Agata Gonschior
Uniwersytet Wrocławski

Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej

Wstęp

Tematyką niniejszego artykułu jest problem ochrony danych osobowych w świetle prawa do prywatności. Wybór takiego tematu podyktowany został aktualnością problemów ochrony w sferze zarówno danych osobowych, jak i prawa do prywatności. Aktualność ta wyraża się w reformie ochrony danych osobowych w prawodawstwie Unii Europejskiej, której to końcowe etapy można obserwować na przestrzeni ostatnich tygodni. Problematyka ta wymagała podjęcia przede wszystkim ze względu na postęp technologiczny, który w niezwykle szybkim tempie wpływa na wszystkie elementy rzeczywistości społecznej, prawnej, gospodarczej i tym samym stanowi podstawową oś trudności związanych z dostosowywaniem ochrony do obecnych wymogów.

Celem rozprawy jest wykazanie korelacji pomiędzy ochroną danych osobowych i prawem do prywatności, ich wzajemnego przenikania się i przez to konieczności kompleksowej ochrony obu wartości poprzez branie pod uwagę jednego z tych dóbr w celu ochrony drugiego. W niniejszym artykule ukazane zostały powiązania i różnice związane z ochroną obu wspomnianych praw. Podstawowym jednak zamierzeniem rozprawy jest ukazanie, jak zachowane zostaje prawo do prywatności w tak specyficznej dziedzinie, jaką jest ochrona danych osobowych, przy okazji przetwarzania danych, a także ukazanie odstępstw od ochrony prywatności w sferze danych osobowych. Zadaniem artykułu jest pokazanie, w jaki sposób i czy w ogóle prawo do prywatności zachowywane jest w sferze danych osobowych przy okazji chociażby przetwarzania danych czy też ich udostępniania, które to przecież niewątpliwie w ową prywatność ingerują. Problem polegający na tym, czy i jak prywatność jest chroniona w takich sytuacjach, za pomocą jakich instrumentów, jakie płyną dla niej zagrożenia i – jeśli ochrona prywatności w sferze danych osobowych w ogóle ma miejsce – czy jej poziom jest dostateczny i odpowiedni jest podstawowym problemem dla niniejszej pracy.

Zakres artykułu obejmuje zarówno problemy związane z ochroną danych osobowych, jak i z ochroną prywatności. Rozprawa bazuje na dorobku naukowym badaczy związanych z dziedzinami ochrony prywatności i ochrony danych osobowych, a także w dużej mierze opiera się na aktach prawa unijnego podstawowych dla ochrony danych osobowych oraz na jeszcze nieobowiązującym rozporządzeniu ogólnym o ochronie danych osobowych będącym efektem wieloletnich prac nad reformą ochrony danych oso-

bowych w UE. W artykule w wielu miejscach występuje porównanie rozwiązań prawnych wynikających z obowiązującej jeszcze dyrektywy i nowego rozporządzenia, mające na celu ukazanie zmian spowodowanych koniecznością dostosowania prawodawstwa do obecnych potrzeb. Podstawą dla artykułu okazało się orzecznictwo TSUE, które to w wielu przypadkach stanowi wskazówkę, jak prawo unijne powinno być stosowane w praktyce i jak powinny być rozumiane jego pojęcia. Orzecznictwo to stanowi w niniejszej pracy ilustrację dla aktualnych problemów związanych z ochroną danych osobowych i prywatności w praktyce, podkreśla trudności w sferze ochrony wartości będących przedmiotem pracy wywołane postępem technologicznym.

Na strukturę artykułu składają się trzy rozdziały. W pierwszym przedstawione zostały podstawowe problemy wprowadzające do tematyki artykułu. Zawiera on podstawowe definicje pojęć kluczowych, takich jak: prywatność, dane osobowe, zakresy tych pojęć, podstawy prawne dla ochrony prywatności i danych osobowych, a także zakres ochrony, przedstawienie poziomu tej ochrony i jej prawnych standardów. Drugi rozdział dotyczy mechanizmów pozwalających na zachowanie prawa do prywatności w sferze ochrony danych osobowych przy okazji operacji na danych osobowych, które mogą stanowić ingerencję w prywatność osoby, od której pochodzą, jak np. przetwarzanie czy udostępnianie danych. Przedstawione zostały też rozwiązania prawne, które mają zapewnić w praktyce zachowanie prawa do prywatności przy przetwarzaniu danych osobowych, a także podstawowy problem dopuszczalności w ogóle przetwarzania danych w świetle prawa do prywatności jako potencjalnie wkraczającego w sferę prywatności. W trzecim rozdziale z kolei przedstawione zostały zagrożenia dla zachowywania prywatności w sferze ochrony danych osobowych, potencjalne mechanizmy, które pozwalają na odstępstwa od zachowywania prywatności przy okazji dokonywania operacji na danych osobowych. Uwydatniony został problem transgranicznego przepływu danych czy też skala zjawiska związana z rozwojem technologii, a w szczególności sieci Internet i przetwarzaniem danych w sieci na niezwykle szeroką skalę. Zasygnalizowany został problem przepływu danych do państw spoza UE, państw trzecich, które nie zawsze zapewniają odpowiedni poziom ochrony danych osobowych, co może stanowić zagrożenie dla prywatności podmiotów danych.

Niniejszy artykuł podejmuje zatem niezwykle ciekawy i aktualny problem ochrony danych osobowych w świetle prawa do prywatności w UE.

1. Ochrona danych osobowych i prawo do prywatności – pojęcia, podstawa prawna, zakres

1.1. Podstawa prawna, pojęcie i zakres prawa do prywatności

1.1.1. Podstawa prawna

Prawo do prywatności zaliczane jest w prawie wewnętrznym, unijnym i międzynarodowym do podstawowych praw człowieka. Uzasadnione jest stwierdzenie, że prawo to chronione jest niemal we wszystkich systemach prawnych. Gwarantowane jest

przez polską Konstytucję z 1997 r., która w art. 47 stanowi, że „Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym" oraz w art. 51[1], którego paragraf 1 stanowi, że „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby".

W prawie Unii Europejskiej prywatność początkowo nie znajdowała ochrony w traktatach ustanawiających Wspólnoty, z biegiem czasu wykształcił się jednak autonomiczny system ochrony praw podstawowych, w tym także prawa do prywatności. Szczególną rolę w tej kwestii odgrywał i odgrywa nadal Trybunał Sprawiedliwości Unii Europejskiej (TSUE), który przez dekady w swoim orzecznictwie podkreślał, że prawa człowieka stanowią część zasad ogólnych dawnego prawa wspólnotowego, a więc zasad branych pod uwagę przy stosowaniu i interpretacji prawa unijnego (wywodzonych przez TSUE z traktatów),wynikających z tradycji kulturowych i konstytucyjnych państw członkowskich UE oraz w EKPC[2]. Ochrona praw podstawowych okazała się na tyle konieczna, że pojawiła się w orzecznictwie właśnie w kontekście zasad ogólnych prawa przy okazji sprawy *Stauder* z 1969 r.[3] Koncepcja ta rozwijana była w kolejnych orzeczeniach aż do kluczowego momentu dla rozwoju ochrony praw podstawowych, a zatem i prawa do prywatności – uznania praw zawartych w Karcie praw podstawowych na mocy art. 6 Traktatu o Unii Europejskiej (TUE) w wersji traktatu z Lizbony[4], kiedy to prawa podstawowe zostały usystematyzowane i uwypuklone, a Karta Praw Podstawowych (KPP) zyskała taką samą moc prawną jak traktaty. Art. 6 TUE zapewnia poszanowanie praw człowieka i podstawowych wolności jako tradycji konstytucyjnych wspólnych dla państw członkowskich, a także poszanowanie praw podstawowych zawartych w europejskiej konwencji praw człowieka i podstawowych wolności (EKPC) jako części zasad ogólnych prawa[5]. Zatem, w odniesieniu do prawa do prywatności, Unia Europejska zobowiązana jest szanować prawa wynikające z art. 8 EKPC, tj. prawa do poszanowania życia prywatnego i rodzinnego obejmujące cztery sfery: ochrona życia prywatnego, rodzinnego, korespondencji, mieszkania[6]. Prawo do prywatności chronione jest art. 7 KPP (prywatność w znaczeniu szerszym), który na mocy traktatu lizbońskiego otrzymał brzmienie: „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się"[7]. Co ciekawe, prawo to jest podobne zakresowo do tego określonego w EKPC[8]. Prawo do prywatności gwarantuje także art. 8 (prywatność informacyjna) KPP[9].

[1] Konstytucja Rzeczypospolitej Polskiej, Dz. U. z 1997 r. Nr 78, poz. 483, art. 47 i 51.

[2] J. Braciak, *Prawo do prywatności*, Wydawnictwo Sejmowe, Warszawa 2004, s. 103.

[3] Wyrok TSUE 29/69, *Stauder przeciwko Ulm*, EU:C:1969:57.

[4] Traktat o Unii Europejskiej, wersja skonsolidowana, Dz. Urz. UE C 326/01 z 26.10. 2012 r., art. 6.

[5] *Ibidem.*

[6] Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r., Dz. U. z 1993 r. Nr 61, poz. 284, art. 8, dalej EKPC.

[7] Karta praw podstawowych Unii Europejskiej, Dz. Urz. UE C 326/391 z 26.10.2012 r., art. 7, dalej KPP.

[8] Art. 8 EKPC.

[9] J. Braciak, *op. cit.*, s. 103.

1.1.2. Pojęcie

Stworzenie precyzyjnej, konkretnej definicji prawa do prywatności jest niemalże niemożliwe – ciągle zmieniająca się sytuacja społeczna, gospodarcza, rozwój techniki – w szczególności przestrzeni informatycznej – powodują, że zakres tego, co „prywatne" także nieustannie się zmienia[10]. Ze względu na przekształcające się realia i szybko postępującą informatyzację życia określenie, choć jedynie ramowe, sfery prywatności jest niezwykle istotne dla jej ochrony. Wagę ochrony prywatności podkreśla Marek Safjan, wskazując, że: „prywatność ma podlegać ochronie właśnie dlatego i tylko dlatego, że przyznaje się każdej osobie prawo do wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a w której wolność od ciekawości innych jest swoistą *conditio sine qua non* swobodnego rozwoju jednostki"[11]. Definicja prawa do prywatności wymaga zatem w pierwszej kolejności zdefiniowana samej prywatności w ogólności.

Przyjmuje się, że pojęcie prawa do prywatności wprowadzili w 1890 r w Ameryce Samuel Warren i Louis Brandeis w swoim artykule pt. *The Right to Privacy*[12]. Choć podwalin wyróżniania prywatności niektórzy autorzy doszukują się już w Biblii, a później w myśli Benjamina Constanta czy Johna Stuarta Milla[13], to dla doktryny prawa szczególne znaczenie miał wspomniany artykuł. Współcześnie pojęcie to definiuje się jako pewną sferę wolną od cudzej ingerencji, przy czym zaznaczyć należy, że definicje nawiązują do rozwijającego się orzecznictwa w tym zakresie poprzez wskazywanie składających się na tę wolną od ingerencji sferę elementów[14]. Prywatność można też definiować jako opozycję do publicznej sfery aktywności. A. Kopff definiuje ją jako „to wszystko, co ze względu na uzasadnione odosobnienie się jednostki od ogółu służy jej do rozwoju fizycznej lub psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej"[15]. M. Jabłoński rozumie prywatność jako autonomię jednostki funkcjonującej w określonej rzeczywistości i sumę wartości na tę autonomię się składających[16]. K. Motyka z kolei wskazuje na poszczególne elementy składowe prawa do prywatności, takie jak: tajemnica korespondencji, ochrona danych osobowych, nietykalność mieszkania, w efekcie eliminując samo pojęcie prywatności[17], co może budzić pewne kontrowersje. M. Chrabonszczewski pisze o prywatności jako o „regulowaniu przez jednostkę dostępności swojej osoby dla innych"[18], dostępności w sensie fizycznym – nietykalności, a także w sensie psychicznym – myśli, przeżyć. Można mó-

[10] *Ibidem*, s. 21.

[11] M. Safjan, *Prawo do ochrony życia prywatnego*, [w:] *Szkoła Praw Człowieka*, Helsińska Fundacja Praw Człowieka, Warszawa 2006, s. 211 i n.

[12] L. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, vol. 4, s. 193 i n.

[13] J. Braciak, *op. cit*., s. 12 i n.

[14] *Ibidem*, s. 36.

[15] A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne*), „Studia Cywilistyczne", t. XX, Warszawa 1972, s. 30 i n.

[16] M. Jabłoński, *Prywatność jako przesłanka ograniczenia dostępu do informacji publicznej*, „Przegląd Prawa i Administracji" 2007, nr 86, s. 280.

