools/eu-privacy-request?cc=pl [dostęp: 10.09.2021].

[422] Chodzi tu jedynie o osoby prywatne, ponieważ żądania właścicieli praw autorskich nie zostały uwzględnione w tej statystyce. 39,9% próśb zostało pozytywnie rozpatrzonych; https://pclab.pl/news67342.html [dostęp: 10.09.2021].

[423] *Ibidem.*

[424] https://transparencyreport.google.com/euprivacy/overview?delisted_urls=start:1401235200000;end:1630367999999;country:PL&lu=delisted_urls&requests_over_time=country:PL [dostęp: 10.09.2021].

wość wniesienia żądania drogą pisemną, ustną (np. nagrywana rozmowa telefoniczna), a także elektroniczną – np. przez „email wysłany z konkretnego, znanego obu stronom adresu, odznaczenie okienka w systemie informatycznym (po zalogowaniu do systemu)"[425] – w szczególności gdy dane osobowe są przetwarzane tą drogą[426].

4.2. Postępowanie podmiotu zobowiązanego w zakresie realizacji prawa do bycia zapomnianym

Wniesienie żądania o usunięcie danych przez osobę, której one dotyczą, wiąże się z podjęciem przez administratora odpowiednich środków, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, a także jasnym i prostym językiem, porozumiewać się z podmiotem danych w celu realizacji przysługującego mu prawa. Komunikacja między wskazanymi podmiotami może mieć dowolną formę, tj. pisemną, elektroniczną[427] lub ustną[428]. W wielu opracowaniach podkreśla się jednocześnie, że „wobec administratorów naruszających podstawowe zasady przetwarzania, a zatem także zasadę przejrzystości oraz prawa podmiotu danych zagwarantowane treścią art. 12 RODO […] może być zastosowana sankcja w postaci administracyjnej kary pieniężnej w maksymalnej określonej przepisami rozporządzenia wysokości"[429].

Każdy administrator musi wprowadzić wewnętrzne procedury:

– identyfikacji i weryfikacji przedmiotu żądania;

[425] https://sylwiaczub.pl/wniosek-o-usuniecie-danych-osobowych-wedlug-rodo/ [dostęp: 10.09.2021].

[426] Motyw 59 RODO.

[427] Odnośnie do formy elektronicznej prawodawca unijny przyjął, że jeżeli osoba, której dane dotyczą, przekazała swoje żądanie w formie elektronicznej, to w miarę możliwości informacje przekazywane są w tej formie, chyba że osoba ta zażąda innej formy, art. 12 ust. 3 *in fine* RODO.

[428] Forma ta jest dopuszczalna na żądanie osoby, której dane dotyczą, o ile innymi sposobami potwierdzi się tożsamość tej osoby, zob. art. 12 ust. 1 RODO.

[429] J. Łuczak, *Komentarz do art. 12*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 476.

– weryfikacji podmiotu występującego z punktu widzenia uznania go za podmiot legitymowany do realizacji praw, o których mowa w art. 15–22 RODO;
– odpowiedniego sprecyzowania etapów postępowania nakierowanego na merytoryczne stwierdzenie zasadności (bądź braku) realizacji uprawnień przez występującego.

Procedura RODO-wska musi więc łączyć się z czytelnym zdefiniowaniem działań podejmowanych przez zobowiązanego (administratora), obejmując nie tylko kwestie identyfikacji odpowiedniej procedury innej niż ta związana z realizacją praw osób, których dane dotyczą, ale równolegle definiujących kolejność poszczególnych działań podejmowanych przez odpowiednio umocowane osoby, działające w imieniu administratora. Musi też łączyć się z wcześniejszym opracowaniem wzorców dokumentów, w tym wezwań do sprecyzowania treści wniosku i wskazania właściwej procedury; wykazania, że z wnioskiem występuje osoba uprawniona (weryfikacja tożsamości wnioskodawcy); wyeliminowania braków formalnych wniosku (odpowiedniego uzupełnienia treści wniosku) – wraz ze zdefiniowaniem terminów oraz skutków niewywiązania się z nich przez wnioskodawcę (*de facto* rozstrzygnięć)[430], całego obszaru merytorycznego rozpatrzenia prawidłowo wniesionych wniosków (w odniesieniu do konkretnych i sprecyzowanych żądań – np. prawa do sprostowania danych – art. 16 RODO, oraz wniosków złożonych, tzn. obejmujących kilka lub sumę gwarantowanych uprawnień), a także odmowy podjęcia działań, o której mowa w art. 12 ust. 5 RODO[431].

[430] Z formalnego punktu widzenia nie będzie miało więc znaczenia, czy nazwiemy je powiadomieniami czy też decyzjami. Wnioskodawca będzie też uprawniony do kwestionowania zasadności takich wezwań.

[431] „Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może: a) pobrać rozsądną opłatę, uwzględ-

Mimo że w treści art. 12 ust. 1 RODO podkreśla się, że ustne udzielenie informacji ma miejsce wtedy, gdy „innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą", to nie budzi wątpliwości, że udostępnienie informacji w każdym przypadku musi wiązać się z koniecznością zweryfikowania, że jest ona udostępniana osobie właściwej[432] (tzn. takiej, której dane są przetwarzane)[433]. Przy czym można zgodzić się z twierdzeniem, że „[…] wymóg potwierdzenia tożsamości osoby, której dane dotyczą, pozwala na przyjęcie, że ograniczenie możliwości korzystania z formy ustnej dotyczy tylko tych informacji, które odnoszą się do konkretnej osoby fizycznej, którą wcześniej należało zidentyfikować – stąd wydaje się, że ograniczenie posługiwania się formą ustną nie powinno dotyczyć wykonania obo-

niając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo b) odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze".

[432] „Nakaz potwierdzania tożsamości wnioskodawcy w sposób niebudzący wątpliwości, zwłaszcza tam, gdzie na skutek zgłoszonego roszczenia mogłoby dojść do udostępnienia danych lub wprowadzenia innego ryzyka dla bezpieczeństwa danych. Administrator powinien wdrożyć rozwiązania mające na celu przeciwdziałanie ujawnieniu danych w wyniku złożenia żądania przez osobę nieuprawnioną. Dlatego też w przypadku przetwarzania niewymagającego identyfikacji, tam gdzie administrator nie jest w stanie zidentyfikować podmiotu danych i okoliczność tę wykaże, może nawet odmówić podjęcia działań" – J. Łuczak, *op. cit.*, s. 471.

[433] W tym zakresie konieczne jest wprowadzenie równoległych procedur weryfikujących dotyczących złożenia wniosku w kancelarii, drogą elektroniczną lub ustnie. Procedury te będą charakteryzowały się różnym stopniem złożoności od najprostszej dotyczącej klasycznej postaci weryfikacji tożsamości w sytuacji osobistego składania żądania, przez wykorzystanie podpisu kwalifikowanego lub profilu zaufanego, czy wreszcie poprzez weryfikację tożsamości polegającą na przesłaniu zwrotnej wiadomości e-maila z linkiem zawierającym prośbę o potwierdzenie złożenia wniosku. Droga telefoniczna musi wiązać się nie tylko z możliwością skutecznego przyjęcia wniosku przez administratora, ale możliwością weryfikacji tożsamości. Nie jest to zadanie niemożliwe do wykonania, ale wymaga wprowadzenia dodatkowych elementów techniczno-organizacyjnych, które pozwalają na weryfikację zgodności posiadanych danych. Procedury takie z powodzeniem stosowane są np. przez operatorów telekomunikacyjnych i innych usługodawców.

wiązków informacyjnych z art. 13 i 14 RODO, choć czysto językowa wykładnia komentowanego przepisu zdaje się temu przeczyć”[434].

Nie budzi też wątpliwości, że zwroty, którymi w treści art. 12 RODO posłużył się ustawodawca unijny (w szczególności: skomplikowany charakter żądania; liczba żądań – ust. 3; żądanie ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter – ust. 5), muszą zostać doprecyzowywane w praktyce stosowania prawa. Takie doprecyzowanie musi nastąpić w treści uzasadnień[435] konkretnych rozstrzygnięć organów (podmiotów) zarówno administracyjnych, jak i innych będących administratorami danych.

Niemniej istotną kwestią jest termin realizacji prawa do bycia zapomnianym, do którego prawodawca unijny odniósł się w art. 17 ust. 1 RODO. W myśl tego przepisu „osoba, której dane dotyczą, ma prawo

[434] 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*, P. Litwiński (red.), Warszawa 2018, s. 356-357.

[435] „Nośnikiem takiej informacji jest uzasadnienie rozstrzygnięcia (także wpadkowego), dokonane wobec osoby zainteresowanej, czy to ustnie, czy pisemnie. Sam fakt istnienia zróżnicowanej praktyki sądowej na tle zwrotu niedookreślonego nie jest świadectwem wadliwości takiego przepisu. Istnienie takiej praktyki jest bowiem wyrazem wykorzystania potencjału, jaki zawiera taki przepis, i nie jest tożsame z istnieniem jego konstytucyjnie nagannej niejasności. Nie w każdym zatem wypadku nieprecyzyjne brzmienie lub niejednoznaczna treść przepisu uzasadniają tak daleko idącą ingerencję w system prawny, jaką jest wyeliminowanie z niego tego przepisu w wyniku orzeczenia Trybunału Konstytucyjnego. Do wyjątków należą sytuacje, gdy dany przepis, zawierający zwrot niedookreślony będzie sam w sobie w takim stopniu wadliwy, że w żaden sposób, przy przyjęciu różnych metod wykładni, nie daje się interpretować w sposób racjonalny i zgodny z Konstytucją. Zdaniem Trybunału Konstytucyjnego, niejasność przepisu może uzasadniać stwierdzenie jego niezgodności z Konstytucją, o ile jest tak daleko posunięta, iż wynikających z niej rozbieżności nie da się usunąć za pomocą zwyczajnych środków mających na celu wyeliminowanie niejednolitości stosowania prawa. Pozbawienie mocy obowiązującej przepisu z powodu jego niejasności jest więc środkiem ostatecznym, stosowanym dopiero wtedy, gdy inne metody usuwania skutków niejasności treści przepisu, w szczególności przez jego interpretację w orzecznictwie sądowym, okażą się niewystarczające (zob. wyrok TK z dnia 9 października 2007 r., SK 70/06, OTK ZU nr 9/A/2007, poz. 103). Sam zaś fakt praktyki zróżnicowanej na tle zwrotu niedookreślonego nie może być utożsamiany z jego «niejasnością»” – wyrok TK z dnia 16 czerwca 2008 r., P 37/07.

żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe", jeżeli zachodzi jedna ze wskazanych w tym przepisie przesłanek.

Jak wynika z treści zacytowanego wyżej artykułu, spełnienie żądania, o którym w nim mowa, ma nastąpić bez zbędnej zwłoki. Użyty w przepisie tym termin „bez zbędnej zwłoki" należy jednak rozpatrywać w kontekście art. 12 ust. 3 RODO, odnosi się on bowiem do proceduralnych aspektów „wykonywania praw osób, których dane dotyczą"[436]. To z kolei oznacza, że w razie wpłynięcia do administratora wniosku o usunięcie danych osobowych, zobowiązany on jest bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – do usunięcia danych osoby, której one dotyczą. W razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. O przedłużeniu terminu oraz podaniu przyczyn opóźnienia, administrator informuje osobę, której dane dotyczą, w terminie miesiąca od otrzymania od niej żądania usunięcia danych[437]. Gdy natomiast administrator zaniecha działań w związku z tym żądaniem, to wówczas niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje podmiot danych o powodach niepodjęcia działania, możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

W procesie realizacji prawa do bycia zapomnianym bardzo ważne jest, aby administrator prowadził wykaz wniesionych wniosków i prowadzonej w związku z nimi korespondencji, w celach dowodowych w razie ewentualnych sporów prowadzonych z podmiotami da-

[436] P. Litwiński, P. Barta, M. Kawecki, *op. cit.,* s. 355.
[437] Zob. art. 12 ust. 3 RODO.

nych[438]. „W tym kontekście istotne jest również właściwe”[439] zidentyfikowanie osoby składającej żądanie, dlatego na podstawie art. 12 ust. 6 RODO, administrator w sytuacji uzasadnionych wątpliwości co do tożsamości takiej osoby, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Może to polegać np. na przesłaniu przez administratora na znany obu stronom adres email, hasła, które trzeba będzie wprowadzić, aby zalogować się do usług oferowanych przez administratora. Weryfikacja tożsamości może więc nastąpić poprzez różne mechanizmy uwierzytelniania. Należy przy tym mieć na uwadze, że administrator może także odmówić spełnienia żądania usunięcia danych, jeżeli wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą[440].

Działania podejmowane w związku z realizacją prawa do bycia zapomnianym są wolne od opłat poza przypadkami, gdy żądanie podmiotu danych jest ewidentnie nieuzasadnione lub nadmierne. Ciężar udowodnienia takiego charakteru żądania spoczywa na administratorze, który dopiero po jego wykazaniu może pobrać rozsądną opłatę[441], albo odmówić podjęcia działań w związku z żądaniem usunięcia danych.

W ramach realizacji wniesionego przez osobę, której dane dotyczą, żądania usunięcia jej danych, administrator w razie pozytywnego rozpatrzenia przedmiotowego żądania zobowiązany jest poinformować o usunięciu danych, którego dokonał na mocy art. 17 ust. 1 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysił-

[438] J. Łuczak, *Komentarz do art. 12 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 471.

[439] *Ibidem.*

[440] Zob. art. 12 ust. 2 RODO.

[441] Pobierając rozsądną opłatę, administrator uwzględnia „administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań”, art. 12 ust. 5 lit. a) RODO.

ku. Administrator informuje osobę, której dane dotyczą, o tych odbiorach, jeżeli wystąpi ona z takim żądaniem (art. 19 RODO).

Jak wynika z przyjętych na gruncie art. 19 RODO rozwiązań, administrator może uchylić się od powyższego obowiązku w dwóch przypadkach. Po pierwsze, gdy powiadomienie okaże się niemożliwe, bo np. „spółka, która była odbiorcą danych, w międzyczasie została zlikwidowana”[442] lub będzie to uwarunkowane przyczynami natury technicznej[443]. Po drugie, gdy powiadomienie będzie wymagać niewspółmiernie dużego wysiłku, z czym będziemy mieli do czynienia „wówczas, gdy wysiłek włożony w przekazanie informacji jest nieproporcjonalny w stosunku do niedogodności spowodowanych brakiem tych informacji u osoby, której dane dotyczą”[444]. I choć przesłanka ta ma charakter uznaniowy, to należy pamiętać, że administrator nie jest zwolniony z obowiązku udokumentowania przeprowadzonej oceny – na okoliczność uchylenia się od obowiązku powiadomienia (art. 19 RODO) – bowiem czynność ta jest niezbędna z uwagi na wiążącą administratora zasadę rozliczalności.

[442] M. Czerniawski, *Komentarz do art. 19,* [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO…*, s. 541.

[443] P. Fajgielski, *Komentarz do art. 19,* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Lex.

[444] 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,* Warszawa 2018, s. 415.

Rozdział IV

Środki techniczne i organizacyjne jako gwarancje bezpieczeństwa przetwarzania danych osobowych

W procesie przetwarzania danych osobowych bardzo ważne jest, aby podmiot zobowiązany skutecznie te dane zabezpieczył. Do osiągnięcia tego celu potrzebne jednak jest wdrożenie odpowiednich środków technicznych i organizacyjnych przy uwzględnieniu stanu wiedzy technicznej, kosztów wdrażania, charakteru, zakresu, kontekstu, celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze (art. 32 ust. 1 RODO).