[17] M. Jagielski, *Konstytucjonalizacja ochrony prywatności*, [w:] R. Małajny (red.), *Konstytucjonalizm a doktryny polityczno-prawne. Najnowsze kierunku badań*, Katowice 2008, s. 267.

[18] M. Chrabonszczewski, *Prywatność. Teoria i praktyka*, Warszawa 2012, s. 93.

wić o prywatności w układzie poziomym jako o zbiorze pewnych dóbr chronionych, z których każde może być chronione indywidualnie (jak np. tajemnica korespondencji, nietykalność cielesna) oraz w układzie pionowym, gdy chronimy sferę intymności i sferę prywatności, a poza zakresem ochrony pozostaje sfera publicznie, ogólnie dostępna[19]. J. Braciak rozróżnia dwie odmiany prywatności: „jedną związaną z wolnością i bezpieczeństwem, tworzącą zamkniętą sferę działań czy zachowań jednostki, niepoddającą się kontroli zewnętrznej, i drugą – wiążącą się z pojęciem godności osobistej, polegającą na stworzeniu dystansu w stosunku do innych osób, na usunięciu zagrożenia przed nieuprawnioną ciekawością, niedyskrecją, nadmierną poufałością"[20]. Ta sama autorka wskazuje na dwojaki charakter prawa do prywatności (podobnie jak wcześniej wspomniany M. Chrabonszczewski) jako kategorii szczególnej, nadrzędnej dla pewnej grupy praw oraz jako samodzielnego dobra podlegającego ochronie. W tym pierwszym przypadku prawo do prywatności wywierałoby wpływ na ocenę realizacji praw znajdujących się w jego zakresie, a uściśleniu podlegałyby wartości objęte zakresem prawa do prywatności. Drugie rozumienie prawa do prywatności – jako dobra samodzielnego – według autorki wzmacnia ochronę osób dochodzących swych praw. Ponieważ ochronie w tym przypadku podlega prywatność w ogólności, a nie poszczególne dobra, ochrona będzie aktywna także w sytuacji, gdy dane dobro nie jest chronione konkretną procedura ochronną[21]. J. Braciak zwraca także uwagę na problemy przy zakreśleniu definicji prywatności, ponieważ to, co znajduje się w sferze prywatnej, zależy od subiektywnej oceny każdego człowieka. W efekcie definicję należałoby w jakiś sposób zobiektywizować. Prywatność jest rozdzielana także na trzy elementy: pierwszy – uprawnienie jednostki do decydowania, jakie informacje na jej temat mogą być udostępniane; drugi – możliwość kontroli udostępnionych informacji i trzeci – stan reglamentowania dostępu do samego siebie[22]. Z tymi elementami łączą się trzy aspekty prywatności: relacyjny (związany z kontaktami z innymi podmiotami), informacyjny (związany z ilością i charakterem przekazywanych informacji) i fizyczny (związany z fizyczną dostępnością do osoby)[23]. Ponieważ pojęcie prywatności jest wspólne dla wielu dziedzin, jego definicja zazwyczaj sprowadza się do sformułowań ogólnych, zmierzających raczej do wyznaczenia ram prywatności niż samej jej treści[24].

Jak widać, stworzenie spójnej, jednolitej definicji prywatności, która byłaby powszechnie aprobowana, jest niemożliwe. Każdy z autorów zajmujących się tą problematyką prezentuje bowiem własną koncepcję i podejście do pojmowania prywatności i jej zakresu.

[19] *Ibidem*, s. 95.
[20] J. Braciak, *op. cit*., s. 47.
[21] *Ibidem.*
[22] R. Dopierała, *Prywatność w perspektywie zmiany społecznej*, Kraków 2013, s. 20.
[23] *Ibidem*, s. 22 i n.
[24] M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 26.

1.1.3. Zakres

Zakres prawa do prywatności jest niezwykle złożony. Jak już zostało wspomniane przy problemach definicyjnych, na pojęcie prawa do prywatności składa się wiele obszarów, które mogą być chronione zarówno jako samoistne wartości, jak i w ramach prawa do prywatności. Wśród takich sfer wymienić należy przede wszystkim: ochronę danych osobowych, korespondencji (lub szerzej tajemnicę komunikowania się), mir domowy, nietykalność cielesną, cześć, godność, wolność sumienia i wyznania, a także wiele innych. Katalog ten wciąż się poszerza, w miarę postępu technologicznego, gospodarczego dodawane są do niego nowe sfery, a precyzyjne wymienienie każdej z nich jest zadaniem niezwykle trudnym. Odnośnie do zakresu prawa do prywatności zakreślonego w Konstytucji RP, J. Braciak pisze: „Z jednej strony nie ma podstaw do przyjmowania, że suma przepisów dotyczących wartości wchodzących w skład sfery życia prywatnego wyznacza jej ostateczne granice czy zakres, a więc że jeśli jakaś dziedzina stosunków nie została przepisami objęta, to pozostaje poza konstytucyjnymi gwarancjami prywatności”[25]. Prywatność nie podlega jednak ochronie absolutnej. Jak każde prawo ma swój koniec tam, gdzie leży granica, początek odpowiadającego prawa innej jednostki. Ochrona prywatności może doznawać pewnych ograniczeń, które uzasadnione będą interesem bądź społecznym, powszechnym, bądź indywidualnym konkretnej jednostki[26]. W pierwszym przypadku prawo do prywatności jest w konflikcie z innymi prawami w sytuacji przedkładania dobra ogółu związanego z tymi innymi prawami nad dobro jednostki[27]. Ograniczanie prywatności nie może być uznaniowe, następować może tylko w ostateczności, w sytuacji braku innego rozwiązania musi przebiegać w zgodzie z przewidzianymi prawem mechanizmami (działania uprawnionego organu i tylko takiego, odpowiadające pewnej procedurze, po spełnieniu przewidzianych przesłanek), nie może następować samowolnie. Uzasadnienie stanowi interes publiczny, który musi znaleźć odzwierciedlenie w przepisach prawa. Tenże interes to podstawowe wartości społeczeństwa, takie jak: bezpieczeństwo, porządek publiczny, ochrona zdrowia publicznego, moralności[28]. Konflikt prywatności z tymi dobrami musi być rozstrzygany w szerokim kontekście w odniesieniu zarówno do prawa, moralności, jak i do finansów. Z kolei naruszenie prywatności wynikające z tego konfliktu powinno być jak najmniejsze i nastąpić w razie konieczności jedynie w niezbędnym zakresie. Równie skomplikowana wydaje się być zatem druga sytuacja naruszania prawa do prywatności, która jest uzasadniana interesem jednostki. W tym przypadku skonfliktowane zostaje prawo do prywatności z innym prawem lub wolnością danej jednostki. Można zaryzykować stwierdzenie, że poza sytuacją ratowania życia lub zdrowia oba z tych skonfliktowanych praw mają wagę w zasadzie równą. Powstaje zatem pytanie, jak ów konflikt powinien zostać rozstrzygnięty i czy w przypadku przypisania przegranej prawu do prywatności taka sytuacja będzie dostatecznie uzasadniona[29]. Osob-

[25] *Ibidem*, s. 164.
[26] *Ibidem*, s. 53.
[27] M. Chrabonszczewski, *op. cit.*, s. 95.
[28] *Ibidem*, s. 111 i n.
[29] *Ibidem*, s. 115.

ną kwestią jest wyrażenie zgody na ograniczenie prywatności w danej sytuacji. Prawo do prywatności jest bez wątpienia prawem niezbywalnym, a więc niemożliwe jest jego zrzeczenie się. Wydaje się jednak, że wyrażenie zgody na ograniczenie bądź naruszenie prawa do prywatności przez konkretną osobę w konkretnej sytuacji jej dotyczącej jest dopuszczalne w myśl sentencji *volenti non fit iniuria*. Zgoda taka musi jednak spełniać pewne niezbędne wymagania. Należą do nich: świadomość jej wyrażenia, brak pozorności, błędu, niewątpliwość zgody[30]. Uzasadnieniem możności wyrażenia zgody na naruszenie prywatności może być także jeden z zasygnalizowanych już problemów leżących u podstaw trudności definicyjnych związanych z prawem do prywatności i prywatnością w ogólności, tj. subiektywność względem oceny tego, co leży w sferze prywatnej, a co już poza nią. W tym kontekście każda jednostka ma jakoby uprawnienie do zakreślania własnych granic swojego prawa do prywatności i konkretnych sfer, które wchodzą w jego skład, zgodnie z własnymi, subiektywnymi przekonaniami, moralnością, dobrem. Te granice nie zawsze muszą pokrywać się z tymi ogólnymi, wyznaczonymi przez normy prawne lub przyjętymi jako ogólna wartość w danej zbiorowości.

1.1.4. Prawne standardy ochrony prawa do prywatności w UE

Standardy ochrony prywatności w państwach członkowskich Unii Europejskiej wynikają z przepisów Europejskiej Konwencji Praw Człowieka, traktatów, Karty praw podstawowych, tradycji wspólnych dla państw członkowskich, aktów prawa wtórnego, a przede wszystkim z orzeczeń TSUE. Przepisy EKPC, którym UE zapewnia poszanowanie na mocy art. 6 TUE, stanowią standard minimalny ochrony, która musi być zapewniona przez poszczególne państwa – strony konwencji. Każde z państw-sygnatariuszy konwencji może zatem zapewnić szerszy zakres ochrony niż wyznaczony wspomnianym aktem prawnym, nie może jednak zejść poniżej wymaganego minimum. Wymienione przez EKPC cztery sfery ochrony nie są precyzyjnie określone, stanowią raczej ogólny i niezdefiniowany dokładnie katalog, co zapewne wynika z samej specyfiki tego aktu jako aktu ogólnego, którego sformułowania w założeniu mają być akceptowane i przyjęte przez możliwie najszerszy krąg sygnatariuszy, i z drugiej strony specyfiki ochrony prywatności jako sfery pojemnej i chronionej w różnym zakresie przez państwa członkowskie. Terminy użyte w regulacji ochrony prywatności EKPC są szerokie[31]. Prawo do prywatności nie jest jednak absolutne, a ingerencja w opisane prawa jest co do zasady niedopuszczalna na gruncie EKPC. Jest ona możliwa jedynie w razie konieczności z uwagi na szczególne przesłanki mieszczące się w ramach interesu publicznego, w przypadkach określonych w ustawie, o czym stanowi art. 8 par. 2 konwencji[32]. Standard ochrony prawa do prywatności wynikający z KPP to w zasadzie przyjęcie standardu wynikającego z EKPC, art. 8 Konwencji wskazuje, że „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji”[33], natomiast

[30] J. Braciak, *op. cit.*, s. 52.
[31] J. Braciak, *op. cit.*, s. 72.
[32] EKPC, art. 8.
[33] *Ibidem*, art. 8.

art. 7 karty, mówi, że „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się”[34]. Sformułowanie tych przepisów jest niemal identyczne. Poszerzeniu ulega tylko zakres ochrony prywatności w sferze komunikowania się, w odniesieniu do EKPC, gdzie ochronie podlega korespondencja, Karta natomiast szerzej wymienia wolność komunikowania się. Stopień ochrony praw zawartych w KPP jest pomocniczo określony w art. 53, który stanowi, że żadne z postanowień Karty nie może być interpretowane jako ograniczające prawa człowieka wynikające z prawa UE, międzynarodowego i wspólnych tradycji państw członkowskich[35]. Podobnie jak w EKPC prawo do prywatności podlega ograniczeniom na mocy art. 52 KPP, zgodnie z którym każde ograniczenie praw musi być proporcjonalne, przewidziane przez ustawę i konieczne ze względu na ogólny interes wynikający z ochrony praw i wolności innych osób[36]. Na podstawie przywołanych powyżej przepisów wynika, że standard ochrony prawa do prywatności wyznaczony przez nie jest niezwykle ogólny. Wynika to z ogólności samych aktów i ich przeznaczenia jako aktów dających pewną podstawę do konkretniejszej regulacji, a także jako aktów, których postanowienia mają być respektowane przez wiele podmiotów zapewniających różny poziom, zakres i stopień ochrony prywatności. Tak nieostre zapisy pozwalają, z jednej strony, swoim zakresem objąć więcej przypadków, mieć zastosowanie w większej liczbie sytuacji i stanów prawnych, a także obejmować coraz to nowe sfery, które wraz ze zmianami technologicznymi czy nawet obyczajowymi ochronie podlegać powinny. Z drugiej strony, brak wyraźnego zakresu i konkretnej sankcji wskazuje na niepewność takiej ochrony i możliwość nadużyć. Kluczowe znaczenie dla standardu ochrony prawa do prywatności ma zatem konkretyzacja występująca w postaci aktów prawa wtórnego UE i w szczególności orzecznictwa Trybunału Sprawiedliwości UE.