Powyższe rozwiązanie jest przykładem przyjętej w RODO „konstrukcji bazującej na kształtowaniu obowiązków, których zakres określany jest przez pryzmat oceny ryzyka *(risk-based approach)*"[445]. W praktyce oznacza to odejście „od jednakowego traktowania wszystkich podmiotów w zakresie obowiązku zabezpieczenia danych osobowych"[446], przez co konieczne jest „dostosowanie zabezpieczeń do ry-

[445] D. Lubasz, *Komentarz do art. 32 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…,* s. 692. Zob. także R. Kania, *Ryzyko, czas i cudze prawa – proces ochrony danych,* „ABI Expert" 2018, nr 2, s. 34 i n.

[446] https://s4edu.pl/pl/centrum-wiedzy/92-gdpr/116-najwieksze-wyzwanie-rodo-on-riks-basedapproach [dostęp: 10.09.2021].

zyk związanych z przetwarzaniem danych osobowych, które u każdego administratora mogą być inne”[447]. Zupełnie inne środki ochrony będą więc stosowane w przypadku przetwarzania danych osobowych przez właściciela sklepu internetowego, a inne przez podmiot świadczący usługi telemedyczne. Wdrożenie tych środków nie ma jednak charakteru stałego, bowiem podejście oparte na zasadzie ryzyka wymaga od podmiotu zobowiązanego ciągłej identyfikacji i analizy poziomu zagrożeń związanych z przetwarzaniem danych, co w konsekwencji łączy się z koniecznością dokonywania ich przeglądów i aktualizacji. Podejście oparte na ryzyku wymusza zatem „na administratorze danych i podmiocie przetwarzającym dbanie o odpowiednią ochronę na wszystkich etapach przetwarzania danych osobowych, tj. podczas całego cyklu życia informacji, od momentu zbierania danych aż do ich usunięcia. Innymi słowy, konieczne jest wbudowanie zasad ochrony danych osobowych w każdy projekt zakładający przetwarzanie danych osobowych, a następnie zapewnienie odpowiedniej ochrony danych osobowych na każdym etapie procesu przetwarzania danych, zgodnie z zasadą uwzględniana ochrony danych w fazie projektowania (ang. *privacy by design*). Zasada ta wymaga, aby potrzeby w zakresie ochrony danych uwzględniane były w całym cyklu przetwarzania danych, tj. od momentu pojawienia się koncepcji systemu przetwarzania, przez budowę projektu, stworzenie systemu, następnie jego wdrożenie i eksploatację, kończąc na usunięciu danych”[448].

Mając powyższe na względzie, nie budzi więc wątpliwości, że zmiana modelu ochrony danych osobowych na podejście oparte na zasadzie ryzyka wymaga od podmiotu zobowiązanego przeprowadzenia wnikliwej analizy, która pozwoli nie tylko „wykazać, zgodnie z zasadą rozliczalności (jedną z głównych zasad RODO), uwzględnienie ochro-

[447] *Ibidem.*

[448] https://uodo.gov.pl/data/filemanager_pl/706.pdf [dostęp: 10.09.2021].

ny danych w fazie projektowania[449] i stosowania domyślnej ochrony danych (art. 25 RODO)"[450], ale także podjąć decyzję o wdrożeniu odpowiednich środków technicznych i organizacyjnych do zagrożeń związanych z przetwarzaniem danych osobowych. Należy jednak pamiętać, że jeżeli podczas dokonywanej oceny okaże się, że operacje przetwarzania danych – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko, wówczas administrator zobowiązany jest przed rozpoczęciem przetwarzania, dokonać oceny skutków dla ochrony danych[451]. Z wyjątkiem wskazanej wyżej sytuacji, ocena ta wymagana jest także m.in. w przypadku:

- systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną[452];
- przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10[453]; lub

[449] Zob. na ten temat, W.R. Wiewiórowski, *Privacy by Design jako paradygmat ochrony prywatności,* [w:] G. Szpor, W.R. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012, s. 13 i n.; A. Kobylańska, Ł. Ślęzak, *op. cit.*, s. 15 i n.; J. Anisimowicz, *Privacy by design z perspektywy architektury i budowy systemów informatycznych,* „ABI Expert" 2018, nr 2, s. 26 i n.

[450] M. Więckowska, *Analiza ryzyka prywatności,* „ABI Expert" 2017, nr 2, s. 48.

[451] Zob. art. 35 ust. 1 RODO.

[452] Art. 35 ust. 3 lit. a) RODO.

[453] Sprostowanie do 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 (ogólne rozporządzenie o ochronie danych), OJ L 127/2, 23.5.2018, art. 35 ust. 3 lit. b).

– systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie[454].

Wskazany wyżej przykładowy wykaz rodzajów operacji przetwarzania podlegających ocenie skutków dla ochrony danych doprecyzowuje organ nadzorczy, tj. Prezes Urzędu Ochrony Danych Osobowych[455]. Proponowany przez PUODO wykaz dostępny jest w formie tabeli, która zawiera trzy kolumny, tj.

– rodzaje/kryteria dla operacji przetwarzania, dla których wymagane jest przeprowadzenie oceny (np. innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych);
– potencjalne obszary wystąpienia/istniejące obszary zastosowań (np. zastosowanie komunikacji między urządzeniami (Internet rzeczy – np. beacony, drony) w przestrzeni publicznej i w miejscach użyteczności publicznej);
– przykłady operacji/zakresu danych/okoliczności, w których może wystąpić wysokie ryzyko naruszenia dla danego rodzaju operacji przetwarzania (np. systemy stosowane do analizy i przekazywania danych dostawcom usługi przy użyciu aplikacji mobilnych z urządzeń przenośnych typu: smartwatch, inte-

[454] Art. 35 ust. 3 lit. c) RODO.

[455] Prezes Urzędu Ochrony Danych Osobowych „może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych", art. 35 ust. 5 RODO. Zgodnie natomiast z art. 35 ust. 6 RODO, jeżeli wykazy rodzajów operacji przetwarzania podlegające i niepodlegające wymogowi dokonania oceny skutków dla ochrony danych, „obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63 RODO".

ligentne opaski, beacony itp. analizujące i przekazujące dane dostawcom przy użyciu aplikacji mobilnych)[456].

W praktyce wykaz ten z pewnością ułatwi wielu administratorom decyzję co do przeprowadzenia oceny skutków dla ochrony danych, która „powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania, nawet jeżeli niektóre operacje przetwarzania nadal są nieznane. Aktualizacja oceny skutków dla ochrony danych przez cały cykl trwania projektu zapewni uwzględnienie ochrony danych i prywatności oraz zachęci do tworzenia rozwiązań promujących zgodność. W miarę postępu procesu rozwoju konieczne może być również powtórzenie poszczególnych etapów oceny, ponieważ wybór niektórych środków technicznych lub organizacyjnych może wpłynąć na prawdopodobieństwo wystąpienia zagrożenia wynikającego z przetwarzania lub jego wagę. Fakt, że aktualizacja oceny skutków dla ochrony danych może okazać się konieczna już po rozpoczęciu procesu przetwarzania, nie uzasadnia odroczenia lub nieprzeprowadzenia oceny skutków dla ochrony danych. Ocena skutków dla ochrony danych jest procesem ciągłym, szczególnie gdy operacja przetwarzania przebiega dynamicznie i podlega ciągłym zmianom”[457]. W trakcie jej przeprowadzania administrator musi wziąć pod uwagę co najmniej:

– systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
– ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

[456] Komunikat PUODO z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, „Monitor Polski” 2019 r. poz. 666.

[457] Grupa Robocza art. 29 ds. ochrony danych. Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzania „może powodować wysokie ryzyko” co celów rozporządzenia 2016/679. Przyjęte w dniu 4 kwietnia 2017 r. Ostatnio zmienione i przyjęte w dniu 4 października 2017 r., s. 17.

– ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
– środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy[458].

W przypadku, gdy po dokonanej ocenie okaże się, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania, konsultuje się on z PUODO[459]. „Z sytuacją taką będziemy mieli do czynienia, kiedy administrator oszacuje ryzyka, lecz nie będzie mógł znaleźć rozsądnych środków z punktu widzenia dostępnych technologii i kosztów wdrożenia, które by eliminowały wysokie ryzyko naruszenia praw lub wolności osób fizycznych"[460].

Mając na względzie rozwiązania przyjęte na gruncie art. 35 RODO, należy stwierdzić, że ocena skutków dla ochrony danych pełni rolę narzędzia, „które odpowiednio wbudowane w kulturę organizacyjną zapewni wysoką ochronę danych. Pozwoli na ich bezpieczne przetwarzanie"[461]. Aby stało się to jednak możliwe, administrator w trakcie tej oceny musi rozważyć m.in. wdrożenie odpowiednich środków technicznych i organizacyjnych. Ich przykłady wskazane zostały w art. 32 ust. 1 RODO. Zalicza się do nich:

– pseudonimizację i szyfrowanie danych osobowych;

[458] Art. 35 ust. 7 RODO. Zob. szerzej na ten temat, A. Mednis, *Wymóg oceny skutków...*, s. 31 i n.

[459] Art. 36 ust. 1 RODO.

[460] M. Jabłoński, J. Węgrzyn, *Zmiana modelu ochrony danych…*, s. 80.

[461] M. Więckowska, *Przewodnik po ocenie skutków dla ochrony danych,* „ABI Expert" 2017, nr 1, s. 48.

– zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
– zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
– regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Odnosząc się do powyższego wyliczenia, dostrzeżemy, że prawodawca unijny w pierwszej kolejności zwraca uwagę na dwa środki techniczne, przy czym definiuje tylko jeden z nich. Mowa tu o pseudonimizacji, przez którą należy rozumieć, „przetworzenie danych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”[462]. Jako przykład można wskazać posługiwanie się przez podmiot zobowiązany „zamiast imieniem i nazwiskiem, przypisanym konkretnej osobie fizycznej numerem identyfikacyjnym. Lista numerów wraz z powiązanymi nazwiskami znajduje się wtedy w innym miejscu i nie jest dostępna jednocześnie z głównym zbiorem danych”[463]. Aby jednak zapewnić skuteczność pseudonimizacji, konieczne jest „zachowanie w tajemnicy:

– stosowanej metody oraz jej atrybutów, np. hasła lub klucza;
– stosowanych funkcji i procedur;
– stosowanych pomocniczych zestawów danych;
– użytych narzędzi, służących do zmiany danych osobowych do postaci chroniącego je pseudonimu.

[462] Art. 4 pkt 5 RODO.
[463] http://lexmanual.pl/2018/02/rodo-pseudonimizacja/ [dostęp: 10.09.2021].

Zaleca się także, aby zastosowana metoda pseudonimizacji i jej atrybuty były unikalne dla każdej instancji i rodzaju procesu pseudonimizującego. Ma to na celu zmniejszenie powtarzalności stosowania tych samych rozwiązań z takimi samymi parametrami, które może doprowadzić do kompromitacji techniki ochronnej i ujawnienia sposobu wykonywania operacji odwrotnej (depseudonimizacja), pozwalającej na poznanie zawartości chronionych spseudonimizowanych danych"[464]. Drugim, rekomendowanym przez prawodawcę unijnego środkiem technicznym jest szyfrowanie. Polega ono na „przekształceniu danych w nieodczytywalny bez znajomości odpowiedniego klucza ciąg znaków"[465], co ma ogromny wpływ na bezpieczeństwo danych znajdujących się np. w komputerach stacjonarnych, urządzeniach mobilnych czy chmurze.

Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania to wymóg określający cechy, jakie powinny spełniać systemy i usługi, aby zagwarantować bezpieczeństwo przetwarzania danych osobowych. Pomimo braku dookreślenia przez prawodawcę unijnego wymienionych wyżej cech należy przyjąć, że „poufność realizowana będzie np. poprzez zastosowanie odpowiednich indywidualnych identyfikatorów systemowych dla użytkowników i nadanie im stosownych uprawnień, a zatem kontrolę dostępu do systemów i usług"[466]. Nadawane uprawnienia powinny być jednak „przydzielone zależnie od sprawowanej funkcji i wykonywanego zakresu obowiązków. Zalecane są takie systemy, gdzie uprawnienia dostępu do danych uzależnione są w pewnym stopniu od

[464] M. Kołodziej, *Pseudonimizacja w RODO – kiedy i jak stosować?,* „ABI Expert" 2018, nr 2, s. 44 i n.

[465] D. Lubasz, *Komentarz do art. 32 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 700.

[466] *Ibidem,* s. 702.

miejsca, jakie użytkownik zajmuje w strukturze organizacyjnej”[467] konkretnej organizacji (np. przedsiębiorstwo finansowe, prywatna klinika, szpital) „i przydzielane są z uwzględnieniem wykonywanych zadań (ról). Na przykład dla osoby zatrudnionej na stanowisku pielęgniarki na oddziale X, domyślnie powinny być przypisywane uprawnienia dostępu do danych osób leczonych tylko na tym oddziale. W przypadku, gdy wystąpi potrzeba obsługi pacjentów innego oddziału, uprawnienia te powinny być stosownie zmodyfikowane. Ich zakres z kolei powinien być odpowiedni do czynności, które ta pielęgniarka wykonuje lub ma prawo wykonywać, w zakresie przydzielonych jej zdań”[468].

Integralność to druga cecha, jaką powinny spełniać systemy i usługi związane z przetwarzaniem danych osobowych. Chodzi tu o zapewnienie spójności, dokładności, a także i wiarygodności przetwarzanych danych za pomocą takich rozwiązań, jak np. program antywirusowy, *firewall*[469], które chronią przed różnymi zagrożeniami, np.

[467] https://www.zdrowie.abc.com.pl/aktualnosci/rodo-nie-wskazuje-srodkow-i-metod-zabezpieczania-danych-jedynie-daje-wskazowki,117451.html [dostęp: 10.09.2021].

[468] *Ibidem.*

[469] *Firewall*, „czyli zapora ogniowa to usługa, urządzenie lub program, który jest jednym z zabezpieczeń komputera przed włamaniem dokonywanym przez hakerów. Zadaniem zapory jest filtrowanie danych wychodzących i przychodzących do komputera poprzez sieć lub Internet. Najczęściej firewallem jest dedykowany program, który użytkownik instaluje w systemie operacyjnym. Bywa także usługa, którą można aktywować u operatora internetowego za drobna opłatą, lub elementem infrastruktury sieciowej – osobnym komputerem, modułem sieciowym lub elementem routera. Firewall zapewnia filtrowanie danych przychodzących (pobieranych), jak i wychodzących (wysyłanych) z komputera. Aby filtrowanie było skuteczne, każdy z producentów oprogramowania lub sprzętu do tego typu zadań opracowuje reguły, według których programy są klasyfikowane na bezpieczne, podejrzane i niebezpieczne. Dzięki temu zaraz po instalacji i przeskanowaniu systemu operacyjnego oznacza bezpieczne aplikacje i ustala dla nich możliwość bezproblemowego pobierania i wysyłania danych. Programy niebezpieczne oznacza i raportuje użytkownikowi jako zablokowane. Potencjalnie niebezpieczne to takie, których nie sklasyfikował producent lub decyzję pozostawia użytkownikowi. W większości przypadków można samemu zdecydować, jakie programy mają mieć możliwość pobierania i wysyłania informacji – osobno dla jednych i drugich operacji. Każdy firewall oferuje dziennik dokonywanych operacji, gdzie mogą być zapisywane wszelkie próby włamań, które hakerzy będą próbowali doko-

złośliwym oprogramowaniem, których skutkiem może być m.in. usunięcie danych, ich modyfikacja czy zniekształcenie. Niemniej ważne znaczenie dla bezpieczeństwa danych osobowych ma kolejna cecha, a mianowicie dostępność systemu i usług przetwarzania danych w każdym czasie niezależnie od występujących zakłóceń, np. „przerwy w dostawie prądu, błędów sprzętowych lub błędów oprogramowania, braku dostępu do sieci z przyczyn tak leżących po stronie dostawców, jak i z przyczyn wewnętrznych. Mechanizmy zapewnienia dostępności związane są zatem z usuwaniem tego typu ryzyk, którego zakres należy zdiagnozować *ad casum,* dobierając odpowiednie środki zaradcze, jak np. wdrożenie rozwiązań utrzymywania zasilania (UPS), tworzenie kopii zapasowych, backup systemowy i sprzętowy”[470]. Wskazane rozwiązania z pewnością są bardzo ważne dla wielu podmiotów zobowiązanych, a zwłaszcza tych, które świadczą np. usługi telemedyczne. W ich przypadku nawet krótkotrwały brak dostępności systemu mógłby przyczynić się do pogorszenia zdrowia pacjenta lub utraty życia. W celu zapewnienia więc wysokiego poziomu bezpieczeństwa podmiot zobowiązany powinien zwrócić także uwagę na odporność syste-

nać. Pamiętać należy, że prócz hakerów w sieci krążą specjalne programy (boty), które automatycznie skanują wszelkie numery IP (sieciowe identyfikatory komputerów) próbując znaleźć niezabezpieczone maszyny. Wykryte furtki niemal od razu są wykorzystywane przez automatyczne skrypty po to, by zaszczepić w nich tak zwane trojany. Programy te, działając w tle, mogą wykradać informacje takie, jak choćby hasła do witryn banków, baz danych, poczty elektronicznej, etc. Dane te mogą posłużyć do wykradania pieniędzy z kont użytkownika, zablokowania ważnych danych i szantażowania właściciela, szpiegostwa przemysłowego i innych przestępstw. Program taki może też służyć do zdalnego wysyłania niepożądanych reklam (spam) lub dokonywania wcześniej wymienionych przestępstw, co może przysporzyć właścicielowi nie lada problemów. […]. Pamiętajcie, że firewall nie zastąpi programu antywirusowego, lecz doskonale z nim współpracuje i tworzy tandem podstawowej ochrony przed włamaniami i niebezpiecznym oprogramowaniem. Mimo skuteczności takich rozwiązań nic nie zastąpi zdrowego rozsądku i ostrożności”, https://www.akademiakomputronik.pl/artykul/co-to-jest-firewall-i-czy-jest-mi-potrzebny [dostęp: 10.09.2021].

[470] D. Lubasz, *Komentarz do art. 32 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…,* s. 702 i n.

mów i usług przetwarzania danych przed różnego rodzaju atakami z zewnątrz, np. atak DoS lub DDoS[471], który uniemożliwia korzystanie z systemu. Aby skutecznie zapobiegać potencjalnym zagrożeniom, należy zatem korzystać z dostępnych na rynku rozwiązań w postaci oprogramowania i dedykowanych urządzeń.

Kolejną ważną wskazówką dla administratora i podmiotu przetwarzającego jest, aby w dążeniu do zapewnienia bezpieczeństwa przetwarzania danych wdrażali oni takie środki techniczne i organizacyjne, które w razie incydentu fizycznego (np. zalanie, awaria zasilania, pożar, włamanie do pomieszczenia ze sprzętem informatycznym) lub technicznego (np. awaria serwera, awaria komputera, zainfekowanie systemu przez wirusy komputerowe) zapewnią zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich[472]. W dążeniu tym nie można jednak zapomnieć o regularnym testowaniu, mierzeniu i ocenie skuteczności środków technicznych i organizacyjnych, które po pewnym czasie mogą przecież okazać się nieadekwatne do ryzyka związanego z przetwarzaniem danych osobowych.

Jak wynika z rozwiązań przyjętych w art. 32 ust. 1 RODO, prawodawca unijny odniósł się w nim do przykładowych środków technicznych i organizacyjnych, które mogą być zastosowane, aby zapewnić adekwatny do zagrożeń stopień bezpieczeństwa przetwarzanych

[471] Ataki typu DoS *(Denial of Service)* „mają na celu utrudnienie lub całkowite uniemożliwienia normalnego działania witryny internetowej, sieci, serwera lub innych zasobów. Hakerzy i twórcy wirusów używają różnych metod do przeprowadzenia ataków DoS. Typowe ataki DoS przeciążają serwery nieustającymi żądaniami. […]. Ataki typu DDoS *(Distributed Denial of service)* różni się od ataku DoS jedynie wykorzystywaną metodą. Atak DDoS przeprowadzany jest równocześnie z wielu komputerów. Hakerzy lub twórcy wirusów zazwyczaj używają zaatakowanego komputera jako komputer «master» oraz koordynują atak pośród innych, tak zwanych komputerów «zombie». Zarówno komputery zombie jak i master są atakowane przez wykorzystywanie luki w oprogramowaniu w celu zainstalowania trojana lub innego szkodliwego kodu", https://www.securelist.pl/glossary/6234,atak_dos.html [dostęp: 10.09.2021].

[472] Zob. na ten temat: A. Cieślik, *Bezpieczeństwo systemów IT zgodne z RODO,* „ABI Expert" 2017, nr 1, s. 33.

danych bez wskazywania jakichkolwiek technik. W doborze tych środków administrator i podmiot przetwarzający musi jednak wziąć pod uwagę kryteria, takie jak: stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cel przetwarzania. Podmiot zobowiązany nie może zatem, powołując się np. na kryterium kosztu, uchylić się od zastosowania danego środka. „Kryterium kosztów podlega ocenie przez pryzmat zasady proporcjonalności, dla zastosowania której punktem odniesienia jest cel w postaci odpowiedniego poziomu ochrony. Istnieje zatem korelacja pomiędzy akceptowalnymi z punktu widzenia analizowanej przesłanki kosztami a ryzykiem i relacja ta ma charakter wprost proporcjonalny, tzn. im większe jest stwierdzane ryzyko, tym większe mogą być adekwatne koszty wdrożenia środków technicznych i organizacyjnych zapewniających odpowiedni poziom ochrony”[473].

W praktyce dobór odpowiednich do zagrożeń środków technicznych i organizacyjnych może okazać się dość problematyczny, zwłaszcza dla tych podmiotów, które przed reformą ochrony danych nie przywiązywały do tego zagadnienia większej niż powinny uwagi. Wsparciem dla wszystkich podmiotów zobowiązanych w doborze tych środków powinny być udostępniane przez Prezesa Urzędu Ochrony Danych Osobowych na stronie podmiotowej w Biuletynie Informacji Publicznej, rekomendacje określające środki technicznej i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych[474], które, miejmy nadzieję, już niebawem zostaną przygotowane. W procesie tym nie można pominąć roli inspektora ochrony danych osobowych, którego administrator i podmiot przetwarzający mają obowiązek wyznaczyć w przypadkach wskazanych

[473] D. Lubasz, *Komentarz do art. 32 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 698.

[474] Art. 53 ust. 1 pkt 4 ustawy z 10 maja 2018 r. o ochronie danych osobowych.

w art. 37 ust. 1[475] RODO. Jego zadaniem jest m.in. doradzanie administratorowi i podmiotowi przetwarzającemu w doborze środków technicznych i organizacyjnych adekwatnych do zagrożeń oraz rodzaju danych objętych ochroną, a także „czuwanie" nad wdrożonymi już środkami.

Odnosząc się do zagadnienia dotyczącego bezpieczeństwa przetwarzania danych, o którym mowa w art. 32 RODO, nie można pominąć kwestii związanej z dokumentacją przetwarzania. W przepisie tym prawodawca unijny pominął ten wymóg, co nie oznacza zwolnienia administratora i podmiotu przetwarzającego z obowiązku wykazania, jakie środki techniczne i organizacyjne zostały wdrożone w celu zagwarantowania adekwatnego do ryzyka bezpieczeństwa danych. Na mocy art. 30 RODO, administrator ma bowiem obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, natomiast podmiot przetwarzający – rejestru wszystkich kategorii czynności przetwarzania dokonanych w imieniu administratora[476], w których

[475] Zgodnie z art. 37 ust. 1 RODO, „Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10" – Sprostowanie do art. 37 ust. 1 lit. c) 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 (ogólne rozporządzenie o ochronie danych), OJ L 127/2, 23.5.2018.

[476] Przykłady takich rejestrów dostępne są na stronie: https://uodo.gov.pl/pl/123/214 [dostęp: 10.09.2021]. Zob. na ten temat, M. Młotkiewicz, *Rejestry czynności – przydatny instrument rozliczalności,* „ABI Expert" 2017, nr 3, s. 24 i n.

to rejestrach zamieszcza się m.in. jeżeli to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO. Z uwagi na charakter tego opisu w praktyce sprowadza się on do wskazania informacji na temat wdrożonych zabezpieczeń, np. kontroli dostępu do systemu informatycznego opartego na loginie i haśle, szyfrowania transmisji danych, stosowania systemu antywirusowego, systemu wykrywania włamań, zamykania szaf w pomieszczeniach, w których przechowywane są dane. Od obowiązku prowadzenia rejestru, prawodawca unijny wprowadził w art. 30 ust. 5 wyjątek względem przedsiębiorców lub podmiotów zatrudniających mniej niż 250 osób. W tym samym przepisie wskazał jednak, że zwolnienie nie dotyczy przypadku, gdy:

– przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
– nie ma charakteru sporadycznego lub
– obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych, o czym mowa w art. 10,

co świadczy, że „krąg podmiotów zobowiązanych do prowadzenia rejestru”[477] jest bardzo szeroki.

Z wyjątkiem rozwiązań przyjętych w art. 30 RODO, należy zwrócić także uwagę na art. 24 ust. 2, który przewiduje względem administratora fakultatywne wdrożenie odpowiednich polityk ochrony danych, „które jest zależne od dokonanej oceny użyteczności tych dokumentów z punktu widzenia realizacji obowiązków nałożonych na niego w art. 24 ust. 1 (a więc wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie

[477] P. Siemieniak, *Wymagania dokumentacyjne przetwarzania danych,* „ABI Expert” 2017, nr 2, s. 31.

z RODO – przyp. M.J. i J.W.), a także art. 25”[478]. W opracowaniu tych polityk administratorzy mogą wzorować się na obowiązującym – przed reformą ochrony danych – rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 2004 r.[479], które nakładało na administratorów obowiązek prowadzenia dokumentacji przetwarzania danych osobowych w formie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym[480], tym bardziej że przepisy RODO nie dookreślają, co powinny zawierać polityki ochrony danych. Nic nie stoi zatem na przeszkodzie, aby np. jednym z elementów polityki ochrony danych był sposób przepływu danych między poszczególnymi systemami, który stanowił obligatoryjny element polityki bezpieczeństwa. Udokumentowanie tego sposobu może okazać się „bardzo przydatne, ponieważ ułatwi to panowanie nad tym, gdzie i w jaki sposób są przesyłane dane osobowe. Przepływy danych mogą dotyczyć procesów obiegu informacji między odpowiednimi komórkami organizacyjnymi administratora, przepływu danych w systemach systemów wewnętrznych (np. serwery, serwery baz danych, serwery plików) oraz przepływu danych do systemów zewnętrznych podmiotów, z którymi administrator danych współpracuje (np. zewnętrzne API, serwery plików). Na podstawie informacji, gdzie i w jaki sposób trafiają dane osobowe, o wiele prostsze będzie określenie np., czy dane są przekazywane w sposób prawidłowy lub czy została uwzględniona zasada minimalizmu w zakresie udostępniania danych”[481]. Ponadto, administratorowi łatwiej bę-

[478] D. Lubasz, *Komentarz do art. 30 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 665 i n.

[479] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz. U. z 2004 r. Nr 100, poz. 1024.

[480] Szerzej na ten temat, M. Sztąberek, K. Ułasiuk, *Bezpieczeństwo danych osobowych. Praktyczny przewodnik,* Wrocław 2017, s. 83 i n.

[481] P. Siemieniak, *op. cit.,* s. 30.

dzie zrealizować prawo do bycia zapomnianym, zwłaszcza że zobowiązany on jest w razie upublicznienia danych osobowych, które ma obowiązek usunąć do poinformowania administratorów przetwarzających dane osobowe, że osoba której dane dotyczą, żąda by usunęli oni wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

Poza wskazanymi wyżej rozwiązaniami należy wspomnieć także o możliwości wywiązania się administratora z obowiązku zapewnienia bezpieczeństwa przetwarzania danych poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji[482]. Otwarcie prawodawcy unijnego na pierwszy z tych instrumentów, tj. kodeks postępowania, uzasadnione jest „przede wszystkim trudnością w projektowaniu rozwiązań legislacyjnych adekwatnych dla szerokiego katalogu administratorów i podmiotów przetwarzających, a przy tym jednocześnie wystarczająco precyzyjnych, aby stanowić dokładne wytyczne co do organizacji procesów przetwarzania. Dlatego na poziomie rozporządzenia ustanowiono kluczowe obowiązki i zasady przetwarzania, a ich ewentualna konkretyzacja i uzupełnienie na poziomie wykonawczym może się odbywać w ramach danej branży"[483]. Kodeksy te mogą opracowywać, zmieniać lub rozszerzać ich zakres, zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Należy zatem zachęcać podmioty uprawnione do tego typu czynności, aby „ułatwić skuteczne stosowanie niniejszego rozporządzenia, z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw"[484]. Monitorowaniem zatwierdzonych przez PUODO kodeksów postępowania zajmuje się podmiot dysponujący

[482] Art. 32 ust. 3 RODO.

[483] K. Witkowska-Nowakowska, *Kodeksy postępowania i certyfikacja,* [w:] D. Lubasz (red.), *RODO w e-commerce,* Warszawa 2018, s. 275.

[484] Motyw 98 RODO.

odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i akredytowany w tym celu przez PUODO[485]. Podmiot ten uprawniony jest do podejmowania odpowiednich działań, gdy dojdzie do naruszenia kodeksu przez administratora lub podmiot przetwarzający, w tym zawiesza lub wyklucza te podmioty spośród stosujących kodeks[486]. O działaniach tych i powodach ich podjęcia podmiot akredytowany informuje PUODO.

Drugim wskazanym wyżej instrumentem jest certyfikacja[487], której celem zgodnie z motywem 100 RODO, jest możliwość dokonania przez osoby, których dane dotyczą, szybkiej oceny stopnia ochrony danych, której podlegają stosowne produkty i usługi. Certyfikacji dokonuje PUODO lub podmiot certyfikujący[488], na wniosek administra-

[485] Zob. art. 41 ust. 1 RODO. Zgodnie z art. 41 ust. 2 RODO Podmiot ubiegający się o akredytację, „może zostać akredytowany w celu monitorowania przestrzegania kodeksu postępowania jeżeli:

a) w sposób satysfakcjonujący wykazał on właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu;
b) dysponuje procedurami, które pozwalają mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania;
c) dysponuje procedurami i strukturami, które pozwolą rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwalają zapewnić przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz
d) w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów".

[486] Zob. art. 41 ust. 4 RODO. Zob. szerzej: U. Góral, P. Makowski, *Komentarz do art. 41 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO.*…, s. 836 i n.