Akty prawa wtórnego odnośnie do prawa do prywatności w UE to m.in.: dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[37] i planowane zastąpienie dyrektywy rozporządzeniem[38] w tym zakresie, dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[39], rozporządzenie nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 o ochronie osób fizycznych w związku

[34] KPP, art. 7.

[35] *Ibidem*, art. 53.

[36] *Ibidem*, art. 52.

[37] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. WE L 281 z 23.11.1995 r.

[38] Rozporządzenie Parlamentu Europejskiego i Rady – Wniosek Komisji w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) z dnia 25 stycznia 2012 r. COM(2012) 11 final. Dalej: Rozporządzenie ogólne

[39] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) Dz. Urz. WE L 201 z 31.07.2002 r.

z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[40]. Aktów praw wtórnego UE w zakresie prawa do prywatności jest wiele. Jak już zaznaczono, odpowiadają one zmianom koniecznym dla ochrony prywatności zachodzącym w wyniku rozwoju technologicznego. Dyrektywa z 1995 r. traktująca o ochronie danych osobowych ma zostać planowo zastąpiona rozporządzeniem uwzględniającym problemy wynikające z rozwoju zagrożeń dla tej sfery prywatności związanych z internetowym gromadzeniem i przetwarzaniem danych i skokiem technologicznym w tym zakresie.

Podsumowując, standard ochrony prywatności wciąż się poszerza, obejmując nie tylko zmiany zakresu ochrony związane z przeobrażeniami społecznymi, gospodarczymi, technologicznymi. Należy zaznaczyć że zmiana z dyrektywy wiążącej państwa członkowskie co do rezultatu, poziomu harmonizacji prawa ochrona wchodzi na poziom rozporządzenia, a więc na poziom ujednolicenia wiążącego państwa bezpośrednio, bez konieczności implementacji. Szczególnie ważne dla wyznaczania ochrony prywatności zdaje się być orzecznictwo TSUE. Wydaje się, że w istocie wyznacza ono zakres i pojemność – standard ochrony praw w UE, w tym w szczególności interesującego prawa do prywatności. W tym zakresie warto zwrócić uwagę na wyrok Trybunału z dnia 18 maja 1982 r. *AM & S Europe Limited przeciwko Komisji Wspólnot Europejskich* (sprawa 155/79), w którym uznano za niedopuszczalne naruszenie tajemnicy korespondencji pomiędzy prawnikiem a jego klientem[41], sprawa C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. LTD*, która dotyczyła ujawniania danych osobowych[42], sprawy, w których Trybunał precyzuje warunki naruszenia prawa do prywatności – stwierdza, że nie jest to prawo absolutne i może podlegać ograniczeniom – w wyroku z dnia 26 czerwca 1980 r. *National Panasonic (UK) Limited przeciwko Komisji Wspólnot Europejskich* (sprawa 136/79)[43] i wskazuje, że naruszenie takie musi odpowiadać nadrzędnym interesom Wspólnoty, a środki muszą być proporcjonalne – w wyroku z dnia 11 lipca 1989 r. *Hermann Schräder HS Kraftfutter GmbH & Co. KG przeciwko Hauptzollamt Gronau* (sprawa 265/87)[44]. Wreszcie trzeba mieć na uwadze orzeczenie z 13 maja 2014 r. dotyczące popularnie określanego „prawa do bycia zapomnianym", które stanowi pewnego rodzaju kamień milowy w zakresie ochrony prywatności[45]. Orzeczenie to szerzej omawiane będzie w dalszej części pracy jako szczególnie

[40] Rozporządzenie nr 45/2001/WE Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz. Urz. L 008 z 12.01.2001 r.

[41] Wyrok Trybunału C-155/79 z dnia 18 maja 1982 r. *AM & S Europe Limited przeciwko Komisji Wspólnot Europejskich*, EU:C:1982:157.

[42] Wyrok Trybunału C-28/08 z dnia 29 czerwca 2010 r. *The Bavarian Lager Co. Ltd przeciwko KWE*, EU:C:2010:378.

[43] Wyrok Trybunału C-136/79 z dnia 26 czerwca 1980 r. *National Panasonic (UK) Limited przeciwko Komisji Wspólnot Europejskich*, EU:C:1980:169.

[44] Wyrok Trybunału C- 265/87 z dnia 11 lipca 1989 r. *Hermann Schräder HS Kraftfutter GmbH & Co. KG przeciwko Hauptzollamt Gronau*, EU:C:1989:303.

[45] Wyrok Trybunału C- 131/12 z dnia 13 maja 2014 r. *Google Spain, Google Inc vs Agencia de Protection de Datos, Mario Costeja Gonzalez*, EU:C:2014:317.

ważne dla ochrony prywatności. Odnośnie do prawa do prywatności Trybunał wypowiadał się zatem wiele razy, a sprawy, którymi się zajmował, dotyczyły wielu sfer wchodzących w skład prywatności – nie sposób nawet przytoczyć wszystkich z najważniejszych spraw.

1.2. Podstawa prawna, pojęcie i zakres ochrony danych osobowych

1.2.1. Podstawa prawna

Ochronę danych osobowych zapewnia wiele systemów międzynarodowych, w tym w szczególności system Rady Europy, który ochronę danych osobowych zapewnia w ramach kilku konwencji międzynarodowych (m.in. konwencji nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonej w Strasburgu)[46]. W Unii Europejskiej dane osobowe chronione są, po pierwsze, na najwyższym stopniu ogólności w art. 16 TFUE, z którego wynika, że każdy ma prawo do ochrony danych osobowych jego dotyczących[47]. Podstawa ochrony jest zawarta także w KPP. Art. 8 Karty stanowi, że „Każdy ma prawo do ochrony danych osobowych, które go dotyczą"[48]. Poza tym dane osobowe odnajdują podstawę do ochrony w kilku dyrektywach, z których najważniejsze znaczenie ma dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i ich swobodnego przepływu[49]. Pozostałe zawierające podstawy ochrony danych osobowych to: dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego[50], dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[51]; dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE[52]. Poza dyrektywami znaczenie dla podstaw ochrony danych osobowych mają rozporządzenia, m.in. rozporządzenie Komisji Nr 611/2013

[46] Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonej w Strasburgu, Dz. U. z 2003 r. Nr 3, poz. 25.

[47] Traktat o funkcjonowaniu Unii Europejskiej, wersja skonsolidowana, Dz. Urz. UE C 326/01 z 26.10.2012 r., art. 16.

[48] KPP, art. 8.

[49] Dyrektywa 95/46/WE.

[50] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego, Dz. Urz. WE L 178 z 17.07.2000 r.

[51] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz. Urz. WE L 201 z 31.07.2002 r.

[52] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług

z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych[53] oraz rozporządzenie nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[54].

Problem ochrony danych osobowych okazał się być na tyle ważny, że podjęto reformę ochrony danych na szczeblu unijnym. Rozwój technologii spowodował, że rozwiązania dyrektywy 95/46/WE stały się niewystarczające i nie zapewniały dłużej odpowiedniego stopnia ochrony danych. W zasadzie to rozwój technologii, w szczególności niezwykle szybki rozwój sieci Internet, wymusił zmiany w modelu ochrony danych osobowych, tak aby dopasować metody ochrony danych do nowo powstałych problemów. Trwające od 2012 r. prace nad reformą mają już właściwie swój finał, 14 kwietnia 2016 r. bowiem projekt ogólnego rozporządzenia o ochronie danych osobowych został przyjęty przez Parlament[55]. Prace nad reformą rozpoczęły się 25 stycznia 2012 r., kiedy to Komisja zaproponowała pakiet legislacyjny składający się z rozporządzenia ogólnego o ochronie danych osobowych i dyrektywy o ochronie danych osobowych przetwarzanych na potrzeby ścigania przestępstw. Rozporządzenie to stanowi przejście z harmonizacji prawa państw członkowskich do ujednolicenia prawa. Będzie bezpośrednio stosowane dwa lata po wejściu w życie.

Podstawa prawna ochrony danych osobowych w Unii Europejskiej jest zatem odnajdywana w wielu aktach różnego szczebla – zarówno w traktatach, jak i w aktach prawa wtórnego.

1.2.2. Pojęcie

Ochrona danych osobowych jako prawo może być przede wszystkim rozumiana dwojako: jako osobne, niezależne prawo[56] bądź jako element prawa do prywatności. W polskiej nauce prawa wyraźny jest także trzeci pogląd – o krzyżowaniu się tych dwóch systemów ochrony i ich niezależności[57]. W tym poglądzie, jeśli pewien stan faktyczny nie znajduje ochrony w ramach ochrony danych osobowych, może znaleźć protekcję poprzez ochronę prywatności. Wydaje się, że taki pogląd można z powodzeniem przenieść na grunt prawa międzynarodowego i unijnego. Same dane osobowe w dyrektywie 95/46/WE rozumiane są jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej”[58]. Osoba ta z kolei to „osoba, której tożsamość można

łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz. Urz. UE L 105 z 13.04.2006 r.

[53] Rozporządzenie Komisji nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, Dz. Urz. L 173 z 26.06.2013 r.

[54] Rozporządzenie nr 45/2001…

[55] Komunikat prasowy Rady Europejskiej i Rady Unii Europejskiej, http://www.consilium.europa.eu/pl/policies/data-protection-reform/, [dostęp: 04.05.2016 r.].

[56] A. Mednis, *Prawna ochrona danych osobowych*, Warszawa 1995, s. 14 i n.

[57] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2004, s. 179.

[58] Dyrektywa 95/46/WE, art. 2 lit. a).

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"[59]. Z identycznym zapisem mamy do czynienia w polskiej ustawie o ochronie danych osobowych[60]. Kluczowym elementem tej definicji jest zatem fakt zidentyfikowania (lub możliwość zidentyfikowania) danej osoby – powiązania konkretnych informacji z konkretną osobą. Za każdym razem więc odszyfrowanie czy dane informacje są danymi osobowymi w rozumieniu art. 2 dyrektywy wymagało będzie rozważenia, czy dana informacja pozwala na identyfikację konkretnej osoby. Rozporządzenie definiuje dane osobowe podobnie, dodając w definicji możliwej do zidentyfikowania osoby szczególne rodzaje przykładowych identyfikatorów: „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"[61]. W definicjach tych akcentuje się zatem nie samą treść danych, ale to, czy informacje te można powiązać z konkretną osobą[62]. Motywy do rozporządzenia ogólnego o ochronie danych osobowych zawierają istotne wskazówki: „Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny"[63]. Nie budzi wątpliwości, że danymi osobowymi będą takie informacje jak: imię, nazwisko, PESEL czy numer dokumentu identyfikującego daną osobę, jak np. dowód tożsamości czy paszport, lub zazwyczaj adres. Problematyczną kwestią natomiast są takie informacje jak adres IP komputera i adres poczty elektronicznej. Nie ulega wątpliwości, że ocena, czy dana informacja stanowi dane osobowe, musi być dokonywana w konkretnych przypadkach, z uwzględnieniem specyfiki tego konkretnego przypadku. Tak też Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 11 grudnia 2014 r. *Nejvyšší správní soud – Republika Czeska – František Ryneš/Úřad pro ochranu osobních údajů* (sprawa C-212/13) uznał, że nagranie z kamery video rejestrujące wizerunek danej osoby, jeśli umożliwia jej identyfikację, stanowi dane osobowe[64]. Sprawa doty-

[59] *Ibidem.*

[60] Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., Dz. U. z 1997 r. Nr 133, poz. 883, art. 6.

[61] Rozporządzenie ogólne, art. 4 pkt 1.

[62] A. Mednis, *Dyrektywa 95/46 w świetle orzecznictwa Trybunały Sprawiedliwości Unii Europejskiej – wybrane zagadnienia*, [w:] A. Mednis (red.), *Prywatność a ekonomia, ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013, s. 130.

[63] Rozporządzenie ogólne, motywy, pkt 26.