[487] Zob. na ten temat, J. Anisimowicz, *Akredytacja dla podmiotów certyfikujących oraz przebieg procesu certyfikacji,* „ABI Expert" 2017, nr 4, s. 30 i n.

[488] Akredytacji podmiotom certyfikującym, które dysponują wiedzą fachową w dziedzinie ochrony danych, udziela Polskie Centrum Akredytacji (art. 12 ust. 1 u.o.d.o. 2018). Podmioty te zostają akredytowane, w przypadku gdy:

a) „w sposób satysfakcjonujący wykazały właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie podlegającej certyfikacji;

tora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek[489].

Zapewnienie adekwatnego do ryzyka poziomu bezpieczeństwa danych osobowych wymaga indywidualnego dobrania przez administratora odpowiednich środków technicznych i organizacyjnych. W doborze tych środków podmiot ten zobowiązany jest uwzględnić stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze. Powyższe rozwiązanie jest przykładem przyjętego w RODO podejścia opartego na ryzyku. W praktyce oznacza to, że administratorzy muszą samodzielnie dokonać analizy ryzyka związanego z przetwarzaniem danych, aby dobrać odpowiednie do zagrożeń środki techniczne i organizacyjne, które mają zapewnić bezpieczeństwo danych osobowych. Kilka przykładów takich środków bez wskazywania konkretnych technik prawodawca unijny wymienia w art. 32 ust. 1 RODO, co świadczy o konsekwentnym zachowaniu przez niego neutralności technicznej przyjętych regulacji. Neutralność ta wydaje się spowodowana pojawianiem się coraz to nowszych zagrożeń, które wymagają od administratora dokonywania przeglądów i aktualizacji przyjętych zabezpie-

b) zobowiązały się do przestrzegania kryteriów, o których mowa w art. 42 ust. 5 i które zostały zatwierdzone przez organ nadzorczy właściwy zgodnie z art. 55 lub art. 56 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63;
c) dysponują procedurami wydawania, okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych;
d) dysponują procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie warunków certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający, oraz które zapewniają przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz
e) w sposób satysfakcjonujący wykażą właściwemu organowi nadzorczemu, że ich zadania i obowiązki nie powodują konfliktu interesów", art. 43 ust. 2 RODO.

[489] Art. 15 ust. 1 u.o.d.o. 2018.

czeń. Oceniając stopień bezpieczeństwa, administrator musi pamiętać, aby uwzględnić w szczególności ryzyko wiążące się z przetwarzaniem, mogącym wynikać m.in. z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych[490]. Wymagające podkreślenia przy realizacji obowiązku zapewnienia bezpieczeństwa przetwarzania jest to, że prawodawca unijny nie przewidział prowadzenia w tym zakresie specjalnej dokumentacji. Wykazaniu tego obowiązku służy prowadzony przez administratorów – oczywiście z uwzględnieniem przewidzianego w art. 30 ust. 5 wyłączenia – rejestr czynności przetwarzania, którego częścią składową jest, o ile to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO. W porównaniu z poprzednio obowiązującymi regulacjami z zakresu ochrony danych osobowych, obecne rozwiązania nie przewidują także obowiązku prowadzenia dokumentacji przetwarzania w postaci polityk ochrony danych. Niewykluczone jednak jest, że mimo charakteru fakultatywnego tych polityk w praktyce są one wdrażane przez administratorów i to nie tylko z uwagi na ułatwienie im realizacji obowiązku polegającego na prowadzeniu rejestru czynności przetwarzania, ale także ze względu na ułatwienie procesu przetwarzania danych, a w konsekwencji i na wyrażoną w art. 5 ust. 2 RODO zasadę rozliczalności[491], zgodnie z którą, administrator musi być w stanie wykazać przestrzeganie przepisów RODO. W realizacji wskazanego wyżej obowiązku, a także wspomnianej zasady przydatne okazują się dwa mechanizmy przewidziane w RODO, a mianowicie kodeksy postępowania lub certyfikacja.

[490] Art. 32 ust. 2 RODO.

[491] Zob. na ten temat, S. Stefaniak, H. Suszek-Borowska, *Rozliczalność przetwarzania danych a systemy informatyczne,* „ABI Expert" 2018, nr 2, s. 22 i n.

Rozdział V

Środki ochrony prawnej, odpowiedzialność i administracyjne kary pieniężne za naruszenie prawa do bycia zapomnianym

1. Skarga do organu nadzorczego na podmiot zobowiązany do realizacji prawa do bycia zapomnianym

Zagwarantowanie praw osobie, której dane dotyczą, wymaga wdrożenia odpowiednich mechanizmów prawnych, które służyć mają ich egzekwowaniu. Jednym z takich instrumentów jest skarga do organu nadzorczego, z której osoba ta może skorzystać w szczególności w państwie członkowskim swojego zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie jej danych osobowych narusza przepisy RODO[492].

W sytuacji więc, gdy osoba, której dane dotyczą, uzna, że doszło do naruszenia przysługującego jej prawa do bycia zapomnianym, może wystąpić ze skargą do organu nadzorczego[493]. Osoba ta może także umocować do wniesienia tego środka – podmiot, organizację lub zrze-

[492] Art. 77 ust. 1 RODO.

[493] Zgodnie z motywem 146 RODO, przetwarzanie dokonywane w sposób naruszający RODO obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy RODO oraz prawo państwa członkowskiego doprecyzowujące RODO.

szenie, jeżeli nie mają one charakteru zarobkowego, zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają cele statutowe leżące w interesie publicznym i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą w związku z ochroną ich danych osobowych[494].

Jak wynika ze wskazanych wyżej rozwiązań, prawodawca unijny zapewnił osobie, której dane dotyczą, prawo wniesienia skargi do organu nadzorczego oparte na jednym z trzech możliwych kryteriów, tj. miejscu swojego zwykłego pobytu, miejscu pracy lub miejscu popełnienia domniemanego naruszenia, które nie zostały jednak w żaden sposób dookreślone. W związku z tym, za miejsce zwykłego pobytu wydaje się, że można uznać miejscowość w państwie członkowskim, w której dana osoba przebywa przez pewien czas bez zamiaru stałego pobytu[495]. Miejsce pracy to z kolei „obszar wykonywania aktywności zawodowej skarżącego"[496]. Natomiast miejscem popełnienia domniemanego naruszenia jest „obszar państwa członkowskiego, w którym dany podmiot działa lub zaniechał działania, do którego był zobowiązany"[497].

Przyjęcie powyższych rozwiązań oznacza, że „podjęciem decyzji w sprawie skargi może […] zająć się organ nadzorczy z innego państwa

[494] Art. 80 ust. 1 RODO.

[495] „Samo przebywanie w danej miejscowości nie stanowi bowiem o zamieszkaniu, lecz musi być połączone z zamiarem stałego pobytu, tj. z takim przebywaniem, które ma cechy założenia tam ośrodka swoich osobistych i majątkowych interesów. Powszechnie przyjmuje się, że oba te elementy – fizyczne przebywanie w danej miejscowości (*corpus*) i zamiar, wola stałego pobytu (*animus*), muszą i występują łącznie. Dla ustalenia miejsca zamieszkania osoby fizycznej nie wystarczy zatem ani samo zamieszkanie w sensie fizycznym, jednak bez zamiaru stałego pobytu, choćby zamieszkanie trwało dłuższy czas, ani sam zamiar stałego pobytu w danej miejscowości niepołączony z przebywaniem w tej miejscowości, przy czym od pojęcia zamieszkania należy odróżnić termin «pobyt», oznaczający fizyczne przebywanie w danym miejscu bez ustalenia zamiaru stałego pobytu", postanowienie Sądu Okręgowego w Toruniu, VIII Cz132/17.

[496] J. Łuczak, *Komentarz do art. 77 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO.…*, s. 1026.

[497] *Ibidem.*

członkowskiego niż państwo administratora"[498], co jest szczególnie ważne z punktu widzenia skarżącego. W sytuacji więc, gdy dojdzie do naruszenia prawa do bycia zapomnianym przez administratora z Holandii, osoba, której dane dotyczą, może wystąpić ze skargą do organu nadzorczego w Polsce, tj. do PUODO, wskazując np. jako kryterium swoje miejsce pracy. Organ nadzorczy może wówczas – co wynika wprost z art. 58 ust. 2 lit. g) RODO – nakazać administratorowi na mocy art. 17 usunięcia danych osobowych oraz nakazać na mocy art. 17 ust. 2 i art. 19 powiadomić o tych czynnościach odbiorców, którym dane osobowe ujawniono i/lub nałożyć zgodnie z art. 83 RODO karę pieniężną, o której piszemy w osobnym punkcie tego rozdziału. Należy jednak mieć na uwadze, że wniesienie skargi do danego organu nadzorczego w tym przypadku do PUODO, nie jest równoznaczne z tym, że to właśnie ten organ będzie rozstrzygał sprawę, której skarga dotyczy. Wynika to z przyjętego mechanizmu kompleksowej współpracy (*one-stop mechanism*), w ramach, którego właściwym do rozpatrywania skarg związanych z transgranicznym przetwarzaniem[499] danych osobowych jest wiodący organ nadzorczy, którego właściwość ustala się w oparciu o główną lub pojedynczą jednostkę organizacyjną[500] administratora lub

[498] N. Zawadzka, *Środki ochrony prawnej, odpowiedzialność i sankcje,* [w:] D. Lubasz (red.), *RODO w e-commerce,* Warszawa 2018, s. 312.

[499] Zgodnie z art. 4 pkt 23 RODO, „Transgraniczne przetwarzanie oznacza:
a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo
b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim".

[500] „Pojęcie «jednostka organizacyjna» zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o odział czy spółkę zależną posiadającą osobowość prawną, nie jest w tym względzie czynnikiem decydującym", motyw 22 RODO.

podmiotu przetwarzającego. W przypadku więc, gdy administrator posiada jednostki organizacyjne w więcej niż jednym państwie członkowskim, główną jednostką organizacyjną jest „miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje”[501]. W przypadku zaś podmiotu przetwarzającego posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim, główną jednostką organizacyjną jest „miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostka organizacyjna podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia”[502].

Od wskazanej wyżej zasady właściwości wiodącego organu nadzorczego prawodawca unijny przewidział kilka wyjątków. Pierwszy z nich dotyczy przetwarzania dokonywanego przez organy publiczne lub podmioty prywatne działające na podstawie art. 6 ust. 1 lit. c) lub e)[503]. Drugi przewiduje możliwość rozpatrzenia skargi przez organ nadzorczy, do którego została ona wniesiona, pomimo że nie ma on statusu wiodącego organu nadzorczego, „jeżeli sprawa dotyczy wyłącznie jednostki organizacyjnej w jego państwie członkowskim lub znacznie wpływa na osoby, których dane dotyczą, wyłącz-

[501] Art. 4 pkt 16 lit. a) RODO.
[502] Art. 4 pkt 16 lit. b) RODO.
[503] Art. 55 ust. 2 RODO.

nie w jego państwie członkowskim”[504]. W takiej sytuacji organ nadzorczy niezwłocznie informuje o danej sprawie organ wiodący, który w terminie trzech tygodni od otrzymania informacji podejmuje decyzję, czy zajmie się daną sprawą zgodnie z procedurą przewidzianą w art. 60 RODO, uwzględniając jednocześnie, czy w państwie członkowskim, którego organ nadzorczy przekazał mu informacje, znajduje się jednostka organizacyjna administratora lub podmiotu przetwarzającego[505]. W razie zajęcia się daną sprawą organ nadzorczy, który przekazał organowi wiodącemu informacje, może przedłożyć projekt decyzji, który w jak największym stopniu powinien uwzględnić wiodący organ nadzorczy, przygotowując projekt własnej decyzji[506]. W przypadku zaś, gdy wiodący organ nadzorczy postanowi nie zająć się daną sprawą, wówczas podejmuje się tego organ nadzorczy, który przekazał informacje wiodącemu organowi nadzorczemu. W takiej sytuacji zastosowanie ma art. 61 i 62 RODO. Z kolei trzeci wyjątek tyczy się trybu pilnego, który ma zastosowanie w wyjątkowych okolicznościach, a mianowicie, gdy organ nadzorczy, którego sprawa dotyczy[507], uzna, że istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, „w szczególności gdy istnieje ryzyko, że wyegzekwowanie prawa przysługującego osobie, której dane dotyczą, może być znacznie utrudnione”[508]. W takim przypadku może on w drodze odstępstwa od mechanizmu spójności lub proce-

[504] Art. 56 ust. 2 RODO.

[505] Art. 56 ust. 3 RODO.

[506] Art. 56 ust. 4 RODO.

[507] Zgodnie z art. 4 pkt 22 RODO, „organ nadzorczy, którego sprawa dotyczy oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:

a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;

b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub

c) wniesiono do niego skargę”.

[508] Motyw 137 RODO.

dury współpracy, niezwłocznie przyjąć środki tymczasowe o określonym okresie obowiązywania, który nie powinien przekraczać trzech miesięcy. O środkach tych oraz powodach ich przyjęcia organ nadzorczy zobowiązany jest niezwłocznie poinformować pozostałe organy nadzorcze, których sprawa dotyczy, Europejską Radę Ochrony Danych i Komisję[509]. Jeżeli organ nadzorczy zastosował środki, o których mowa, i uzna, że istnieje potrzeba pilnego przyjęcia środków o charakterze ostatecznym, może on zwrócić się z uzasadnionym wnioskiem o pilne wydanie opinii lub wiążącej decyzji do Europejskiej Rady Ochrony Danych, która dokonuje tej czynności w terminie dwóch tygodni zwykłą większością głosów swoich członków[510]. Z wnioskiem o pilne wydanie opinii lub wiążącej decyzji może wystąpić również każdy organ nadzorczy, jeżeli właściwy organ nadzorczy nie zastosował odpowiedniego środka w sytuacji, w której istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą[511].

Odnosząc się do zagadnienia związanego z możliwością wniesienia skargi do organu nadzorczego w kontekście transgranicznym, należy pamiętać, że tyczy się ona nie tylko przetwarzania danych osobowych przez administratorów lub podmioty przetwarzające z UE, ale także i spoza niej. Prawodawca unijny przewidział bowiem, że „gdy administrator lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii przetwarza dane osobowe osób, których dane dotyczą, znajdujących się w Unii, a jego czynności przetwarzania wiążą się z oferowaniem towarów lub usług tym osobom w Unii (niezależnie od tego, czy wymaga od tych osób płatności) lub z monitorowaniem ich zachowania (o ile ma ono miejsce w Unii), to taki administrator lub podmiot prze-

[509] Art. 66 ust. 1 RODO.
[510] Art. 66 ust. 2 i 4 RODO.
[511] Art. 66 ust. 3 RODO.

twarzający powinien wyznaczyć przedstawiciela[512], chyba że przetwarzanie ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych, lub jeżeli administrator jest organem lub podmiotem publicznym. Przedstawiciel powinien działać w imieniu administratora lub podmiotu przetwarzającego i może być adresatem ewentualnych działań organu nadzorczego. […] powinien wykonywać swoje zadania zgodnie z upoważnieniem otrzymanym od administratora lub podmiotu przetwarzającego, w tym współpracować z właściwymi organami nadzorczymi w odniesieniu do wszelkich działań służących zapewnieniu przestrzegania RODO"[513]. Przyjęcie powyższych rozwiązań oznacza, że „jeśli przetwarzanie przez administratora spoza Unii Europejskiej odnosi skutek tylko w jednym państwie, wówczas właściwy jest organ nadzorczy tego państwa"[514]. W sytuacji zaś, gdy administrator spoza Unii oferuje towary lub usługi w kilku państwach członkowskich, wówczas „będzie miał tu zastosowanie mechanizm wzajemnej pomocy oraz będą możliwe wspólne operacje organów nadzorczych wobec przedstawicieli

[512] „Przedstawiciel oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia", art. 4 pkt 17 RODO.

[513] Sprostowanie do 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 (ogólne rozporządzenie o ochronie danych), OJ L 127/2, 23.5.2018, motyw 80 RODO. Zob. także art. 27 RODO.

[514] A. Mednis, *Prawo do wniesienia skargi do organu nadzorczego,* [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie RODO,* Wrocław 2017, s. 364.

administratorów z państw trzecich”[515], natomiast nie będzie miał zastosowania mechanizm współpracy i spójności, bowiem tyczy się on wyłącznie „administratorów posiadających jednostkę organizacyjną lub jednostki organizacyjne w Unii Europejskiej. Jeżeli przedsiębiorstwo nie posiada jednostki organizacyjnej w UE, sama obecność przedstawiciela w państwie członkowskim nie powoduje uruchomienia systemu kompleksowej współpracy. Oznacza to, że administratorzy nieposiadający żadnej jednostki organizacyjnej w UE muszą się kontaktować z lokalnymi organami nadzorczymi w każdym państwie członkowskim, w którym działają, za pośrednictwem swoich lokalnych przedstawicieli”[516].

W celu ułatwienia wniesienia skargi do organu nadzorczego organ ten powinien udostępnić jej formularz, który można wypełnić również elektronicznie, nie wykluczając przy tym innych sposobów komunikacji[517]. Na organie nadzorczym ciążą także obowiązki informacyjne, do których zalicza się poinformowanie skarżącego o postępach i efektach rozpatrywania skargi w tym o możliwości skorzystania ze środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu[518] oraz o potrzebie prowadzenia „dalszego postępowania wyjaśniającego lub koordynacji działań z innym organem nadzorczym”[519].

W przypadku więc, gdy skarga składana jest do organu nadzorczego w Polsce, tj. PUODO, musi ona zawierać:

1) imię i nazwisko oraz adres zamieszkania składającego skargę;

[515] *Ibidem.*

[516] Grupa Robocza Art. 29, Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego, przyjęte w dniu 13 grudnia 2016 r. Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r., s. 12. Wytyczne dostępne na stronie: https://www.giodo.gov.pl/pl/1520344/10392 [dostęp: 10.09.2021]. Por. M. Piech, *One stop shop. Mechanizmy podejmowania decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE,* „Monitor Prawniczy” 2016, nr 20, s. 85.

[517] Art. 57 ust. 2 RODO.

[518] Art. 77 ust. 2 RODO.

[519] Motyw 141 RODO.

2) wskazanie podmiotu, na który składana jest skarga (nazwę/imię i nazwisko oraz adres siedziby/zamieszkania);
3) dokładny opis naruszenia;
4) żądanie, tj. wskazanie, podjęcia jakich działań składający oczekuje od organu (np. usunięcia danych, wypełnienia obowiązku informacyjnego, sprostowania danych, ograniczenia przetwarzania danych itd.);
5) własnoręczny podpis[520].

Jeżeli skarga składana jest w formie elektronicznej, to oprócz wskazanych wyżej wymogów musi być ona:

a) „opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym, lub uwierzytelniona w sposób zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej,
b) zawierać adres elektroniczny wnoszącego”[521].

W przypadku składania skargi w formie elektronicznej przez pełnomocnika, „pełnomocnictwo w formie dokumentu elektronicznego powinno być opatrzone […] kwalifikowanym podpisem elektronicznym albo podpisem zaufanym albo podpisem osobistym. Jeżeli odpisy pełnomocnictw lub odpisy innych dokumentów wykazujących umocowanie zostały sporządzone w formie dokumentu elektronicznego, to ich uwierzytelnienia dokonuje się opatrując odpisy kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Uwierzytelniane elektronicznie odpisy pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie muszą być sporządzane w formatach danych zgodnych z ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne”[522].

[520] https://uodo.gov.pl/pl/83/154 [dostęp: 10.09.2021].
[521] https://uodo.gov.pl/pl/83/153 [dostęp: 10.09.2021].
[522] *Ibidem.*

Z uwagi na to, że przepisy RODO nie określają procedury rozpatrywania skargi, powoduje to „potrzebę stosowania krajowych przepisów proceduralnych”[523], do których zalicza się ustawę o ochronie danych osobowych z 10 maja 2018 r., która w rozdziale 7 odnosi się do tego zagadnienia.

2. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi za naruszenie prawa do bycia zapomnianym

Naruszenie przez administratora lub podmiot przetwarzający praw przysługujących osobie, której dane dotyczą, gwarantuje jej możliwość skorzystania ze środka ochrony prawnej przed sądem niezależnie od skargi do organu nadzorczego czy innych środków ochrony prawnej. Postępowanie przeciwko wskazanym podmiotom wszczyna się przed sądem państwa członkowskiego, w którym posiadają one jednostkę organizacyjną. Postępowanie takie może jednak zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, jeżeli administrator lub podmiot przetwarzający nie są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne (art. 79 ust. 2 RODO)[524].

Odnosząc się do zagadnienia dotyczącego ochrony prawnej przed sądem, o której mowa w art. 79 RODO, należy zwrócić uwagę na motyw 147, w którym prawodawca unijny wyraźnie zaakcentował, że jeżeli RODO „przewiduje szczegółowe przepisy o jurysdykcji – w szczególności odnośnie do postępowań w zakresie środków ochrony prawnej

[523] G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia,* „Monitor Prawniczy” 2016, nr 20, s. 19.

[524] Por. motyw 145 RODO.

przed sądem, w tym odszkodowania, przeciwko administratorowi lub podmiotowi przetwarzającemu – ogólne przepisy o jurysdykcji, takie jak rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012, nie powinny naruszać stosowania takich szczegółowych przepisów". Nie ulega więc wątpliwości, że szczególnym przepisem jest nie tylko wskazany wyżej art. 79 ust. 2, ale także i art. 81 RODO, na mocy którego przyjęto, że jeżeli właściwy sąd państwa członkowskiego posiada informację, iż przed sądem w innym państwie członkowskim prowadzone jest postępowanie w tej samej sprawie w odniesieniu do przetwarzania przez tego samego administratora lub ten sam podmiot przetwarzający, kontaktuje się z tym sądem w innym państwie członkowskim, aby potwierdzić istnienie takiego postępowania. Poza tym właściwy sąd, inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić swoje postępowanie, a jeżeli postępowania toczą się w pierwszej instancji, może także – na wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji, jeżeli sąd, przed którym jako pierwszym wszczęto postępowanie, ma jurysdykcję względem przedmiotowych spraw, a jego prawo dopuszcza ich połączenie.

Jak wynika ze wskazanego wyżej motywu, prawodawca unijny przyznał pierwszeństwo przepisom RODO odnośnie do kwestii jurysdykcyjnych przed ogólnymi przepisami o jurysdykcji, takimi jak rozporządzenie 1215/2012. Wobec tego pojawia się pytanie „czy uznawanie i wykonywanie orzeczeń zapadłych w takich sprawach o charakterze transgranicznym będzie następować na podstawie rozporządzenia 1215/2012. Wydaje się, że odpowiedź powinna być twierdząca"[525], tym bardziej że przepisy RODO „nie regulują w sposób kompleksowy zagadnień jurysdykcyjnych związanych z dochodzeniem roszczeń od ad-

[525] W. Kuberska, *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu,* [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie RODO,* Wrocław 2017, s. 396.

ministratora czy podmiotu przetwarzającego”[526], w związku z czym „muszą być one uzupełniane innymi normami, które nie naruszają tych przepisów szczególnych”[527]. „W konsekwencji takie orzeczenia, ugody i inne dokumenty pochodzące z innych państw członkowskich Unii Europejskiej powinny być uznane za objęte rozporządzeniem 1215/2012 i powinny stanowić tytuły wykonawcze w Rzeczypospolitej Polskiej na podstawie art. 1153^{14} kpc. Odmienna interpretacja prowadziłaby do pogorszenia sytuacji stron z transgranicznych postępowań z zastosowaniem środka ochrony prawnej z art. 79 RODO w porównaniu ze stronami innych spraw cywilnych i handlowych regulowanych rozporządzeniem 1215/2012”[528].

Mając powyższe na względzie, nie jest zatem wykluczone, że w przypadku gdy dojdzie do naruszenia prawa do bycia zapomnianym przez administratora, który posiada jednostkę organizacyjną w Polsce, a skarżący zwróci się o rozpoznanie sprawy do sądu właściwego ze względu na jego miejsce zwykłego pobytu, którym jest Belgia, to wówczas właściwy będzie sąd belgijski. W przypadku zaś, gdy naruszenia wskazanego wyżej prawa dokona administrator posiadający jednostkę organizacyjną w Belgii, a skarżący zwróci się o rozpoznanie sprawy do sądu właściwego ze względu na jego miejsce zwykłego pobytu, którym jest Polska, wówczas właściwy będzie sąd okręgowy, co wynika z art. 93 u.o.d.o. 2018. Sąd ten zawiadamia niezwłocznie PUODO o wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia prawa do bycia zapomnianym[529]. Z kolei PUODO zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej

[526] J. Łuczak, *Komentarz do art. 79 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 1039.

[527] *Ibidem.*

[528] W. Kuberska, *op. cit.*, s. 396. Zob. także W. Kuberska, *Środek ochrony prawnej przed sądem,* „ABI Expert” 2017, nr 4, s. 51 i n.

[529] Art. 94 ust. 1 u.o.d.o. 2018.

tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed PUODO lub sądem administracyjnym albo została zakończona. PUODO informuje również sąd o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia[530]. Przy czym, jeżeli sprawa, o której mowa, została wszczęta przed PUODO, sąd zawiesza wówczas postępowanie[531]. Sąd umarza zaś postępowanie w zakresie, w jakim prawomocna decyzja PUODO o stwierdzeniu naruszenia przepisów o ochronie danych osobowych uwzględnia roszczenie dochodzone przed sądem[532]. Odnośnie do postępowania przed sądem w przypadku naruszenia przez administratora prawa do bycia zapomnianym należy wspomnieć, że PUODO może występować za zgodą powoda do postępowania przed sądem w każdym jego stadium[533], chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych[534]. W takim sytuacji do PUODO stosuje się odpowiednio przepisy Kodeksu postępowania cywilnego[535] o prokuraturze[536].

3. Prawo do odszkodowania i odpowiedzialność w razie naruszenia prawa do bycia zapomnianym

W razie naruszenia przez administratora lub podmiot przetwarzający przepisów RODO, każda osoba, która poniosła z tego tytułu

[530] Art. 94 ust. 2 u.o.d.o. 2018.

[531] Art. 95 u.o.d.o. 2018.

[532] Art. 96 u.o.d.o. 2018.

[533] PUODO, jeżeli uzna, że przemawia za tym interes publiczny, przedstawia sądowi istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, art. 99 u.o.d.o. 2018.

[534] Art. 98 ust. 2 u.o.d.o. 2018.

[535] Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, t.j. Dz. U. z 2019 r. poz. 1460 ze zm.

[536] Art. 98 ust. 3 u.o.d.o. 2018.

szkodę[537] majątkową lub niemajątkową, ma prawo uzyskać od nich odszkodowanie. Odpowiedzialność tych podmiotów będzie jednak zróżnicowana, bowiem administrator odpowiada za każde naruszenie przepisów RODO[538], natomiast podmiot przetwarzający wyłącznie, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające lub gdy działa poza zgodnymi z prawem poleceniami administratora lub wbrew takim poleceniom[539]. Od wskazanej wyżej zasady prawodawca unijny przewidział jednak wyjątek, a mianowicie, gdy administrator lub podmiot przetwarzający udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody[540].

Odnośnie do zasad dotyczących odpowiedzialności odszkodowawczej wyrażonych w art. 82 RODO, należy podkreślić, że w przypadku, gdy w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający, lub uczestniczą w nim oba te podmioty, to wówczas ponoszą oni odpowiedzialność solidarną za całą szkodę, aby zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania[541]. Jeżeli jednak okaże się, że któryś z podmiotów zobowiązanych zapłacił odszkodowanie za całą wyrządzoną szkodę, może on dochodzić roszczeń regresowych wobec pozostałych

[537] Zgodnie z motywem 146 RODO „Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia. Nie ma to wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego". Na temat szkody zob. D. Klimas, P.M. Wróbel, *Prawo do bycia zapomnianym glosa C-121/12*, *Cywilnoprawna odpowiedzialność za naruszenie ochrony danych osobowych na gruncie RODO – wstęp do zagadnienia,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *op. cit.*, s. 113 i n.

[538] „Przetwarzanie dokonywane w sposób naruszający niniejsze rozporządzenie obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy niniejszego rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące niniejsze rozporządzenie", motyw 146 RODO.

[539] Art. 82 ust. 2 RODO.

[540] Art. 82 ust. 3 RODO.

[541] Art. 82 ust. 4 RODO.

administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu.

Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Postępowanie takie może jednak zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, jeżeli administrator lub podmiot przetwarzający nie są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.

Odnosząc się do zagadnienia dotyczącego odpowiedzialności odszkodowawczej administratorów lub podmiotów przetwarzających wobec osoby, która poniosła szkodę w wyniku naruszenia przepisów RODO, należy zwrócić uwagę na motyw 147, w którym prawodawca unijny wyraźnie zaakcentował, że jeżeli RODO „przewiduje szczegółowe przepisy o jurysdykcji – w szczególności odnośnie do postępowań w zakresie środków ochrony prawnej przed sądem, w tym odszkodowania, przeciwko administratorowi lub podmiotowi przetwarzającemu – ogólne przepisy o jurysdykcji, takie jak rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012, nie powinny naruszać stosowania takich szczegółowych przepisów". Nie ulega więc wątpliwości, że szczególnym przepisem jest nie tylko art. 79 ust. 2, ale także i art. 81 RODO, na mocy którego przyjęto, że jeżeli właściwy sąd państwa członkowskiego posiada informację, iż przed sądem w innym państwie członkowskim prowadzone jest postępowanie w tej samej sprawie w odniesieniu do przetwarzania przez tego samego administratora lub ten sam podmiot przetwarzający, kontaktuje się z tym sądem w innym państwie członkowskim, aby potwierdzić istnienie takiego postępowania. Poza tym, właściwy sąd inny niż ten, przed którym jako pierwszym wszczęto postępowanie, może zawiesić swoje postępowanie, a jeżeli postępowania te toczą się w pierwszej in-

stancji, może także – na wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji, jeżeli sąd, przed którym jako pierwszym wszczęto postępowanie, ma jurysdykcję względem przedmiotowych spraw, a jego prawo dopuszcza ich połączenie.

Jak wynika ze wskazanego wyżej motywu, prawodawca unijny przyznał pierwszeństwo przepisom RODO odnośnie do kwestii jurysdykcyjnych przed ogólnymi przepisami o jurysdykcji, takimi jak rozporządzenie 1215/2012. Wobec tego pojawia się pytanie, „czy uznawanie i wykonywanie orzeczeń zapadłych w takich sprawach o charakterze transgranicznym będzie następować na podstawie rozporządzenia 1215/2012. Wydaje się, że odpowiedź powinna być twierdząca”[542], tym bardziej że przepisy RODO „nie regulują w sposób kompleksowy zagadnień jurysdykcyjnych związanych z dochodzeniem roszczeń od administratora czy podmiotu przetwarzającego”[543], w związku z czym „muszą być one uzupełniane innymi normami, które nie naruszają tych przepisów szczególnych”[544]. „W konsekwencji takie orzeczenia, ugody i inne dokumenty pochodzące z innych państw członkowskich Unii Europejskiej powinny być uznane za objęte rozporządzeniem 1215/2012 i powinny stanowić tytuły wykonawcze w Rzeczypospolitej Polskiej na podstawie art. 1153^{14} kpc. Odmienna interpretacja prowadziłaby do pogorszenia sytuacji stron z transgranicznych postępowań z zastosowaniem środka ochrony prawnej z art. 79 RODO w porównaniu ze stronami innych spraw cywilnych i handlowych regulowanych rozporządzeniem 1215/2012”[545].