[64] Wyrok Trybunału C-212/13 z dnia 11 grudnia 2014 r. *František Ryneš/Úřad pro ochranu osobních údajů*, EU:C:2014:2428.

czyła nagrań z monitoringu prywatnej posesji i fragmentu drogi, które to nagrania pomogły w zidentyfikowaniu sprawców szkód na posesji, a widoczny w niej jest także dodatkowy problem, tj. konflikt ochrony danych osobowych sprawcy i ochrony prywatności, bezpieczeństwa właściciela posesji. W sprawie 446/12 *Willems i in*. Trybunał nie podaje nawet w wątpliwość, że danymi osobowymi są dane biometryczne pobierane i przetwarzane w celu wydania paszportu lub dokumentu tożsamości i jego sprawdzania[65]. W orzeczeniu z dnia 16 grudnia 2008 r. w sprawie C-524/06 *Heinz Huber przeciwko Bundesrepublik Deutschland* dotyczącym przetwarzania danych w rejestrze odpowiednim dla prowadzenia działalności gospodarczej dla obywateli państw trzecich Trybunał uznał, że dane zawarte w tym rejestrze są z całą pewnością danymi osobowymi w świetle dyrektywy 95/46/WE[66]. W sprawie C-101/01 *Göta hovrätt przeciwko Bodil Lindqvist* Trybunał orzekł, że informacja o nazwisku w połączeniu z numerem telefonu stanowi dane osobowe w rozumieniu przepisu dyrektywy 95/46[67]. W sprawach połączonych C-465/00, C-138/01 i C-139/01 Trybunał wskazał, że informacja o nazwisku i osiąganych rocznych dochodach stanowi dane osobowe[68], podobnie jak w sprawie C-73/07, gdzie za dane uznano informacje o dochodach z działalności zarobkowej[69].

Z powołanych orzeczeń wynika duża rola TSUE w ustalaniu, co można za dane osobowe uznać, oraz uwidocznienie związku konkretnej informacji z możliwością identyfikacji konkretnej osoby. Za dane osobowe mogą być uznane bardzo różne informacje, co widać na przykładzie nagrań z monitoringu w przywołanym orzeczeniu. Pod pojęciem „dane osobowe" mogą zatem kryć się rozmaite informacje, a nawet obrazy czy nagrania – aby za takie je uznać, konieczne jest spełnienie ogólnych przesłanek wynikających z art. 2 dyrektywy. Ogólność sformułowań definicji danych jest podstawą do doprecyzowywania ich znaczenia przez praktykę, tworzy ona zasadniczo duże pole dla interpretacji[70].

Dyrektywa wprowadza także osobną kategorię danych, tzw. dane wrażliwe. Art. 8 definiuje je jako takie dane osobowe, które ujawniają informacje o pochodzeniu rasowym, etnicznym, opinie polityczne, przekonania religijne, filozoficzne, przynależność do związków zawodowych, dane dotyczące zdrowia i życia seksualnego[71]. Już wstępna analiza przywołanego przepisu pozwala na stwierdzenie, że dane wrażliwe to ten szczególny

[65] Wyrok Trybunału C-446/12 do C-449/12 z dnia 16 kwietnia 2015 r. *W.P. Willems* (C-446/12) *przeciwko Burgemeester van Nuth, H. J. Kooistra* (C-447/12) *przeciwko Burgemeester van Skarsterlân, M. Roest* (C-448/12) *przeciwko Burgemeester van Amsterdam i L.J.A. van Luijk* (C-449/12) *przeciwko Burgemeester van Den Haag*, EU:C:2015:238.

[66] Wyrok Trybunału C-524/06 z dnia 16 grudnia 2008 r. *Heinz Huber przeciwko Bundesrepublik Deutschland*, EU:C:2008:724.

[67] Wyrok Trybunału C-101/01 z dnia 6 listopada 2003 r. *Göta hovrätt przeciwko Bodil Lindqvist*, EU:C:2003:596.

[68] Wyrok Trybunału z dnia 20 maja 2003 r. *Rechnungshof* (C-465/00) *przeciwko Österreichischer Rundfunk i innym oraz Christa Neukomm* (C-138/01) *i Joseph Lauermann* (C-139/01) *przeciwko Österreichischer Rundfunk, sprawy połączone*, EU:C:2003:294.

[69] Wyrok Trybunału C-73/07 z dnia 16 grudnia 2008 r. *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy, Satamedia Oy*, EU:C:2008:727.

[70] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy Europejskie*, Warszawa 2010, s. 43.

[71] Dyrektywa 95/46/WE, art. 8.

rodzaj informacji, które potencjalnie najpowszechniej powodują dyskryminację. Ta specyficzna kategoria danych podlega co do zasady zakazowi przetwarzania. Rozporządzenie ogólne o ochronie danych osobowych podobnie wskazuje zakres danych wrażliwych, dodatkowo wymieniając wśród nich orientację seksualną, dane biometryczne i dane genetyczne[72]. Dane biometryczne to z kolei „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 twarzy lub dane daktyloskopijne"[73]. Dane genetyczne to „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"[74]. Te dwie nowe kategorie danych wprowadzone w rozporządzeniu zdają się odpowiadać na nowe rodzaje informacji, które mogą stanowić dane osobowe.

Na potrzeby artykułu warto zaznaczyć także znaczenie terminów istotnych dla ochrony danych osobowych: przetwarzania, administratora danych i przetwarzającego. Przetwarzanie oznacza „każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych"[75], wśród przykładów dyrektywa wymienia gromadzenie, przechowywanie, modyfikację, odzyskiwanie[76]. Administrator danych to podmiot określający cele i sposoby przetwarzania, może być on osobą fizyczną, prawną lub organem władzy publicznej. Przetwarzający z kolei to podmiot przetwarzający dane w imieniu administratora, który – podobnie jak administrator – może być osobą fizyczną, prawną lub organem władzy publicznej[77]. Definicje te nie doznają znaczących zmian w rozporządzeniu.

1.2.3. Zakres

Dane osobowe chronione są w Unii Europejskiej kilkoma dyrektywami. Zatem zakres ochrony obejmuje zarówno gromadzenie i przetwarzanie danych przez podmioty prywatne, jak i gromadzenie i przetwarzanie danych przez instytucje UE. Ochrona obejmuje łączność zarówno elektroniczną, jak i telekomunikację. Standard wyznaczony przez przepisy dyrektywy 95/46/WE jest standardem minimalnym, a rozumienie terminów „dane osobowe" i „przetwarzanie danych" przyjęte w dyrektywie jest szerokie. Pozwala to na objęcie danych osobowych szerszym zakresem ochrony[78], na który w UE wpływa też zabezpieczenie tej ochrony sankcją i możliwością dochodzenia swoich praw. Już Traktat o funkcjonowaniu Unii Europejskiej w art. 16 par. 2 zapewnia, że przestrzeganie zasad ochrony danych osobowych podlega kontroli niezależnego organu[79]. Podob-

[72] Rozporządzenie ogólne, art. 9.
[73] *Ibidem*, art. 4, pkt 14.
[74] *Ibidem*, pkt 13.
[75] *Ibidem*, pkt 13.
[76] Dyrektywa 95/46/WE, art. 2.
[77] *Ibidem*.
[78] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 90.
[79] TFUE, art. 16.

ny zapis znajduje się w Karcie praw podstawowych w art. 8 par. 3[80]. Zakres stosowania omawianej dyrektywy doznał jednak pewnych wyłączeń. I tak na mocy art. 3 dyrektywa nie ma zastosowania do przetwarzania danych w ramach działalności związanej z pewnym interesem publicznym, do którego zaliczane jest tu bezpieczeństwo publiczne, obronność, bezpieczeństwo (w szerokim rozumieniu obejmujące także dobro gospodarcze państwa). W tym zakresie wyłączenie to pod względem przesłanek jest podobne do dozwolonych ograniczeń prywatności i ingerencji w prawo do prywatności. Kolejnym wyłączeniem z zakresu dyrektywy jest przetwarzanie i gromadzenie danych „przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze"[81]. Takie kwestie zostały także poruszone w wyroku Trybunału do wspomnianej już sprawy C-212/13 *František Ryneš/Úřad pro ochranu osobních údajů*. Trybunał orzekł, że nawet nagrywanie kamerą monitoringu rejestrującą obraz w sposób ciągły prywatnej posesji i części drogi publicznej nie jest czynnością o czysto prywatnym lub domowym charakterze i tym samym podlega wymogom przetwarzania i gromadzenia danych określonych w dyrektywie, a to z uwagi na choćby tylko częściowe wykroczenie na przestrzeń publiczną. W opisywanej sprawie TSUE poczynił także znaczące dla zakresu ochrony wywody – zaznaczył, że stosowanie dyrektywy pozwala w razie konieczności na uwzględnienie uzasadnionych interesów administratora stosownie do art. 7 lub 11. Tymi interesami będzie w szczególności ochrona własności, życia, zdrowia[82]. Przepisy dyrektywy wprowadzają także zakaz przetwarzania szczególnej kategorii danych, tzw. danych wrażliwych[83] w art. 8[84] – są to takie dane jak pochodzenie etniczne lub rasowe, przekonania religijne czy też poglądy polityczne. Ich przetwarzanie i gromadzenie jest możliwe tylko w szczególnych wypadkach, po spełnieniu szczególnych przesłanek. W tej kwestii w orzeczeniu z dnia 6 listopada 2003 w sprawie C-101/01 Trybunał uznał, że umieszczenie na stronie internetowej informacji o urazie nogi i zatrudnieniu na niepełny etat jako skutku tego urazu są danymi wrażliwymi z art. 8 par. 1, danymi dotyczącymi stanu zdrowia. W spawie chodziło o umieszczenie na stronie internetowej informacji osobowych o pracownikach parafii, co stanowiło przetwarzanie danych osobowych niespełniające warunków wymaganych dyrektywą i aktem krajowym wydanym w wyniku jej implementacji (w szczególności chodziło tu o wymogi zgody na przetwarzanie danych)[85]. Sprawa ta dowodzi też, jak szeroki jest zakres stosowania dyrektywy – obejmuje ona zbieranie i udostępnianie danych na pozór naturalne, prywatne, a w rzeczywistości także podlegające wszelkim rygorom ich gromadzenia i udostępniania.

[80] KPP, art. 8.

[81] Dyrektywa 95/46/WE, art. 3.

[82] Wyrok Trybunału C-212/13 *František Ryneš*…

[83] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 92.

[84] Dyrektywa 95/46/WE, art. 8.

[85] Wyrok Trybunału C-101/01 z dnia 6 listopada 2003 r. *Göta hovrätt przeciwko Bodil Lindqvist*, EU: C:2003:596.

1.2.4. Prawne standardy ochrony danych osobowych

1.2.4.1. Zasady odpowiedniego poziomu ochrony

Ochrona danych osobowych powinna być zapewniona na odpowiednim, wysokim poziomie. Taki poziom ochrony został wprowadzony w art. 25 dyrektywy 95/46/WE jako jeden z wymogów przy transferze danych do państw trzecich, które to państwo ma zapewnić. Niewątpliwie zatem co najmniej taki sam stopień powinien być zapewniany wewnątrz UE. Jak mów przepis, poziom ten należy oceniać „w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji; szczególną uwagę zwracać się będzie na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, przepisy prawa, zarówno ogólne, jak i branżowe, obowiązujące w państwie trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym państwie”[86]. Brak jest definicji terminu „odpowiedni poziom ochrony”, wprowadzone zostają jedynie zasady odpowiedniości i kryteria, które przy ocenie bierze uprawniona do stwierdzenia na mocy art. 25 dyrektywy 95/46/WE Komisja[87]. Ocena więc i zasady odpowiedniego stopnia ochrony danych osobowych obejmują uwzględnienie wielu czynników[88]. Zasady odpowiedniego poziomu ochrony zdaje się też w ogólności wprowadzać projekt rozporządzenia, które ma zastąpić obowiązującą dyrektywę 95/46/WE. Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych przedstawiła Komisja Europejska 25 stycznia 2012 r. Założeniem projektu jest jeszcze większy zakres ochrony danych osobowych z zachowaniem bazy obowiązującej dyrektywy. Zasadami panującymi w rozporządzeniu jest m.in.: zasada przejrzystości przetwarzania danych, a więc spełnianie obowiązków informacyjnych w uproszczonej, łatwiej dostępnej i przejrzystej dla osoby, od której dane pochodzą, formie; zasada ochrony danych niezależnie od miejsca ich przetwarzania; zasada prywatności jako opcji wyjściowej – związana jest ona w szczególności ze zgodą na przetwarzanie danych, która musi być wyrażona dosłownie, nie może być domyślna, gdyż taka jest tu prywatność, oraz z możliwością decydowania o własnych, indywidualnych ustawieniach prywatności[89]. Zasady odpowiedniego stopnia ochrony danych osobowych sformułowane zostały w dokumencie Grupy Roboczej art. 29 w dokumentach z dnia 26 czerwca 1997 r. nr WP 4 oraz z dnia 24 lipca 1998 r. nr WP 12[90]. Zasady te są podobne do prawnych wymogów gromadzenia i przetwarzania danych z dyrektywy: zasada celowości (dane muszą być przetwarzane w określonych celach), jakości i adekwatności danych (dane muszą być poprawne), wymóg zgody (wymagana jest zgoda osoby, od której dane pochodzą, na przetwarzanie danych), zasady wprowa-

[86] Dyrektywa 95/46/WE, art. 25.