Mając powyższe na względzie, nie jest zatem wykluczone, że w przypadku gdy dojdzie do naruszenia prawa do bycia zapomnianym

[542] W. Kuberska, *Prawo do skutecznego środka ochrony prawnej…*, s. 396.

[543] J. Łuczak, *Komentarz do art. 79 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 1039.

[544] *Ibidem.*

[545] W. Kuberska, *Prawo do skutecznego środka ochrony prawnej…*, s. 396. Zob. także: W. Kuberska, *Środek ochrony prawnej…*, s. 51 i n.

przez administratora, który posiada jednostkę organizacyjną w Polsce, w wyniku czego osoba, której dane dotyczą, poniosła szkodę, osoba ta będzie mogła wystąpić z roszczeniem o odszkodowanie do sądu właściwego ze względu na miejsce zwykłego pobytu, którym są np. Czechy. W takiej sytuacji postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem czeskim.

W przypadku zaś, gdy naruszenia wskazanego wyżej prawa dokona administrator posiadający jednostkę organizacyjną w Czechach, w wyniku czego osoba, której dane dotyczą, poniosła szkodę, osoba ta może wystąpić z roszczeniem o odszkodowanie do sądu właściwego ze względu na miejsce zwykłego pobytu, którym jest np. Polska. Wówczas postępowanie dotyczące odszkodowania jest wszczynane przed sądem polskim, którym jest sąd okręgowy. Sąd ten zawiadamia niezwłocznie PUODO o wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia prawa do bycia zapomnianym. Z kolei PUODO zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed PUODO lub sądem administracyjnym albo została zakończona. PUODO informuje również sąd o wszczęciu każdego postępowania w sprawie dotyczącego tego samego naruszenia[546].

Ustalenia prawomocnej decyzji PUODO o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów[547]. W sprawach o roszczenia z tytułu

[546] Art. 94 ust. 2 u.o.d.o. 2018.
[547] Art. 97 u.o.d.o. 2018.

naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie przed sądem (np. powództwo z tytułu naruszenia prawa do bycia zapomnianym i łącznie z nim dochodzone roszczenie odszkodowawcze), PUODO może wytaczać powództwa na rzecz osoby, której dane dotyczą, za jej zgodą, a także występować za zgodą powoda do postępowania w każdym jego stadium[548].

4. Administracyjna kara pieniężna jako konsekwencja naruszenia prawa do bycia zapomnianym

W celu zapewnienia skutecznego egzekwowania przepisów RODO prawodawca unijny przyznał organom nadzorczym możliwość nakładania na administratora, podmiot przetwarzający – administracyjnej kary pieniężnej zgodnie z zasadami określonymi w art. 83 RODO. Do rozstrzygnięcia pozostawił natomiast państwom członkowskim, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie[549].

Jak wynika z rozwiązań przyjętych we wskazanym wyżej przepisie, administracyjne kary pieniężne mogą być nakładane w przypadku

[548] Art. 98 ust. 1 u.o.d.o. 2018.

[549] Art. 83 ust. 7 RODO. Zgodnie z art. 102 u.o.d.o. 2018, *PUODO może nałożyć w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych na:*

– jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-12 i 14 ustawy z 27 sierpnia 2009 r. o finansach publicznych. W przypadku jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 13 tej ustawy, administracyjne kary pieniężne nakładane są do 10000 złotych;
– instytut badawczy;
– NBP;

przy czym odbywa się to na podstawie i na warunkach określonych w art. 83 RODO. Por. M. Jabłoński, *Rola i znaczenie RODO w procesie definiowania gwarancji niezależności i spójności krajowego systemu ochrony danych osobowych,* [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda (red.), *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym,* Wrocław 2017, s. 95 i n.

naruszenia przepisów RODO[550]. W zależności jednak od rodzaju naruszeń, wysokość tych kar może być niższa[551] bądź wyższa. Te ostatnie – których górna granica wynosi 20 000 000 euro[552], a w przypadku przedsiębiorstwa[553] 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa[554] – wymierza się m.in. za naruszenie prawa do bycia zapomnianym, o którym mowa w art. 17 RODO. W sytuacji więc, gdy dojdzie do tego typu naruszenia, niewykluczone jest, że organ nadzorczy, tj. PUODO, może nakazać usunięcie danych i nałożyć na administratora karę finansową lub nałożyć tylko karę finansową, co oczywiście uzależnione jest od okoliczności każdego indywidualnego przypadku. Podejmując decyzję o nałożeniu kary i jej wysokości, PUODO musi dokonać indywidualnej oceny zwracając uwagę na:

– charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby po-

[550] „Jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie", art. 83 ust. 3 RODO.

[551] Wymierzana ona jest do wysokości 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, art. 83 ust. 4 RODO.

[552] „Równowartość wyrażonych w euro kwot […], oblicza się w złotych według średniego kursu euro ogłoszonego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, a w przypadku gdy w danym roku Narodowy Bank Polski nie ogłasza średniego kursu euro w dniu 28 stycznia – według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów Narodowego Banku Polskiego", art. 103 u.o.d.o. 2018.

[553] „Jeżeli administracyjna kara pieniężna jest nakładana na przedsiębiorstwo, to «przedsiębiorstwo» należy do tych celów rozumieć zgodnie z art. 101 i 102 TFUE. Jeżeli administracyjna kara pieniężna jest nakładana na osobę niebędącą przedsiębiorstwem, organ nadzorczy, ustalając właściwą wysokość kary pieniężnej, powinien wziąć pod uwagę ogólny poziom dochodów w danym państwie członkowskim oraz sytuację ekonomiczną tej osoby", motyw 150 RODO.

[554] Art. 83 ust. 5 RODO.

szkodowanych osób, których dane dotyczą oraz rozmiaru poniesionej przez nie szkody;
- umyślny lub nieumyślny charakter naruszenia;
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;
- wszelkie wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
- kategorie danych osobowych, których dotyczyło naruszenie;
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
- jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;
- stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz
- wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty[555].

[555] Art. 83 ust. 2 RODO.

PUODO nakłada na administratora, który naruszył prawo do bycia zapomnianym, o którym mowa w art. 17 RODO, karę finansową w drodze decyzji[556]. Karę tę uiszcza się w terminie 14 dni od dnia upływu terminu na wniesienie skargi, albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego[557]. Na uzasadniony wniosek administratora PUODO może odroczyć termin uiszczenia kary pieniężnej albo rozłożyć ją na raty[558], jeżeli przemawia za tym ważny

[556] Tak było w sprawie stwierdzenia naruszenia przez ClickQuickNow Sp. z o.o. z siedzibą w Warszawie przepisów art. 5 ust. 1 lit. a), art. 6 ust. 1, art. 7 ust. 3, art. 12 ust. 2, art. 17 ust. 1 lit. b) oraz art. 24 ust. 1 rozporządzenia 2016/679. Wysokość nałożonej na spółkę kary pieniężnej wyniosła 201559,50 PLN. Decyzja PUODO z 16 października 2019 r., ZSPR.421.7.2019. Również organy nadzorcze państw członkowskich UE podejmowały decyzje w sprawie naruszenia prawa do bycia zapomnianym. Na przykład:

- szwedzki organ nadzorczy decyzją z 10 marca 2020 r. nałożył na Google LLC karę pieniężną w wysokości 7 000 000 euro;
- łotewski organ nadzorczy decyzją z 26 sierpnia 2019 r. nałożył na łotewskiego operator sklepu internetowego karę pieniężną w wysokości 7000 euro;
- węgierski organ nadzorczy decyzją z 4 marca 2019 r. nałożył na instytucję kredytową karę pieniężną w wysokości 3200 euro;

zob. szerzej M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne,* Warszawa 2020, s. 139 i n.

[557] Art. 105 ust. 1 u.o.d.o. 2018.

[558] W przypadku odroczenia terminu uiszczenia administracyjnej kary pieniężnej albo rozłożenia jej na raty, PUODO nalicza nieuiszczone kwoty odsetki w stosunku rocznym, przy zastosowaniu obniżonej stawki odsetek za zwłokę, ogłaszanej na podstawie art. 56d ustawy z 29 sierpnia 1997 r. – Ordynacja podatkowa, od dnia następującego po dniu złożenia wniosku (art. 105 ust. 4 u.o.d.o. 2018). W przypadku rozłożenia administracyjnej kary pieniężnej na raty, odsetki, o których mowa, są naliczane odrębnie dla każdej raty (art. 105 ust. 5 u.o.d.o. 2018). W przypadku niedotrzymania odroczonego terminu uiszczenia administracyjnej kary pieniężnej albo terminu uiszczenia jej rat, odsetki są naliczane za okres od dnia upływu odroczonego terminu uiszczenia kary albo terminu uiszczenia poszczególnych rat (art. 105 ust. 6 u.o.d.o. 2018). PUODO może uchylić odroczenie terminu uiszczenia administracyjnej kary pieniężnej albo rozłożenie jej na raty, jeżeli ujawniły się nowe lub uprzednio nieznane okoliczności istotne dla rozstrzygnięcia lub jeżeli rata nie została uiszczona w terminie (art. 105 ust. 7 u.o.d.o. 2018). PUODO, na wniosek podmiotu ukaranego prowadzącego działalność gospodarczą, może udzielić ulgi w wykonaniu administracyjnej kary pieniężnej, określonej w ust. 2 art. 105, która:

interes wnioskodawcy[559]. Rozstrzygnięcie w tym przedmiocie następuje w drodze postanowienia.

1) nie stanowi pomocy publicznej;
2) stanowi pomoc *de minimis* albo pomoc *de minimis* w rolnictwie lub rybołówstwie – w zakresie i na zasadach określonych w bezpośrednio obowiązujących przepisach prawa UE dotyczących pomocy w ramach zasady *de minimis*;
3) stanowi pomoc publiczną zgodną z zasadami rynku wewnętrznego UE, której dopuszczalność została określona przez właściwe organu UE,

art. 105 ust. 9 u.o.d.o. 2018.

[559] Art. 105 ust. 2 i 3 u.o.d.o. 2018.

Zakończenie

W dobie powszechnego dostępu do Internetu i rozwoju nowych technologii, informacje ze sfery prywatnej jednostki, w tym także jej dane osobowe, stały się wartościowym towarem. Aby zapewnić sobie do nich dostęp, dostawcy usług wirtualnych, umożliwiają internautom bezpłatne korzystanie z nich, co okazuje się skuteczne.

Przenoszenie informacji ze świata rzeczywistego do wirtualnego dla wielu osób nie sprawia żadnych trudności. Problem w tym, że nie każdy, decydując się na taki krok, rozumie warunki regulaminu danej usługi lub co gorsze w ogóle ich nie czyta. W konsekwencji, brak zainteresowania internautów ochroną prywatności i danych osobowych prowadzi do unicestwienia tych wartości, co potwierdzają wypowiedzi szefów korporacji internetowych. Na przykład, przewodniczący zarządu Google, Eric Schmidt, stwierdził odnosząc się do prywatności, że „«jeżeli coś robicie i nie chcecie, aby ktoś się o tym dowiedział, to lepiej wcale tego nie róbcie» […]. Wypowiedź ta odzwierciedla pogląd, że każdy sam odpowiada za dane, które wygenerował poprzez swoje zachowanie. Wzajemne powiązania użytkowników sieci ujawniają jednak tyle informacji o ludziach, że pojedynczy człowiek traci nad tym kontrolę. W przemówieniu wygłoszonym w Berlinie w 2010 r. Schmidt sformułował to jeszcze wyraźnie: «koncepcja prywatności jest anachronizmem i musimy się nią pożegnać». Dodał, że dzięki sieci nigdy nie jesteśmy sami i że maszyny wszystko o nas wiedzą”[560].

[560] C. Kurz, F. Rieger, *op. cit.*, s. 87.

Brak świadomości wielu internautów na temat zagrożeń występujących w sieci, a przez to i lekkomyślne ich postępowanie, okazuje się ogromnym problemem, który przyczynia się do przekreślenia granic prywatności i danych osobowych. Wszystko to odbywa się jednak za przyzwoleniem jednostki, która przecież dobrowolnie korzysta z różnego rodzaju usług wirtualnych. W konsekwencji prowadzi to do tego, że ceniona od dawna sfera prywatności wraz z permanentnym postępem cyfrowym zaczęła być dla niektórych sferą przezroczystą i niemającą znaczenia. Nie można zatem nikogo zmusić, aby troszczył się o swoją prywatność, której „nie potrzebuje i nie rozumie, w czym utwierdza go”[561] chęć podążania za trendami internetowymi.

Nie ulega wątpliwości, że prawo do bycia zapomnianym od czasu wydania wyroku w sprawie *Google Spain* jest przedmiotem szczególnego zainteresowania. W poprzednim stanie prawnym 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 z kolei wiązało się z tym, że dotarcie do niechcianej informacji było możliwe po wpisaniu w wyszukiwarce innego – niż imię i nazwisko – sformułowania. Obecnie, prawo do bycia zapomnianym ma szerszy zakres zastosowania. Odnosi się nie tylko do operatorów wyszukiwarek internetowych, ale także do innych podmiotów, które posiadają status administratora w rozumieniu art. 4 pkt 7 RODO. O szerszym zasięgu działania tego prawa świadczy także zamknięty katalog przesłanek, od których uzależniona jest jego realizacja. W sytuacji więc, gdy osoba, której dane dotyczą, wystąpi z żądaniem ich usunięcia, administrator będzie musiał usunąć dane nie tylko z systemu, ale także i z innych miejsc, w których je przetwarzał, np. chmury, dysków zewnętrznych, dokumentacji papierowej, pod warunkiem ziszczenia się jednej przesłanki

[561] R. Piotrowski, *op. cit.,* s. 31.

z art. 17 ust. 1 RODO. Co więcej, w razie upublicznienia danych osoby, której one dotyczą, administrator zobowiązany jest do poinformowania administratorów przetwarzających te dane, że osoba ta żąda, aby usunęli oni wszelkie informacje na jej temat (art. 17 ust. 2 RODO).

Brak w przepisach RODO odniesienia zarówno co do treści, jak i formy wniosku o usunięcie danych osobowych oznaczać może w praktyce przyjęcie różnych w tym zakresie rozwiązań. Dopuszczalne zatem jest złożenie wniosku z oznaczeniem danych wnioskodawcy i wskazaniem, że zaszła jedna z okoliczności wymienionych w art. 17 ust. 1, choć w niektórych przypadkach niewykluczone wydaje się także złożenie wniosku bez uzasadnienia. Forma wniesienia żądania może przybrać dowolną postać, byle na jej podstawie można było potwierdzić tożsamość osoby, której dane dotyczą.

W procesie realizacji prawa do bycia zapomnianym bardzo ważny z punktu widzenia podmiotu danych jest termin. Z przyjętych w RODO rozwiązań wynika, że proces ten powinien nastąpić bez zbędnej zwłoki. Terminu tego nie należy jednak utożsamiać z terminem natychmiastowym, o czym przesądza treść art. 12 ust. 3 RODO.