[87] *Ibidem*.

[88] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014, s. 28.

[89] *Ibidem*, s. 21.

[90] Discussion document: First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy) – Grupa robocza Art. 29, WP 4, z dnia 26 czerwca 1997 r. i Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive – WP 12 z dnia 24 lipca 1998 r.

dzenia obowiązku informacyjnego (zapewnienie informacji o celu i sposobie przetwarzania), zabezpieczenia danych (zapewnienie wszelkich środków bezpieczeństwa przetwarzania) i prawa dostępu do danych (informacja o danych i prawo do ich poprawiania dla osoby, od której pochodzą)[91]. Zasady te są więc minimalnymi i podstawowymi standardami i wymogami przetwarzania, które musi spełniać każde z państw członkowskich UE przy gromadzeniu i przetwarzaniu danych, a które szerzej omówione zostaną w dalszej części pracy.

1.2.4.2. Kryteria oceny odpowiedniości poziomu ochrony danych osobowych

Kryteria oceny czy poziom ochrony danych osobowych jest odpowiedni są zawarte w przywoływanym już art. 25 par. 2 dyrektywy. Stwierdzenia odpowiedniego stopnia ochrony dokonuje Komisja Europejska na podstawie całości prawa krajowego danego państwa, a także aktów prawa międzynarodowego przez to państwo przyjętych po uwzględnieniu wszelkich okoliczności dotyczących przekazania danych, takich jak: ich charakter, cel i czas operacji prowadzonych na danych[92]. Ocena, czy dane kryteria są spełnione, dokonywana jest w formie decyzji. Ich analiza pozwala na stwierdzenie, że Komisja wydaje decyzje o odpowiednim poziomie ochrony w różnych zakresach. Możemy znaleźć decyzje ogólne, takie, które stwierdzają pożądany poziom ochrony jedynie w jakimś określonym zakresie, ale też i decyzje stwierdzające brak takiego poziomu. Szczególnie ciekawą jest w zakresie oceny odpowiedniego poziomu ochrony decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA. Decyzja Safe Harbor miała stanowić pewnego rodzaju kompromis i dostosowanie ochrony do standardów europejskich w celu zapewnienia odpowiedniego poziomu ochrony danych osobowych w związku z transferem danych na terytorium USA[93]. Zaznaczyć należy, że bezpieczna przystań obejmowała organizacje przetwarzające dane osobowe na terytorium USA, które przystąpiły do programu „bezpieczna przystań", nie zaś w ogólności transfer danych na terytorium USA. Decyzja zawiera zasady ochrony, a odpowiedni poziom ochrony miał być zapewniony poprzez poddanie podmiotów przetwarzających dane kontroli Federalnej Komisji Handlu i wymogowi ujawniania mechanizmów ochrony danych[94]. Funkcjonowanie Safe Harbor było jednak oceniane krytycznie. Jak pisze M. Krzysztofek, „uczestnictwo importera danych w Safe Harbor oznacza domniemanie adekwatnego poziomu ochrony danych przekazanych z Unii, a więc usuwa barierę wynikającą ze statusu USA jako kraju trzeciego"[95], co stanowi

[91] M. Krzysztofek, *op. cit.*, s. 32.

[92] Dyrektywa 95/46/WE, art. 25 par. 2 i par. 6.

[93] M. Krzysztofek, *op. cit.*, s. 131.

[94] Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA, Dz. Urz. WE L 215 z 25.08.2000 r.

[95] M. Krzysztofek, *op. cit.*, s. 133.

punkt wyjścia w rozważaniach na temat funkcjonowania programu. Znaczna liczba uczestników programu nie spełniała podstawowych kryteriów uczestnictwa w bezpiecznej przystani, a wykazano ponad to utrudnienia w realizacji praw przez osoby, których dane były przetwarzane niezgodnie z wymogami programu[96]. Komisja Europejska w wielu swoich raportach sygnalizowała o nieprawidłowościach w programie Safe Harbor, a w raporcie z dnia 27 listopada 2013 sformułowała 13 postulatów mających za cel poprawę funkcjonowania programu i wezwała władze USA do podjęcia kroków w celu poprawy sytuacji[97]. Wyrok Trybunału C-362/14 z dnia 6 października 2015 r. dowodzi, że nieprawidłowości nie zostały usunięte. Sprawa ta dotyczyła użytkownika portalu społecznościowego Facebook Maximiliana Schremsa, który to zażądał od komisarza zakazania w ramach kompetencji przekazywania danych do spółki Facebook Inc z siedzibą w USA w związku z niewystarczającym stopniem ochrony danych osobowych przez spółkę. Komisarz odmówił przeprowadzenia dochodzenia, uznając, że na podstawie wcześniej przywoływanej decyzji Komisji Safe Harbor poziom ochrony uznawany jest apriorycznie za odpowiedni. W związku z odmową Schrems wniósł skargę do High Court, który zwrócił się z pytaniem prejudycjalnym do TSUE. Pytanie dotyczyło kompetencji niezależnego urzędnika państwowego powołanego do pełnienia funkcji związanych z ochroną danych osobowych do badania w razie wątpliwości skarżącego odpowiedniego poziomu ochrony danych transferowanych do państwa trzeciego i ewentualnego bezwzględnego związania ustaleniami UE wynikającymi z decyzji Komisji. Trybunał w odpowiedzi uznał, że decyzja Komisji, taka jak decyzja 2000/520, jest wiążąca dla wszystkich organów państw członkowskich, dopóki TSUE nie stwierdzi jej nieważności. Jednak taki stan rzeczy nie może pozbawiać obywateli możliwości wniesienia skargi do krajowych organów powołanych w celu ochrony praw wynikających z ochrony danych osobowych. Organ nie może samodzielnie stwierdzić nieważności decyzji Komisji, ponieważ jest to kompetencja Trybunału, ale jest obowiązany do rozpatrzenia skargi. W przedmiocie ważności decyzji 2000/520 Trybunał wskazał na szereg uchybień sprzecznych z prawem unijnym: brak uregulowania drogi prawnej w celu dostępu do danych przez jednostkę, możliwości ich sprostowania lub usunięcia, brak określenia reguł w razie ingerencji w zagwarantowane prawa podstawowe. Trybunał uznał w efekcie, że nieważny jest art. 1 decyzji, a w związku z pozbawieniem krajowych organów nadzorczych ich kompetencji w świetle art. 3 decyzji – TSUE uznał nieważność także tego zapisu. W związku z tym, że oba uznane za nieważne artykuły mają wpływ na decyzję w całości, w konsekwencji Trybunał orzekł o nieważności decyzji Komisji 2000/520[98]. To orzeczenie może mieć ogromne konsekwencje. Po pierwsze, organy krajowe są obowiązane do rozpatrzenia spraw dotyczących ochrony danych osobowych nawet w sytuacjach uregulowanych postanowieniami unijnych przepisów bezpośrednio obowiązujących, w trakcie postępowania mają możliwość skierowania do

[96] Raport firmy Galexia, http://www.galexia.com/public/research/articles/research_articles-pa08.html, [dostęp: 10.01.2016 r.].

[97] M. Krzysztofek, *op. cit.*, s. 135.

[98] Wyrok Trybunału C-362/14 z dnia 6 października 2015 r. *Maximillian Schrems Przeciwko Data Protection Commissioner, przy udziale: Digital Rights Ireland Ltd*, EU:C:2015:650.

TSUE pytanie prejudycjalnego. Po drugie, nieważność decyzji umożliwiającej transfer danych osobowych na teren USA ma duże znaczenie gospodarcze. Uznanie za odpowiedni poziom ochrony poziomu gwarantowanego przez uczestników bezpiecznej przystani było zapewne dużym ułatwieniem w wymianie handlowej. W sytuacji nieważności decyzji 2000/520 może okazać się, że poziom ochrony danych osobowych podlegających transferowi do USA nie był odpowiedni i zostały naruszone prawa wielu osób, od których dane te pochodziły.

1.3. Konkluzje

Podsumowując, prywatność najogólniej rozumieć można jako sferę wolną od ingerencji zarówno władzy, jak i drugiego człowieka. Trudno o jednoznaczną, precyzyjną definicję. Problemy definicyjne mają niewątpliwie wpływ na sposób i poziom ochrony prywatności. Trudności związane z ochroną prywatności wynikają z niemożliwości precyzyjnego rozgraniczenia tego, co mieści się w sferze prawa do prywatności. Definicje opierają się na przykładowym wyliczeniu obszarów, które mogą wchodzić w zakres omawianego prawa. Należy zaznaczyć, że poszczególne aspekty prywatności zmieniają się na przestrzeni lat wraz z rozwojem chociażby technologii. Aprobowanym podejściem jest ujęcie rzeczonego prawa jako instrumentu hamowania nadmiernej ingerencji w obszar wolności jednostki[99].

Dane osobowe – w przeciwieństwie do prywatności – posiadają swoje definicje legalne w ustawodawstwach zarówno krajowych, jak i aktach prawa unijnego. Tak jak i w przypadku ochrony prywatności, rozwój technologiczny ma wpływ na problemy interpretacyjne i problemy z określaniem, czy dane, konkretne informacje, którymi dysponuje podmiot, są danymi osobowymi w świetle obowiązujących przepisów. Problemy definicyjne i interpretacyjne w przypadku obu omawianych praw – do prywatności i do ochrony danych osobowych – stwarzają trudności w projektowaniu efektywnej ochrony na poziomie zarówno krajowym, jak i unijnym. Oba prawa niewątpliwie wymagają ochrony, a sam problem efektywnej ich ochrony zdaje się być na przestrzeni lat coraz ważniejszy, czego dowodem jest trwająca reforma ochrony danych osobowych w UE i przyjęcie ogólnego rozporządzenia o ochronie danych osobowych. Reforma ta ma być odpowiedzią na brak odpowiedniej ochrony danych osobowych, a przez to i prywatności, wynikającej z postępu technologicznego i nieadekwatności mechanizmów ochrony przewidzianych rozporządzeniem z 1995 r. Podstawowe trudności i aspekty ochrony prawa do prywatności i ochrony danych osobowych, jako praw ze sobą powiązanych, zostaną omówione w dalszej części pracy.

[99] M. Sakowska-Baryła, *op. cit.*, s. 30.

2. Treść prawa do ochrony danych osobowych jako przejaw prawa do prywatności

2.1. Dopuszczalność przetwarzania danych osobowych w świetle prawa do prywatności

Przy określeniu dopuszczalności przetwarzania danych osobowych w świetle prawa do prywatności konieczne jest powrócenie do problemów definicyjnych obu tych wartości i określenie relacji tych dwóch praw. W literaturze zauważyć można dwa odmienne poglądy. Według pierwszego z nich prawo do ochrony danych osobowych jest prawem będącym częścią składającą się na prawo do prywatności, elementem prawa do prywatności. Drugi pogląd z kolei akcentuje odrębność obu praw. Przyjęcie szerokiego rozumienia terminu „prywatność" pozwala na objęcie nim ochrony danych osobowych jako sfery wymagającej ochrony w ramach ochrony prywatności. Ochrona danych osobowych ma na calu zachowanie anonimowości, a co za tym idzie – bycie pozostawionym w spokoju, wolnym od ingerencji, co w istocie ma zapewniać prywatność[100]. Z drugiej jednak strony zmiany w dziedzinie ochrony prywatności związane głównie z coraz powszechniejszym i łatwiejszym dostępem do informacji powodują konieczność wyspecjalizowania tej ochrony, wyjście poza ramy samego prawa do prywatności[101]. Argumentem na potwierdzenie drugiego stanowiska może też być fakt, że ochrona danych osobowych znajduje poparcie w osobnym przepisie w aktach unijnych w KPP i TFUE[102]. Trudno jednoznacznie opowiedzieć się za którymś z przedstawionych stanowisk i odrzucić drugie, oba bowiem trafnie opisują dwa aspekty powiązań pomiędzy prawem do prywatności i prawem do ochrony danych osobowych. Oba prawa z całą pewnością łączą się w zakresie informacji o danej osobie i jej autonomii informacyjnej, dysponowaniu informacjami o swoim życiu i decydowaniu o udostępnianiu ich[103]. Prywatność ma wpływ na ochronę danych osobowych i tym samym kwestię dopuszczalności przetwarzania danych osobowych. Skoro oba te prawa są ze sobą powiązane, a jednostka powinna mieć wyłączne prawo do dysponowania informacjami o sobie, co stanowi przejaw prawa do prywatności, powstaje pytanie, czy przetwarzanie danych osobowych jest dopuszczalne w świetle prawa do prywatności. Prywatność zakłada sferę wolną od ingerencji. Ustalenia wymaga, czy przetwarzanie danych osobowych stanowi ingerencję w prywatność. W obecnym stanie prawnym gromadzenie i przetwarzanie danych osobowych jest możliwe w UE na podstawie dyrektywy 95/46/WE[104]. Wymaga jednak spełnienia kilku warunków. Reforma ochrony danych osobowych i przyjęcie rozporządzenia ogólnego o ochronie danych osobowych także przewiduje przetwarzanie danych osobowych po spełnieniu pewnych warunków. Wydaje się zatem, że przetwarzanie danych osobowych nie stanowi ingerencji w prywatność, jest w świetle prawa do prywatności

[100] *Ibidem*, s. 92.