Odnośnie do prawa do bycia zapomnianym należy mieć na uwadze, że nie ma ono charakteru absolutnego. W art. 17 ust. 3 prawodawca unijny wymienił bowiem enumeratywny katalog przesłanek wyłączających to prawo. Ponadto, należy wspomnieć, że prawo, o którym mowa, może zostać ograniczone w prawie unijnym lub krajowym, zgodnie z art. 23 RODO.

Prawo do bycia zapomnianym, o którym mowa w art. 17 ust. 1 RODO, służyć ma uniknięciu „przetrzymywania danych osobowych, które utraciły aktualność lub stały się zbędne dla administratora”[562]. W praktyce, wystąpienie przez osobę, której dane dotyczą, z żądaniem

[562] B. Fischer, *Prawo do usunięcia…*, s. 211.

ich usunięcia wymaga indywidualnego rozpatrzenia. Niewykluczone przecież jest, że żądanie, o którym mowa, będzie możliwe do zrealizowania jedynie częściowo. Może to nastąpić w sytuacji, gdy laureat konkursu internetowego wystąpi z wnioskiem o usunięcie danych przekazanych administratorowi na potrzeby konkursu, takich jak imię i nazwisko, adres zamieszkania, data urodzenia, email, telefon. W związku z ciążącym na administratorze obowiązkiem przechowywania danych do celów podatkowych, będzie on mógł jedynie usunąć email i telefon, bowiem dane te nie są wymagane do wskazanego celu.

Nie budzi wątpliwości, że uprawniony do realizacji prawa będzie w wielu przypadkach inicjował wystąpienia nie tylko ze skargą do organu nadzorczego, ale również środkiem ochrony prawnej z art. 79 RODO, którym jest powództwo cywilne, administracyjne kary pieniężne czy inne sankcje[563]. Każde z tych narzędzi ma istotne znaczenie dla ochrony danych, niemniej najwięcej obaw wśród administratorów i podmiotów przetwarzających wywołują kary pieniężne, które jak podkreśla Grupa Robocza Art. 29, są „ważnym narzędziem, które organy nadzorcze powinny stosować w odpowiednich okolicznościach. Zachęca się organy nadzorcze do stosowania rozważnego i wyważonego podejścia w zakresie stosowania środków naprawczych, tak aby

[563] Zgodnie z art. 84 ust. 1 RODO „Państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenie niniejszego rozporządzenia, w szczególności za naruszenie niepodlegające administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

Ust. 2. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych zgodnie z ust. 1, a następnie niezwłocznie o każdej późniejszej ich zmianie".

Mając powyższe na względzie należy podkreślić, że prawodawca krajowy w art. 107 i 108 u.o.d.o. 2018 przewidział sankcje karne. Pierwszy z tych przepisów odnosi się do czynu polegającego na przetwarzaniu danych osobowych, w tym szczególnych kategorii danych osobowych bez podstawy prawnej. Z kolei drugi tyczy się czynu udaremnienia lub utrudnienia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych.

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”[564]. Miejmy więc nadzieję, że osoby, których dane dotyczą, dzięki rozwiązaniom przyjętym w RODO będą mieć większe poczucie pewności prawa i jego stosowania w praktyce.

[564] Wytyczne Grupy Roboczej Ds. Ochrony Danych Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679, przyjęte w dniu 3 października 2017 r., s. 7.

Wykaz literatury

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne*, Warszawa 2020.

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Ochrona danych w wybranych państwach Azji*, Wrocław 2019.

Alama K., Kawecki M., *Zmiana pogody dla usług chmurowych,* „ABI Expert" 2017, nr 1(2) .

Anisimowicz J., *Akredytacja dla podmiotów certyfikujących oraz przebieg procesu certyfikacji,* „ABI Expert" 2017, nr 4.

Anisimowicz J., *Privacy by design z perspektywy architektury i budowy systemów informatycznych,* „ABI Expert" 2018, nr 2.

Banaszak B., *Konstytucyjna regulacja małżeństwa a prawo do zawarcia małżeństwa,* [w:] M. Jabłoński (red.), *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym,* Wrocław 2014.

Banaszewska A., *Prawo do prywatności we współczesnym świecie,* „Białostockie Studia Prawnicze", z. 13, Białystok 2013.

Banyś T.A.J., Łuczak J., *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Wrocław 2014.

Baran B., Południak-Gierz K., *Perspektywa regulacji prawa do bycia zapomnianym w Internecie. Zarys problematyki,* „Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego Nauki Społeczne" 2017, nr 17 (2).

Barta J., Markiewicz R., *Ochrona danych osobowych. Komentarz,* Kraków 2001.

Barta J., Markiewicz R., *Internet a prawo*, Kraków 1998.

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz,* Warszawa 2011.

Barta P., *Prawnie uzasadniony interes w działalności marketingowej,* „ABI Expert" 2018, nr 3.

Baszkiewicz J., Ryszka F., *Historia doktryn politycznych i prawnych,* Warszawa 1973.

Bierć A., Zawirska P., *Konstytucjonalizacja ochrony prywatności na tle standardów europejskich,* [w:] J. Kuciński (red.), *Piętnaście lat Konstytucji RP z 1997 roku. Inspiracje, uregulowania, trwałość,* Warszawa 2012.

Błażewski M., Behr J., *Środki ochrony danych osobowych,* Wrocław 2018.

Braciak J., *Prawo do prywatności,* [w:] B. Banaszak, A. Preisner (red.), *Prawa i wolności obywatelskie w Konstytucji RP,* Warszawa 2002.

Braciak J., *Prawo do prywatności,* [w:] S. Pajączkowski, A. Preisner (red.), *Zeszyty Luksemburskie 1. Praktyczne i teoretyczne problemy współczesnego państwa. Wybrane zagadnienia,* Lublin 2012.

Buczyńska-Borowy A., *Alfabet ODO,* „ABI Expert" 2017, nr 2.

Cieślik A., *Bezpieczeństwo systemów IT zgodne z RODO,* „ABI Expert" 2017, nr 1.

Cieślik A., *Zagrożenia dla prywatności – Phishing,* „ABI Expert" 2016, nr 1.

Czakowski M., *Zagrożenie prywatności w obliczu wojny w sieci,* [w:] *Sapientiae Servientes. Księga Jubileuszowa Profesor Krystyny Kwaśniewskiej,* Bydgoszcz 2015.

Czarny-Drożdżejko E., *Ochrona danych osobowych w internecie w świetle orzecznictwa Trybunału Sprawiedliwości,* „Przegląd Sejmowy", listopad-grudzień 2015.

Czerniawski M., *Komentarz do art. 17 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Czerniawski M., *Komentarz do art. 19,* [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Czerniawski M., *Portale społecznościowe a prawo do ochrony danych osobowych – zarys problemu,* [w:] G. Szpor, W.R. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012.

Darowska K., Lewandowska J., *Ochrona dóbr osobistych w Internecie ze szczególnym uwzględnieniem portali społecznościowych,* [w:] A. Kalisz (red.), *Prawa człowieka. Współczesne zjawiska, wyzwania, zagrożenia,* T. II, Sosnowiec 2015.

Demczuk A., *„Prawo do bycia zapomnianym" jako szczególne prawo jednostki do kontroli informacji o sobie w społeczeństwie informacyjnym w kontekście*

RODO, „Zarządzenie i Finanse. Journal of Management and Finance" 2018, Vol. 16, No. 4/2.

Drobek P., *Komentarz do art. 5 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Dyjak D., *Zasady podstawowe przetwarzania danych osobowych w świetle RODO,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne,* Wrocław 2017.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2018.

Fazlioglu M., *Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet,* "International Data Privacy Law" 2013, Vol. 3, No. 3.

Fischer B., *Cloud computing – nowy technologiczny paradygmat zagrożeniem dla ochrony danych osobowych i prywatności,* Kraków 2013.

Fischer B., *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych – wybrane zagadnienia,* „Monitor Prawniczy" 2014, nr 9 – dodatek.

Fischer B., *Prawo do usunięcia danych,* [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie RODO,* Wrocław 2017.

Garlicki L., *Komentarz do art. 8,* [w:] L. Garlicki (red.), *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18,* Warszawa 2010.

Gawroński M., Kunda K., *Prawo do usunięcia danych, prawo do bycia zapomnianym (art. 17 RODO),* [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami,* Warszawa 2018.

Gawrysiak P., *Portale internetowe – zagrożenia realne i pozorne,* [w:] G. Szpor, W.R. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012.

Gonschior A., *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej,* [w:] D. Kornobis-Romanowska (red.), *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego – aspekty teoretyczne i praktyczne*, Wrocław 2017.

Góral U., Makowski P., *Komentarz do art. 41 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Górski M., *„Właściciel" fanpage'a na portalu społecznościowym jako administrator,* „ABI Expert" 2018, nr 3.

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 12.

Hildebrandt M., *Defining profiling: new type of knowledge?,* [w:] M. Hildebrandt, S. Gutwirth (eds.), *Profiling the European Citizens, Cross-Disciplinary Perspectives,* Springer 2008.

Jabłoński M., *Prywatność jako przesłanka ograniczenia dostępu do informacji publicznej,* „Przegląd Prawa i Administracji" LXXVI, Wrocław 2007.

Jabłoński M., *Rola i znaczenie RODO w procesie definiowania gwarancji niezależności i spójności krajowego systemu ochrony danych osobowych,* [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda (red.), *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym,* Wrocław 2017.

Jabłoński M., Węgrzyn J., *Ochrona tajemnic osób wykonujących prawnicze zawody zaufania publicznego,* Wrocław 2016.

Jabłoński M., Węgrzyn J., *Zmiana modelu ochrony danych osobowych – podejście oparte na ryzyku, privacy by design i privacy by default,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne,* Wrocław 2017.

Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice,* Wrocław 2002.

Jabłoński M., Wygoda K., *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej. Aspekty praktyczne,* Warszawa 2021.

Jabłoński M., Wygoda K., *Praktyczne znaczenie podstawowych pojęć RODO – wybrane zagadnienia,* Wrocław 2019.

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., Sakowska-Baryła M., Wygoda K., *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018.

Jagielski M., *Konstytucjonalizacja ochrony prywatności,* [w:] R.M. Małajny (red.), *Konstytucjonalizm a doktryny polityczno-prawne. Najnowsze kierunki badań,* Katowice 2008.

Jaskiernia A., *Ochrona prywatności w epoce cyfrowej w perspektywie regulacyjnej Unii Europejskiej,* [w:] J. Jaskiernia (red. nauk.), *Europejski system ochrony praw człowieka. Aksjologia – instytucje – efektywność,* Toruń 2015.

Kania R., *Ryzyko, czas i cudze prawa – proces ochrony danych,* „ABI Expert" 2018, nr 2.

Karczewska O., *RODO w Internecie – prawo do bycia zapomnianym,* [w:] A. Surma, E. Chodźko (red.), *Współczesne wyzwania cyfryzacji – przegląd i badania,* Lublin 2019.

Klimas D., Wróbel P., *Cywilnoprawna odpowiedzialność za naruszenie ochrony danych osobowych na gruncie RODO – wstęp do zagadnienia,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne,* Wrocław 2017.

Kobylańska A., Ślęzak Ł., *Ochrona danych w fazie projektowania – privacy by design,* „ABI Expert" 2016, nr 1.

Kocot W.J., *Charakter prawa „do bycia zapomnianym" – restytucja reputacji w internecie*, [w:] I. Matusiak, K. Szczepanowska-Kozłowska, Ł. Żelechowski (red.), *Opus auctorem laudat. Księga jubileuszowa dedykowana Profesor Monice Czajkowskiej-Dąbrowskiej*, Warszawa 2019.

Kołodziej M., *Pseudonimizacja w RODO – kiedy i jak stosować?,* „ABI Expert" 2018, nr 2.

Konarski X., *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce,* „Monitor Prawniczy" 2016, nr 2.

Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne),* „Studia Cywilistyczne", t. XX, Kraków 1972.

Kowalik P., Wociór D., *Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego,* [w:] *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem ogólnego rozporządzenia unijnego,* Warszawa 2016.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016.

Krzysztofek M., *Prawo do bycia zapomnianym i inne aspekty prywatności w epoce Internetu w prawie UE,* „Europejski Przegląd Sądowy" 2012.

Kuberska W., *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu,* [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą na podstawie RODO,* Wrocław 2017.

Kuberska W., *Środek ochrony prawnej przed sądem,* „ABI Expert" 2017, nr 4.

Kurek J., *Prawo do uzyskania powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,* [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, Wrocław 2017.

Kurz C., Rieger F., *Pożeracze danych. O zawłaszczaniu danych i o tym, jak odzyskać nad nimi kontrolę,* Warszawa 2013.

Leja P., *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, „Prawo Mediów Elektronicznych", 2017, nr 3.

Lew-Starowicz Z., *Psychospołeczne podstawy seksualności,* [w:] Z. Lew-Starowicz, V. Skrzypulec (red.), *Podstawy seksuologii*, Warszawa 2010.

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,* P. Litwiński (red.), Warszawa 2018.

Lubasz D., *Komentarz do art. 4 pkt 11 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Lubasz D., *Komentarz do art. 4 pkt 25 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Lubasz D., *Komentarz do art. 6 ust. 1 lit. a) RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Lubasz D., *Komentarz do art. 8 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Lubasz D., *Komentarz do art. 30 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Lubasz D., *Komentarz do art. 32 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Łakomiec K., *Konstytucyjne gwarancje ochrony prywatności informacyjnej wobec rozwoju nowych technologii*, „Przegląd Legislacyjny", 2015, nr 1 (91).

Łuczak J., *Komentarz do art. 12 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Łuczak J., *Komentarz do art. 77 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Łuczak J., *Komentarz do art. 77 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

McCarthy H., *All the World's a Stage: The European right to be forgotten revisited from a US perspective*, „Journal of Intellectual Property Law and Practice" 2016, Vol. 11, No. 5.

McGoldrick D., *Developments in the Right to be Forgotten,* „Human Rights Law Review" 2013, Vol. 12, No. 3.

Mednis A., *Prawo do prywatności a interes publiczny,* Zakamycze 2006.

Mednis A., *Prawo do wniesienia skargi do organu nadzorczego,* [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie RODO,* Wrocław 2017.

Mednis A., *Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?,* [w:] A. Mednis (red.), *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość,* Warszawa 2016.

Mednis A., *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych,* „Monitor Prawniczy" 2016, nr 20.

Michałkiewicz E., Milczarek E., *Prawo do prywatności w dobie Internetu,* „Prawo Mediów Elektronicznych" 2015, nr 2.

Młotkiewicz M., *Rejestry czynności – przydatny instrument rozliczalności,* „ABI Expert" 2017, nr 3.

Molenda-Kropielnicka E., *Cloud computing – zagadnienia prawne,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2013, nr 1.

Olszewski H., *Historia doktryn politycznych i prawnych,* Warszawa 1986.

Padova Y., *Is the right to be forgotten a universal, regional, or 'glocal' right?,* „International Data Privacy Law" 2019, Vol. 9, No. 1.

Piech M., *One stop shop. Mechanizmy podejmowania decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE,* „Monitor Prawniczy" 2016, nr 20.

Piotrowski R., *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne,* [w:] A. Mednis (red.), *Prywatność a jawność – Bilans 25-lecia i perspektywy na przyszłość,* Warszawa 2016.