[101] *Ibidem*, s. 93.

[102] KPP, art. 8, TFUE art. 16.

[103] K. Wygoda, *Ochrona danych osobowych i prawo do informacji o charakterze osobowym*, Warszawa 2002, s. 402.

[104] Dyrektywa 95/46/WE, art. 1.

dopuszczalne, ale jedynie wówczas, gdy przebiega w zgodzie z przepisami prawa. Powinny one wyznaczać takie wymogi przetwarzania danych osobowych, aby w istocie przetwarzanie to odbywało się w warunkach zachowania prywatności osoby, od której dane pochodzą. Art. 1 przywołanej dyrektywy stanowi o celu dyrektywy, „Zgodnie z przepisami niniejszej dyrektywy, Państwa Członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych”[105]. Z podanego przepisu wynika, że przy przetwarzaniu danych osobowych powinno być respektowane prawo do prywatności. Odbywa się to poprzez spełnienie pewnych wymogów, m.in. zgody na przetwarzanie danych osoby, od której one pochodzą, adekwatności, celowości przetwarzania, a także spełnienia szeregu wymogów technicznych, których zachowanie ma na celu zmaksymalizowanie bezpieczeństwa procesu przetwarzania i przechowywania danych[106]. Wymogi te omówione zostaną w dalszej części pracy.

2.2. Wzmacniająca rola prawa do prywatności w realizacji treści prawa ochrony danych osobowych

Jak już zaznaczono, prawo do prywatności odgrywa istotną rolę w realizacji ochrony danych osobowych, w szczególności przy ich udostępnianiu i przetwarzaniu. Wspomniany już art. 1 dyrektywy 95/46/WE zaznacza tę rolę, nakazując respektowanie prawa do prywatności w odniesieniu do przetwarzania danych osobowych. Rolę prawa do prywatności w tym aspekcie podkreślają i uwydatniają także motywy do rzeczonej dyrektywy. Punkt 2 motywów stwierdza: „Systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi; muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności, szczególnie prawo do prywatności”[107]. Rola prawa do prywatności pojawia się także w punkcie 10: „Celem krajowych przepisów prawa dotyczących przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności, które zostało uznane zarówno w art. 8 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz w zasadach ogólnych prawa wspólnotowego; z tego powodu zbliżanie przepisów prawa nie powinno wpłynąć na zmniejszenie ochrony, jaką gwarantują, lecz przeciwnie, musi dążyć do zapewnienia jak najwyższego stopnia ochrony we Wspólnocie”[108]. Z tego sformułowania wynikają wzajemne powiązania prawa do prywatności i ochrony danych osobowych i wzmacniająca rola jednego przy ochronie drugiego. Zarówno motywy dyrektywy, jak i sam jej art. 1 określający cel dyrektywy podkreślają prawo do prywatności i jego rolę w realizacji ochrony danych osobowych.

W kwestii roli prywatności w ochronie danych osobowych uwagę należy zwrócić na wspominaną już sprawę C-212/13 F *Ryneš przeciwko Úřad pro ochranu osobních údajů*. W sprawie tej Trybunał rozstrzygnąć musiał pewnego rodzaju konflikt pomiędzy

[105] *Ibidem*.
[106] *Ibidem*, art. 6.
[107] *Ibidem*, motywy, pkt 2.
[108] *Ibidem*, pkt 10.

prawem do prywatności a ochroną danych osobowych. F. Ryneš w celu ochrony swojej prywatności, majątku, zdrowia i życia zainstalował system kamer monitoringu rejestrujących obraz w sposób ciągły, bez możliwości przeglądu nagrań w czasie rzeczywistym. Kamery rejestrowały wejście do domu oraz fragment drogi publicznej, a ustawione były w pozycji stałej, bez możliwości obracania się[109]. Wielokrotnie dochodziło do ataków na posiadłość F. Ryneš, nieznani sprawcy wielokrotnie wybijali szyby domu. Incydent powtórzył się, a całe zdarzenie zostało zarejestrowane przez system monitoringu. Obejrzenie materiału z kamer umożliwiło identyfikację sprawców. W związku z tym powstało pytanie, czy rejestrowanie obrazu (obejmującego wizerunek osób) za pomocą kamer monitoringu stanowi przetwarzanie danych osobowych w świetle obowiązującej dyrektywy 95/46/WE i powinno odbywać się w zgodzie z jej wymogami, czy też jest to przetwarzanie danych o czysto osobistym charakterze przez osobę fizyczną i w związku z tym podlega wyłączeniu z zakresu stosowania dyrektywy na mocy art. 3 par. 2. Trybunał rozstrzygnął, że korzystanie z kamer monitoringu w celu ochrony swojej prywatności mieści się w zakresie art. 3 par. 2 dyrektywy. Jednak z uwagi na to, że w opisywanej sprawie kamery wykraczały poza przestrzeń prywatną – na drogę publiczną – rejestrowanie obrazu było w istocie przetwarzaniem danych osobowych wymagającym spełnienia wymogów przewidzianych dyrektywą. W pkt 33 wyroku Trybunał zaznacza: „O ile nadzór kamer wideo, taki jak ten w postępowaniu głównym, rozciąga się choćby częściowo na przestrzeń publiczną i tym samym jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, o tyle nie powinien on być rozumiany jako czynność o czysto «osobistym lub domowym charakterze» w rozumieniu art. 3 ust. 2 tiret drugie dyrektywy 95/46”[110]. To przetwarzanie danych powinno podlegać wymogom dyrektywy – w tym zgody osób, od których dane pochodzą, na przetwarzanie, której to zgody nie było. Trybunał nie ma wątpliwości co do tego, że zarejestrowany obraz stanowi dane osobowe, o ile na jego podstawie możliwa jest identyfikacja osoby fizycznej[111]. W opisanej sprawie mamy zatem do czynienia z kolizją prawa do prywatności, broniącego swojej prywatności F. Ryneš, z ochroną danych osobowych sprawców naruszeń. Trybunał wskazuje tu na wagę ochrony danych osobowych i wzmacniającą rolę prawa do prywatności w jej ochronie w przypadku sprawców naruszeń. Idąc za wyrokiem, „Jak wynika z art. 1 i motywu 10 dyrektywy 95/46, jej celem jest zapewnienie wysokiego poziomu ochrony podstawowych praw i wolności osób fizycznych, a szczególnie prawa do prywatności w zakresie przetwarzania danych osobowych. W tym względzie należy zauważyć, że zgodnie z utrwalonym orzecznictwem ochrona prawa podstawowego do prywatności, zagwarantowanego przez art. 7 Karty praw podstawowych Unii Europejskiej, wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia były stosowane jedynie wtedy, gdy jest to absolutnie konieczne. W zakresie, w jakim przepisy dyrektywy 95/46 regulujące kwestię przetwarzania danych osobowych mogącego naruszyć podstawowe wolności, a w szczególności prawo do prywatno-

[109] Wyrok Trybunału C-212/13 *František Ryneš*, pkt 13 i 14.
[110] *Ibidem*, pkt 33.
[111] *Ibidem*, pkt 22.

ści, muszą być bezwzględnie interpretowane z punktu widzenia praw podstawowych, które zostały zawarte w wyżej wskazanej karcie, odstępstwo przewidziane w art. 3 ust. 2 tiret drugie tej dyrektywy musi podlegać ścisłej wykładni”[112]. Trybunał wskazuje zatem na konieczność zapewnienia wymogów ochrony danych osobowych jako zapewniających prawo do prywatności. Wzmacniająca rola prawa do prywatności w realizacji ochrony danych osobowych jest w tym przypadku uwypuklona. Trybunał zaznacza, że naruszenia wymogów przetwarzania danych osobowych i odstępstwa od ochrony danych stanowią naruszenie prawa do prywatności.

Rola prawa do prywatności w ochronie danych osobowych i realizacji tej ochrony jest niezwykle ważna, co potwierdza przywołany wyrok. Nie można zaprzeczyć wzajemnym powiązaniom pomiędzy prawem do prywatności a prawem do ochrony danych osobowych.

2.3. Praktyczne przejawy zachowania prawa do prywatności w sferze ochrony danych osobowych

2.3.1. Prawne wymogi przetwarzania danych – zasady przetwarzania, kryteria legalności, uprawnienia podmiotu, od którego dane pochodzą, mechanizmy nadzorcze i wymogi techniczne

Rola, jaką odgrywa prywatność w ochronie danych osobowych, została już zaznaczona. Problem dopuszczalności przetwarzania danych osobowych w świetle prawa do prywatności opiera się na takim ich przetwarzaniu, aby zachowane zostały warunki nieingerencji w sferę wolności jednostki. Prywatność w przetwarzaniu danych osobowych zapewniana jest zatem poprzez pewne wymogi, których spełnienie determinuje możliwość przetwarzania danych. Każde odstępstwo od tych wymogów skutkuje naruszeniem prywatności danej osoby, od której dane pochodzą. Wymogi te wymienia dyrektywa 95/46/WE, a są to: rzetelność, celowość, adekwatność przetwarzania, konieczność, zgoda osoby, od której dane pochodzą, zapewnienie możliwości aktualizowania i poprawiania danych[113]. Do elementów zapewniających poszanowanie prywatności przy przetwarzaniu danych osobowych należy zaliczyć także szereg obowiązków informacyjnych ciążących na podmiocie przetwarzającym dane, a także zapewnienie odpowiedniej jakości danych oraz wymogi techniczne i organizacyjne mające zagwarantować bezpieczeństwo przetwarzania danych. Kolejnym mechanizmem mającym zabezpieczyć prywatność jest prawo sprzeciwu i dostępu do danych osoby, od której te pochodzą. Za aspekt ochrony prywatności można uznać także wymóg utworzenia organu nadzoru w systemie ochrony danych osobowych.

2.3.1.1. Zasady przetwarzania danych osobowych

Zasady przetwarzania danych osobowych wymienia art. 6 dyrektywy 95/46/WE i odpowiednio art. 5 ogólnego rozporządzenia o ochronie danych, a są to wymogi: rze-

[112] *Ibidem*, pkt 27 i n.

[113] Dyrektywa 95/46/WE, art. 6.

telności i legalności, celowości, adekwatności danych, ograniczenia czasowego i zapewnienia możliwości dochodzenia swoich praw[114].

Wymóg działania rzetelnego i zgodnego z prawem przetwarzania danych osobowych określony w art. 6 par. 1 lit. a) dyrektywy nakłada na podmiot przetwarzający dane obowiązek rzetelności – dbania o interesy osoby, od której dane pochodzą. Rzetelność ta przejawiać powinna się w takim podejmowaniu czynności przetwarzania danych, które w jak najmniejszym stopniu naruszą dobro i interesy podmiotu danych, będą możliwie jak najmniej uciążliwe. Kluczowe jest zachowanie odpowiedniego balansu pomiędzy dobrami podmiotu danych i celami podmiotu przetwarzającego dane[115]. Wymóg zgodnego z prawem przetwarzania danych nakłada z kolei na podmiot przetwarzający takie działania, które nie naruszają jakichkolwiek przepisów prawa. Legalność przetwarzania danych oznacza podjęcie czynności w sposób określony prawem, spełniający wszelkie przesłanki i wymogi[116].

Zasada celowości sformułowana jest w art. 6 par.1 lit. b) dyrektywy. Stanowi on, że dane powinny być: „gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem"[117]. Administrator danych ma zatem obowiązek określenia celu przetwarzania danych. Ponadto cel ten musi być legalny, zgodny z prawem[118]. Zasada ta wymaga poinformowania odpowiednich podmiotów, czemu ma służyć przetwarzanie danych, nie wskazując jednocześnie stopnia określoności celu[119]. Określenie celu jest w praktyce rozumiane jako związane z działalnością administratora danych, a zatem przetwarzanie danych musi pozostawać w związku i w zakresie działalności prowadzonej przez podmiot przetwarzający dane[120]. Rozporządzenie z kolei wprost określa, że dane mają być „zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach"[121].

Kolejną z zasad przetwarzania danych jest wyrażona pod literą c) art. 6 par. 1 dyrektywy zasada adekwatności czy też minimalizmu. Przetwarzanie danych ma być „prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone"[122]. Oznacza to, że podmiot przetwarzający dane osobowe może gromadzić tylko takie dane, które są niezbędne ze względu na cel przetwarzania, oraz z drugiej strony usuwać dane, gdy okażą się zbędne[123]. Podkreśla się tu niezbędność gromadzonych i przetwarzanych danych ze względu na cele przetwarzania, a nie odpowiedniość[124]. W projektowanym rozporządzeniu odpowiadający art. 6 par. 1 lit. c) przepis ma brzmienie podkreślające minimalizm, dane osobowe mają być

[114] *Ibidem*.
[115] M. Jagielski, *Prawo do ochrony danych osobowych...*, s. 79.
[116] *Ibidem*, s. 80 i n.
[117] Dyrektywa 95/46/WE, art. 6.
[118] M. Krzysztofek, *op. cit.*, s. 105.
[119] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 89 i n.
[120] *Ibidem*, s. 91.
[121] Rozporządzenie ogólne, art. 5.
[122] Dyrektywa 95/46/WE, art. 6.
[123] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 88.
[124] M. Krzysztofek, *op. cit.*, s. 110.

„adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane”[125].

Zasada jakości danych wyrażona jest pod literą d) wspominanego przepisu. Dane mają być prawidłowe i aktualizowane. Należy podjąć wszelkie działania mające na celu utrzymanie prawidłowych danych, a więc usuwanie i poprawianie danych. Zasada zakłada ścisłość i aktualność danych, tj. utrzymanie stanu merytorycznej prawidłowości z obecnym stanem faktycznym[126]. Podobnie rozporządzenie wymaga, aby dane były „prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane”[127].

Kolejną zasadą jest zasada ograniczenia czasowego. Według art. 6 par. 1 lit. e) dane mają być: „przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane”[128], zapis ten ma podobne brzmienie także w rozporządzeniu. Dalsze przetwarzanie jest także dopuszczalne, ale jedynie dla celów historycznych, statystycznych lub naukowych i jedynie po spełnieniu odpowiednich środków zabezpieczających w dyrektywie, a w rozporządzeniu środków technicznych i organizacyjnych[129].

2.3.1.2. Kryteria legalności przetwarzania danych osobowych

Kryteria legalności przetwarzania danych osobowych to tytuł sekcji II dyrektywy 95/46/WE, w którym wymienione są jedne z najważniejszych przesłanek koniecznych do przetwarzania danych osobowych. Odpowiadający art. 7 dyrektywy art. 6 rozporządzenia ogólnego o ochronie danych osobowych nosi z kolei tytuł „zgodność przetwarzania z prawem”. Wspomniane przepisy wymieniają warunki, z których spełnienie co najmniej jednego jest konieczne do przetwarzania danych.

Pierwszym warunkiem jest zgoda osoby, której dane dotyczą. Dyrektywa wymaga, aby zgoda ta była jednoznaczna[130]. Art. 2 lit. h) dyrektywy zawiera definicję legalną zgody, stanowiąc, że „zgoda osoby, której dane dotyczą, oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych”[131]. W tej kwestii art. 4 pkt 11 rozporządzenia stanowi dodatkowo, że to przyzwolenie ma nastąpić „w formie oświadczenia lub wyraźnego działania potwierdzającego”[132]. Zgoda ta ma być jednoznaczna i jasna, ma więc nie budzić wątpliwości, nie może być dorozumiana[133]. Elementem zgody musi także być swoboda jej wyrażenia. Podmiot danych musi mieć

[125] Rozporządzenie ogólne, art. 5.
[126] M. Krzysztofek, *op. cit.*, s. 108.
[127] Rozporządzenie ogólne, art. 5.
[128] Dyrektywa 95/46/WE, art. 6.
[129] *Ibidem*.
[130] *Ibidem*, art. 7.
[131] *Ibidem*, art. 2.
[132] Rozporządzenie ogólne, art. 4.
[133] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 104 i n.

zapewnione odpowiednie warunki do zdecydowania o swojej zgodzie. Kolejnym wymogiem jest konkretność, określenie jej przedmiotu, sprecyzowanie rodzaju danych podlegających przetworzeniu, podmiotu przetwarzającego, celu, określenie rodzaju operacji na danych osobowych czy też czasu przetwarzania[134]. Zgoda musi być świadoma, a zatem podmiot danych musi zostać należycie poinformowany o okolicznościach przetwarzania danych. Szczególną kategorią zgody na przetwarzanie danych osobowych w dyrektywie 95/46/WE, ale też w rozporządzeniu ogólnym o ochronie danych osobowych, jest zgoda na przetwarzanie tzw. danych wrażliwych uchylająca generalny zakaz przetwarzania tej kategorii danych[135]. Zgoda ta ma być wyraźna, co oznacza konieczność spełnienia szczególnego wymagania. Na administratorze danych ciąży obowiązek udowodnienia, że udzielona została zgoda na przetwarzanie danych. Spełnienie warunków zgody w praktyce nie jest łatwe przez ilość wymogów, którym musi ona odpowiadać. Przykładem może być często spotykane współcześnie zaznaczenie kratki „wyrażam zgodę" przy klauzuli o przetwarzaniu danych osobowych[136]. Praktyka ta została oceniona negatywnie przez grupę roboczą w sprawie wspólnej wykładni art. 26, kiedy to grupa uznała, że zaznaczenie takiej kratki nie powinno być wystarczające do uznania za wyrażenie zgody[137]. Szczególne regulacje co do zgody zawiera rozporządzenie ogólne o ochronie danych osobowych. Art. 7 rozporządzenia określa warunki co do wyrażenia zgody. Zgodnie z tym przepisem administrator musi być w stanie wykazać, że została wyrażona zgoda na przetwarzanie danych osobowych. W przypadku zgody w pisemnym oświadczeniu zgoda na przetwarzanie danych osobowych musi wyróżniać się spośród innych postanowień oświadczenia. Art. 7 wyraźnie stanowi o możliwości wycofania zgody w dowolnej chwili i o tym, że „wycofanie zgody musi być równie łatwe jak jej wyrażenie"[138]. Przepis ten także akcentuje wymóg dobrowolności zgody, wymagając, aby przy ocenie dobrowolności brana była pod uwagę okoliczność, czy od zgody na przetwarzanie danych osobowych uzależniono wykonanie umowy[139]. Uregulowana została także kwestia zgody wyrażonej przez dziecko w przypadku usług społeczeństwa informacyjnego. Przetwarzanie danych osobowych na podstawie takiej zgody będzie legalne w przypadku, gdy dziecko ukończyło 16 lat, a w przeciwnym razie w przypadku potwierdzenia zgody przez osobę sprawującą władzę rodzicielską[140].

Innymi kryteriami legalności przetwarzania danych są: niezbędność przetwarzania dla wykonania umowy, której jedną ze stron jest osoba, od której dane pochodzą; niezbędność przetwarzania dla realizacji zobowiązania prawnego administratora danych; konieczność przetwarzania dla ochrony interesów podmiotów danych lub dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osób trze-

[134] *Ibidem*, s. 106 i n.

[135] Dyrektywa 95/46/WE, art. 8.

[136] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 117.

[137] Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995, (WP 114 z 25.11.2005), s. 11.

[138] Rozporządzenie ogólne, art. 7.

[139] *Ibidem*.

[140] *Ibidem*, art. 8.

cich; konieczność przetwarzania dla realizacji zadania wykonywanego w interesie publicznym lub władzy publicznej przekazanej administratorowi danych[141]. Te przypadki to, obok zgody podmiotu danych, sytuacje, w których dane można przetwarzać. Brak zgody jest w tych sytuacjach rekompensowany przez konieczność dokonywania operacji na danych. Nie dowolność, a kwalifikowany stan, w którym zachodzi niekwestionowana, niezbędna potrzeba przetwarzania danych, dodatkowo wzmocniona uzasadnionym interesem podmiotu danych, administratora czy publicznym. Owa konieczność i istnienie uzasadnionego interesu są uwypuklone w art. 7 dyrektywy.

2.3.1.3. Uprawnienia podmiotu, od którego dane pochodzą

Prywatność w zakresie ochrony danych osobowych znajduje protekcję także poprzez pewne uprawnienia przysługujące podmiotom danych. Te uprawnienia to wyraz ochrony prywatności już na etapie, gdy dane są lub były przetwarzane w przeszłości.

Niewątpliwie znaczenie mają tu uprawnienia informacyjne osoby, której dane są przetwarzane. Uprawnieniom tym odpowiadają obowiązki informacyjne administratora danych. Podmiot danych ma zagwarantowane prawo do informacji o czynnościach dokonywanych na danych jego dotyczących w celu ochrony jego interesów i weryfikacji tych czynności[142]. Informacja ta może następować w efekcie realizacji prawa do informacji na żądanie lub też jako wykonanie nałożonego prawem obowiązku. Skorzystanie z jednego rozwiązania nie wpływa na realizację drugiego, są one bowiem od siebie niezależne w realizacji[143]. Obowiązki w tym zakresie przewiduje art. 10 i 11 dyrektywy. Administrator danych ma obowiązek udzielić informacji w szczególności o swojej tożsamości, celach przetwarzania i innych informacji, jak np. o odbiorcy danych czy istnieniu prawa do wglądu i poprawiania danych[144]. Katalog ten w dyrektywie jest otwarty. Mocniejszy nacisk na obowiązek informacyjny administratora kładzie rozporządzenie ogólne w sprawie ochrony danych osobowych. Art. 12 rozporządzenia zobowiązuje administratora danych do przekazywania określonych informacji w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny. Administrator ma ponadto obowiązek ułatwiać podmiotowi danych wykonywanie jego uprawnień przysługujących na mocy rozporządzenia[145]. Katalog danych, które administrator ma przekazać, jest szerszy i bardziej szczegółowy niż w dyrektywie, wprowadzony zostaje także termin udzielenia informacji[146].

Podmiotowi danych zapewnia się także prawo dostępu do danych. Uprawnienie to sformułowane zostało w art. 12 dyrektywy i koresponduje z obowiązkami informacyjnymi administratora. Idąc za tym przepisem, podmiot danych ma prawo do uzyskania informacji o tym, czy dane jego dotyczące są przetwarzane, o celu przetwarzania, kategoriach danych, odbiorcach. Informacja o danych poddanych przetwarzaniu ma być

[141] Dyrektywa 95/46/WE, art. 7.
[142] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 119.
[143] *Ibidem*, s. 121.
[144] Dyrektywa 95/46/WE, art. 10.
[145] Rozporządzenie ogólne, art. 12.
[146] *Ibidem*, art. 13 i n.

wyrażona w zrozumiałej formie, bez opóźnienia[147]. Prawo dostępu do danych formułuje także rozporządzenie w art. 15. Rozporządzenie wymienia katalog informacji, do których w ramach tego uprawnienia podmiot danych ma dostęp[148]. Katalog ten został w porównaniu do dyrektywy znacznie rozszerzony.

Podmiot danych ma prawo do poprawiania danych. Prawo to łączy się z zasadą zapewnienia aktualności i prawidłowości danych. Wydaje się zatem, że może być ono realizowane na wniosek osoby, od której dane pochodzą, ale też automatycznie przez administratora danych, jako realizacja obowiązku zapewnienia aktualności i prawidłowości danych[149]. Osoba, której dane dotyczą, ma wg art. 12 lit. b) prawo do „sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z przepisami niniejszej dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych"[150]. Rozporządzenie rozdziela natomiast prawo do poprawiania danych od prawa do ich usunięcia. Art. 16 rozporządzenia mówi o prawie do żądania sprostowania nieprawidłowych danych i uzupełnienia niekompletnych danych[151]. Prawo usunięcia danych jest sformułowane w art. 17, który to nakłada na administratora obowiązek niezwłocznego usunięcia danych w przypadku zajścia wymienionych w przepisie przesłanek, takich jak cofnięcie zgody, niezgodność przetwarzania z prawem[152].