Rivero A.F., *Right to be forgotten in the European Court of Justice Google Spain Case: The right balance of privacy rights, procedurę, and extraterritoriality,* „European Union Law Working Papers" 2017, No. 19, Stanford-Vienna Transatlantic Technology Law Forum.

Rogacka-Łukasik A., *Prawo do prywatności w dobie współczesnej ekspansji Internetu,* [w:] A. Kalisz (red.), *Prawa człowieka. Współczesne zjawiska, wyzwania, zagrożenia,* t. II, Sosnowiec 2015.

Rojszczak M., *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE,* „Prawo Mediów Elektronicznych" 2017, nr 3.

Rutkowska P., *Prawo do bycia zapomnianym w cyfrowym świecie. Wybrane zagadnienia*, „Społeczeństwo i Polityka" 2019, nr 1.

Rzucidło J., Węgrzyn J., *Prawne aspekty ochrony anonimowości konsumenta w Internecie,* „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie" 2013.

Sakowska-Baryła M., *Prawo do ochrony danych osobowych,* Wrocław 2015.

Sakowska-Baryła M., *Konstytucjonalizacja prawa do ochrony danych osobowych w Polsce*, „Przegląd Prawa Konstytucyjnego" 2016, nr 4 (32).

Sakowska-Baryła M., *Komentarz do art. 19,* [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018.

Sarnecki P., *Komentarz do art. 51,* [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. III, Warszawa 2003.

Sartor G., *The right to be forgotten in the Draft Data Protection Regulation,* „International Data Privacy Law" 2015, Vol. 5, No. 1.

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia,* „Monitor Prawniczy" 2016, nr 20.

Sibiga G., *Kryterium „zadania publicznego" w ustawie z 10.5.2018 r. o ochronie danych osobowych oraz jego konsekwencje dla wykonywania obowiązków administratora oraz realizacji praw osoby, której dane dotyczą (dodatek MoP 22/2018),* „Monitor Prawniczy" 2018, nr 22.

Siemieniak P., *Wymagania dokumentacyjne przetwarzania danych,* „ABI Expert" 2017, nr 2.

Sieńczyło-Chlabicz J., *Geneza i rozwój prawa do prywatności,* [w:] *O prawie i jego dziejach. Księgi dwie. Studia ofiarowane Profesorowi Adamowi Lityńskiemu w czterdziestopięciolecie pracy naukowej i siedemdziesięciolecie urodzin, Księga II,* Białystok-Katowice 2010.

Sieńczyło-Chlabicz J., *Ochrona prawa do prywatności w Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, Karcie Praw Podstawowych oraz w prawie krajowym,* [w:] M. Pecyna, J. Pisuliński, M. Podrecki (red.), *Rozprawy cywilistyczne. Księga pamiątkowa dedykowana Profesorowi Edwardowi Drozdowi,* Warszawa 2013.

Siewicz K., *Prywatność w serwisach społecznościowych. Nowe wyzwania dla ruchu wolnego oprogramowania,* [w:] G. Szpor, W. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012.

Siwicki M., *Cyberprzestępczość,* Warszawa 2013.

Sławiński A.A., *„Prawo do bycia zapomnianym" w świetle ogólnego rozporządzenia o ochronie danych osobowych i orzecznictwa TSUE,* [w:] M. Wiązek (red.), *Prawo do prywatności – współczesne wyzwania,* Warszawa 2019.

Sobczak J., *Komentarz do art. 7 Karty Praw Podstawowych Unii Europejskiej,* [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz,* Warszawa 2013.

Sokolewicz W., *Prawo do prywatności,* [w:] *Prawa człowieka w Stanach Zjednoczonych,* Warszawa 1985.

Stefaniak S., Suszek-Borowska H., *Rozliczalność przetwarzania danych a systemy informatyczne,* „ABI Expert" 2018, nr 2.

Such J.M., Garcia-Fornes A., Botti V., *Automated buyer profiling control based on human privacy attitudes,* „ElectronicCommerce Research and Applications", 2013, vol. 12, no. 6, November.

Sut P., Wojciechowski M., *Co zamiast prywatności? Czy prawo do intymności jest prawem człowieka?,* [w:] J. Jaskiernia (red. nauk.), *Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania tom 1,* Warszawa 2014.

Szot L., *Prawo d obycia zapomnianym w sieci,* [w:] W. Kitler, J. Taczkowska-Olszewska (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne,* Warszawa 2017.

Sztąberek M., Ułasiuk K., *Bezpieczeństwo danych osobowych. Praktyczny przewodnik,* Wrocław 2017.

Tinnefeld M.T., *Jak Internet zmienia prawne ramy prywatności?,* [w:] G. Szpor, W. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012.

Vries K., *Identity, profiling algorithms and a world of ambient intelligence, "*Ethics and Information Technology", vol. 12, no. 1.

Warren S., Brandeis L., *The Right to Privacy,* Harward Law Review, Vol. IV, December 15, 1980, No. 5.

Wąglowski P., *Internet a dobra osobiste człowieka*, [w:] T. Zasępa, R. Chmura (red.), *Internet – fenomen społeczeństwa informacyjnego*, Częstochowa 2001.

Wątor W., *Prawo do bycia zapomnianym a swoboda wypowiedzi. Glosa do wyroku ETPC z dnia 28 czerwca 2018 r., 60798/10 i 65599/10,* „Europejski Przegląd Sądowy" 2019, nr 5.

Wiewiórowski W.R., *Privacy by Design jako paradygmat ochrony prywatności,* [w:] G. Szpor, W.R. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług,* Warszawa 2012.

Więckowska M., *Analiza ryzyka prywatności,* „ABI Expert" 2017, nr 2.

Więckowska M., *Przewodnik po ocenie skutków dla ochrony danych,* „ABI Expert" 2017, nr 2.

Witkowska-Nowakowska K., *Kodeksy postępowania i certyfikacja,* [w:] D. Lubasz (red.), *RODO w e-commerce,* Warszawa 2018.

Woch P., *Sfera życia prywatnego i jego ochrona przed naruszeniami w Cyberprzestrzeni,* [w:] R. Skubisz (red.), *Internet 2000. Prawo-Ekonomia-Kultura*, Lublin 2000.

Wociór D., *Informacje wstępne,* [w:] D. Wociór (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego,* Warszawa 2016.

Wróbel M., *Prawo do „bycia zapomnianym" – glosa – C-131/12*, „Monitor Prawniczy" 2017, nr 2.

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

Wyrzykowski M., *Ochrona danych – zagadnienia konstytucyjne,* [w:] Wyrzykowski (red.), *Ochrona danych osobowych,* Warszawa 1999.

Wysocki B., *Prawo do bycia zapomnianym – prawem cyfrowej rzeczywistości,* „Ars Educandi" 2016, nr 13.

Zawadzka N., *Środki ochrony prawnej, odpowiedzialność i sankcje,* [w:] D. Lubasz (red.), *RODO w e-commerce,* Warszawa 2018.

Żak J., *Koncepcja „prawa do bycia zapomnianym",* [w:] M. Jabłoński, S. Jaroszyżukowska (red.), *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi,* Wrocław 2014.

Wykaz stron internetowych

http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1586575

http://curia.europa.eu/juris/document/document.jsf?text=%2522dyrektywa-%2B95%252F46%2522&docid=184668&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=994471#ctx1

http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=263718

http://curia.europa.eu/juris/document/document.jsf?text=%2522dyrektywa-%2B95%252F46%2522&docid=169195&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=303606#

https://pl-pl.facebook.com/about/privacy/

http://bitdefender.pl/phishing-co-to-jest-i-czy-potrafisz-go-rozpoznac

https://www.avast.com/pl-pl/c-pharming

https://pl-pl.facebook.com/legal/terms/update

http://www.voxeurop.eu/pl/content/article/1090601-europa-kontra-facebook

http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf

https://poradnikprzedsiebiorcy.pl/-spam-definicja-rodzaje-historia-powstania-oraz-sposoby-ochrony/3

https://poradnikprzedsiebiorcy.pl/-spam-definicja-rodzaje-historia-powstania-oraz-sposoby-ochrony/2

http://prawo.vagla.pl/node/7900

https://forsal.pl/artykuly/1431643,niewidocznosc-w-internecie-wyrok-tsue-ws-google.html

https://giodo.gov.pl/pl/1520110/4214

http://communication.oxfordre.com/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189

https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636594911489394651-2718733419&hl=pl&rd=1

https://giodo.gov.pl/pl/1520203/8648

https://sylwiaczub.pl/wniosek-o-usuniecie-danych-osobowych-wedlug-rodo/

https://s4edu.pl/pl/centrum-wiedzy/92-gdpr/116-najwieksze-wyzwanie-rodo-on-riks-basedapproach

https://uodo.gov.pl/data/filemanager_pl/706.pdf

http://lexmanual.pl/2018/02/rodo-pseudonimizacja/

https://www.zdrowie.abc.com.pl/aktualnosci/rodo-nie-wskazuje-srodkow-i-metod-zabezpieczania-danych-jedynie-daje-wskazowki,117451.html

https://www.akademiakomputronik.pl/artykul/co-to-jest-firewall-i-czy-jest-mi-potrzebny

https://www.securelist.pl/glossary/6234,atak_dos.html

https://uodo.gov.pl/data/filemanager_pl/1186.pdf

https://uodo.gov.pl/pl/123/214

https://www.giodo.gov.pl/pl/1520344/10392

https://uodo.gov.pl/data/filemanager_pl/708.pdf

https://uodo.gov.pl/pl/83/154

https://uodo.gov.pl/pl/83/153

Publikacje z dyscypliny nauki prawne – prawo konstytucyjne, które ukazały się w e-Wydawnictwie WPAE UWr

Justyna Węgrzyn, *Prawo konsumenta do informacji w Konstytucji RP i w prawie unijnym*, Wrocław 2013
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/40651

Współczesne koncepcje ochrony wolności i praw podstawowych, red. Andrzej Bator, Mariusz Jabłoński, Marek Maciejewski, Krzysztof Wójtowicz, Wrocław 2013
Dostęp online: http://bibliotekacyfrowa.pl/publication/42456

Małgorzata Masternak-Kubiak, *Odesłania do prawa międzynarodowego w Konstytucji RP,* Wrocław 2013
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/41352

Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym, red. Mariusz Jabłoński, Wrocław 2014
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/51986

Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi, red. Mariusz Jabłoński i Sylwia Jarosz-Żukowska, Wrocław 2014
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/56032

Krzysztof Wójtowicz, *Constitutional Courts and European Union Law,* Wrocław 2014
Online access: http://www.bibliotekacyfrowa.pl/publication/54527

Zasada pierwszeństwa prawa Unii Europejskiej w praktyce działania organów władzy publicznej RP, red. Mariusz Jabłoński, Sylwia Jarosz-Żukowska, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/64552

Artur Ławniczak, *Geneza Konstytucji,* Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/65468

Teoretyczne i praktyczne aspekty realizacji prawa petycji, red. Ryszard Balicki i Mariusz Jabłoński, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/66901

Ewolucja państwowości w Brazylii, Polsce i Eurazji. Evolução do estado no Brasil, Polônia e Eurásia, red. Marcos A. Maliska, Krystian Complak, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/64761

Międzynarodowa ochrona praw człowieka – współczesne problemy na świecie, red. Mariusz Jabłoński, Tomasz Jurczyk, Patryk Gutierrez, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/67621

Identyfikacja granic wolności i praw jednostki. Prawnoporównawcza analiza tożsamego przypadku pod kątem praktyki stosowania prawa amerykańskiego i polskiego, red. Mariusz Jabłoński, Wrocław 2016
Dostęp online: http://www.bibliotekacyfrowa.pl/dlibra/publication/79781

Instytucje demokracji bezpośredniej w praktyce, red. Olga Hałub, Mariusz Jabłoński, Mateusz Radajewski, Wrocław 2016
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/80567

Aktualne problemy ochrony wolności i praw mniejszości w Polsce i na świecie, red. Joanna Beata Banach-Gutierrez, Mariusz Jabłoński, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/84127

Współczesne polityczno-prawne systemy państw Europy, Azji i Ameryki Łacińskiej, red. Krystian Complak, Patryk Gutierrez, Jolanta Rosiak, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/dlibra/publication/84639

Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne, red. Mariusz Jabłoński, Kinga Flaga-Gieruszyńska, Krzysztof Wygoda, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/92803

Magdalena Bainczyk, *Polski i niemiecki Trybunał Konstytucyjny wobec członkostwa państwa w Unii Europejskiej*, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/84085

Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi, red. Ryszard Balicki, Mariusz Jabłoński, Wrocław 2018
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/95368

Ryszard Balicki, *Funkcja europejska Sejmu RP,* Wrocław 2019
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/101626

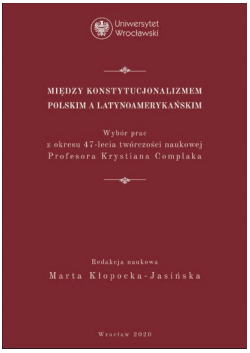
Specyfika organizacji i funkcjonowania organów władzy publicznej. Analiza porządków prawnych państw współczesnych, red. Mariusz Jabłoński, Magdalena Abu Gholeh, Wrocław 2019
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/101490

Anna Śledzińska-Simon**,** *Analiza proporcjonalności ograniczeń konstytucyjnych praw i wolności. Teoria i praktyka*, Wrocław 2019
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/102713

Olga Hałub-Kowalczyk, Mariusz Jabłoński, Mateusz Radajewski, *Identyfikacja treści prawa do sądu – wybrane zagadnienia*, Wrocław 2019
Dostęp online: https://www.bibliotekacyfrowa.pl/publication/104603

Osobowość prawna jako przesłanka wykonywania konstytucyjnych wolności i praw, red. Michał Bernaczyk, Mariusz Jabłoński, Wrocław 2019
Dostęp online: https://www.bibliotekacyfrowa.pl/publication/108539

Magdalena Abu Gholeh, Dominka Kuźnicka-Błaszkowska, *Ochrona danych osobowych w wybranych państwach Azji*, Wrocław 2019
Dostęp online: https://www.bibliotekacyfrowa.pl/publication/112255



Między konstytucjonalizmem polskim a latynoamerykańskim. Wybór prac z okresu 47-lecia twórczości naukowej Profesora Krystiana Complaka, red. Marta Kłopocka-Jasińska, Wrocław 2020
Dostęp online: https://www.bibliotekacyfrowa.pl/publication/115875

Co istotne, jest to pierwsza tego typu i w tej tematyce monografia naukowa na rynku. Dlatego też z wielkim uznaniem należy się odnieść do wyboru tematyki przez Autorów.

Z recenzji wydawniczej dr hab. Sabiny Grabowskiej, prof. UR

[...] Autorzy poddali analizie podstawowe elementy treści rozwiązań, które pozwoliły na zrozumienie charakteru i znaczenia prawa do bycia zapomnianym. Dlatego też przedstawiono „otoczenie" sfery chronionej, czyli prywatności jednostki i danych osobowych, oraz przyjęty w polskim porządku prawnym model definiujący przesłanki: realizacji przedmiotowego prawa; jego ograniczeń i wyłączeń oraz odpowiedzialności za jego naruszenie. Po przeprowadzeniu tejże analizy Autorzy formułowali ostateczne oceny w kontekście skuteczności i efektywności realizacji prawa do bycia zapomnianym, również w praktyce orzeczniczej polskich organów wymiaru sprawiedliwości.

Z recenzji wydawniczej dr. hab. Radosława Grabowskiego, prof. UR

ISBN 978-83-66601-69-7 (druk)
ISBN 978-83-66601-70-3 (online)