Kolejnym uprawnieniem jest prawo sprzeciwu wobec przetwarzania danych. Zagwarantowane zostało ono w art. 14 dyrektywy i art. 21 rozporządzenia. Prawo to nie ma na celu doprowadzenia do stanu zgodności danych przetwarzanych ze stanem faktycznym, jak uprawnienia opisane w akapicie poprzedzającym, ale wyrażenie braku zgody podmiotu danych na ich przetwarzanie[153]. Sprzeciw ten może nastąpić z uzasadnionych, ważnych przyczyn dotyczących podmiotu danych[154]. W efekcie administratorowi nie wolno już dalej przetwarzać danych objętych sprzeciwem. Prawo to skonstruowane jest podobnie w rozporządzeniu[155]. Ani dyrektywa, ani rozporządzenie nie określają, jakie są to uzasadnione przyczyny pozwalające na wniesienie sprzeciwu. Chodzi tu jednak zapewne o sytuacje, w których dalsze przetwarzanie danych stałoby się dla podmiotu danych wyraźnie uciążliwe, niekorzystne[156].

Opisane uprawnienia podmiotu danych niewątpliwie stanowią wyraz dbałości o prawo do prywatności w realizacji ochrony danych osobowych. Warto zaznaczyć, że reforma ochrony danych osobowych przewiduje nowe, dodatkowe uprawnienia w rozporządzeniu. Są to m.in. prawo do ograniczenia przetwarzania polegające na żądaniu od administratora ograniczenia przetwarzania na odpowiedni czas w określonych przypadkach czy też prawo do przenoszenia danych polegające na uprawnieniu do otrzymania

[147] Dyrektywa 95/46/WE, art. 12.
[148] Rozporządzenie ogólne, art. 15.
[149] M. Krzysztofek, *op. cit.*, s. 149.
[150] Dyrektywa 95/46/WE, art. 12.
[151] Rozporządzenie ogólne, art. 16.
[152] *Ibidem*, art. 17.
[153] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 139.
[154] Dyrektywa 95/46/WE, art. 14.
[155] Rozporządzenie ogólne, art. 21.
[156] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 140.

danych w określonym formacie i przekazania ich innemu administratorowi danych[157]. Środkami, z których skorzystać może podmiot danych w celu ochrony swojej prywatności w zakresie danych osobowych, są także środki indywidualne, a więc wszelkiego rodzaju skargi do organów o kompetencjach nadzorczych czy też do sądu.

2.3.1.4. Mechanizmy nadzorcze i wymogi techniczne

Bezpieczeństwo danych, które ma być zapewnione poprzez stosowanie szeregu wymogów technicznych przewidzianych prawem, jest wyrazem realizacji ochrony prywatności osób, od których dane pochodzą. Obowiązek odpowiedniego zabezpieczenia danych poprzez zapewnienie odpowiednich środków technicznych i organizacyjnych spoczywa na administratorze[158]. Ma to chronić przed bezprawną bądź przypadkową utratą, zniszczeniem, zmianą danych[159]. Obowiązek odpowiedniego zabezpieczenia danych przewiduje także rozporządzenie[160]. Oba akty nie precyzują jednak wymogów technicznych mających zapewnić bezpieczeństwo danych, ograniczając się jedynie do wskazania, że mają być one „odpowiednie". Rozwiązanie takie podyktowane jest tym, że ze względu na różnorodność podmiotów przetwarzających dane, dziedzin, skali działalności wskazanie konkretnych rozwiązań byłoby niemożliwe i nie zapewniałoby adekwatnej ochrony[161].

Faktyczne wypełnianie postulatów ochrony prywatności w kwestiach danych osobowych jest możliwe poprzez zagwarantowanie odpowiedniego nadzoru nad systemem ochrony danych osobowych. Odpowiednie środki i organy nadzoru zapewniają wykonywanie postanowień dotyczących ochrony danych osobowych przewidzianych prawem. Art. 28 dyrektywy nakłada na państwa członkowskie obowiązek ustanowienia co najmniej jednego organu nadzorczego, który będzie odpowiedzialny za kontrolę stosowania przepisów dyrektywy[162]. Organ ten według przepisów dyrektywy wyposażony jest w uprawnienia dochodzeniowe, jak np. prawo dostępu do danych, i uprawnienia interwencyjne, jak np. wyrażanie opinii czy zarządzanie usunięcia lub blokady danych[163]. Organ ten ma działać w sposób całkowicie niezależny[164]. Dyrektywa jako podstawowy środek nadzoru przyjmuje powiadomienie, które określone jest w art. 18. Administrator danych przed przystąpieniem do przetwarzania danych ma obowiązek powiadomić odpowiedni organ nadzorczy[165]. Funkcja powiadomienia wyjaśniona jest w motywach do dyrektywy jako ujawnienie „celów i głównych cech operacji przetwarzania danych, co ma pozwolić na ustalenie, czy operacje te są zgodne z krajowymi przepisami przyjętymi na podstawie dyrektywy"[166]. Nadzór zapewniony w myśl przepisów dyrektywy ma na

[157] Rozporządzenie ogólne, art. 18 i 20.
[158] Dyrektywa 95/46/WE, art. 17.
[159] *Ibidem*.
[160] Rozporządzenie ogólne, art. 32.
[161] M. Krzysztofek, *op. cit.*, s. 158.
[162] Dyrektywa 95/46/WE, art. 28.
[163] *Ibidem*.
[164] *Ibidem*, motywy, pkt 62.
[165] *Ibidem*, art. 18.
[166] *Ibidem*, motywy, pkt 48.

celu przeprowadzenie postępowania kontrolnego zanim jeszcze przetwarzanie danych zostanie rozpoczęte[167]. Rozporządzenie ogólne także przewiduje ustanowienie organu nadzorczego i podkreśla jego niezależność. Art. 52 stanowi: „1. Każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem działa w sposób w pełni niezależny. 2. Członek lub członkowie każdego organu nadzorczego podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem pozostają wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują"[168]. Art. 57 z kolei wymienia zadania organu nadzorczego. Są to m.in.: monitorowanie i egzekwowanie postanowień rozporządzenia, upowszechnianie wiedzy, uprawnienia doradcze[169].

Znaczenie ma także utworzenie na mocy rozporządzenia 45/2001 stanowiska Europejskiego Inspektora Danych Osobowych o szerokich kompetencjach w kwestiach ochrony danych osobowych w UE[170].

2.3.2. Prawo do bycia zapomnianym

Szczególnie ważnym aspektem ochrony prywatności jest tzw. prawo do bycia zapomnianym. W efekcie niezwykle szybkiego tempa przemian technologicznych i związanych z tym problemów przetwarzania danych w Internecie konieczne było znalezienie rozwiązania będącego odpowiedzią na niekontrolowane i długotrwałe przetwarzanie danych osobowych w sieci. Rozwiązaniem zdaje się być prawo do bycia zapomnianym zaznaczone w orzecznictwie TSUE w szczególnie ważnym w tej kwestii wyroku C-131/12 *Google Spain przeciwko Agencia Española de Protección de Datos (AEPD)*. W sprawie tej obywatel Hiszpanii M. Gonzalez domagał się usunięcia nieaktualnej informacji przez Google Inc, która pojawiała się w wynikach wyszukiwania po wpisaniu nazwiska M. Gonzalez do wspomnianej wyszukiwarki. W wyniku skargi do hiszpańskiego organu właściwego dla ochrony danych osobowych skierowano do TSUE pytanie prejudycjalne o rozstrzygnięcie wątpliwości co do tego, czy czynności dokonywane przez operatora wyszukiwarek stanowią przetwarzanie danych osobowych w świetle dyrektywy 95/46/WE[171]. Trybunał, po pierwsze, uznał, że takie czynności stanowią przetwarzanie danych osobowych: „Należy zatem stwierdzić, że operator wyszukiwarki internetowej, przeszukując Internet w zautomatyzowany, stały i systematyczny sposób w poszukiwaniu opublikowanych w nim informacji, «gromadzi» takie dane, «odzyskiwane», «zapisywane» i «porządkowane» przezeń następnie za pomocą oprogramowania indeksującego, «przechowuje» je na swych serwerach oraz, w odpowiednim przypadku, «ujawnia» i «udostępnia» je swym użytkownikom w postaci listy wyników ich wyszukiwań. Ze względu na to, że operacje te zostały wyraźnie i bezwarunkowo wskazane

[167] M. Jagielski, *Prawo ochrony danych osobowych…*, s. 181.
[168] Rozporządzenie ogólne, art. 52.
[169] *Ibidem*, art. 57.
[170] M. Sakowska-Baryła, *op. cit.*, s. 81 i n.
[171] Wyrok Trybunału C-131/12 *Google Spain…*

w art. 2 lit. b) dyrektywy 95/46, należy uznać je za «przetwarzanie» w rozumieniu tego przepisu, i bez znaczenia jest przy tym fakt, iż ten operator wyszukiwarki internetowej przeprowadza te same operacje również w odniesieniu do innego rodzaju informacji i nie wprowadza rozróżnienia między nimi a tymi danymi osobowymi"[172]. Po drugie, Trybunał wyraźnie zaznacza, że działalność operatorów wyszukiwarek internetowych może znacząco oddziaływać na prawo do prywatności i ochrony danych osobowych i dlatego powinna spełniać wymogi dyrektywy w taki sposób, aby w pełni zapewniać poszanowanie dla prywatności[173]. Co w związku z tym kluczowe, Trybunał uznał możliwość usunięcia takich danych: „biorąc pod uwagę znaczenie, jakie zawarte w tych ogłoszeniach informacje mają dla prywatności tej osoby, […] osoba, której dotyczą dane, ma uzasadnione prawo do tego, aby informacje te nie były już wiązane przez taką listę wyników wyszukiwania z jej imieniem i nazwiskiem. Ze względu zatem na to, że w niniejszym przypadku wydaje się, iż nie zachodzą szczególne powody uzasadniające nadrzędny interes kręgu odbiorców polegający na posiadaniu w ramach takiego wyszukiwania dostępu do tych informacji – czego sprawdzenie należy do sądu odsyłającego – osoba, której dotyczą dane, może na podstawie art. 12 lit. b) oraz art. 14 akapit pierwszy lit. a) dyrektywy 95/46 domagać się usunięcia tych linków z tej listy wyników wyszukiwania"[174]. Trybunał zatem stwierdził, że prawa osób, od których pochodzą dane, są nadrzędne w stosunku do interesu odbiorców korzystających z wyników wyszukiwania, uznał, że dyrektywa daje podstawy do usunięcia takich danych i tym samym przyznał „prawo do bycia zapomnianym" w Internecie wywiedzione z przepisów dyrektywy i KPP. Prawo do usunięcia danych przysługuje nawet, gdy nie zostały usunięte ze strony źródłowej i były tam przetwarzane zgodnie z prawem[175]. Wyrok ten niewątpliwie stanowi przełom dla ochrony prywatności w sieci.

Prawo do bycia zapomnianym znalazło się także w rozporządzeniu ogólnym o ochronie danych osobowych. Wspominany już przy okazji innych uprawnień podmiotów danych art. 17 rozporządzenia precyzuje i wyznacza ramy prawa do bycia zapomnianym i możliwości żądania usunięcia danych w określonych rozporządzeniem sytuacjach. Prawo usunięcia danych rozciąga się także na osoby trzecie – dalszych administratorów danych w przypadku upublicznienia danych[176]. Należy zwrócić uwagę, że prawo do bycia zapomnianym nie przysługuje bezwarunkowo w każdej sytuacji, a jedynie jako narzędzie korygowania błędów administratorów danych[177]. Przesłankami do żądania usunięcia danych są bowiem takie sytuacje jak: cofniecie zgody, niezgodność przetwarzania z prawem, wniesienie sprzeciwu czy też brak dalszej niezbędności danych dla celów, w których zostały zebrane[178]. Jak zaznacza M. Krzysztofek, stosowanie prawa do bycia zapomnianym w kształcie określonym przez art. 17 rozporządzenia może

[172] *Ibidem*, pkt 28.
[173] *Ibidem*, pkt 38.
[174] *Ibidem*, pkt 98.
[175] M. Krzysztofek, *op. cit.*, s. 165.
[176] Rozporządzenie ogólne, art. 17.
[177] M. Krzysztofek, *op. cit.*, s. 160.
[178] Rozporządzenie ogólne, art. 17.

w praktyce nastręczać wielu trudności. Postęp technologii powoduje problemy z dezaktualizowaniem się podstawowych pojęć w dziedzinie ochrony danych osobowych. Jako przykład może służyć pojęcie administratora danych i konieczność rozważenia, jakie podmioty powstałe w związku z postępującą cyfryzacją o specyficznych, szczególnych cechach mogą być uznawane za administratora danych[179].

2.4. Konkluzje

Prawo do prywatności niewątpliwie pozostaje w relacji z prawem do ochrony danych osobowych. Często pełni rolę wzmacniająca dla ochrony danych, a często także ochrona danych osobowych jest realizowana jako konkretyzacja prawa do prywatności. Prywatność w przetwarzaniu danych osobowych zagwarantowana jest szeregiem wymogów i warunków, których spełnienie jest konieczne, aby do przetwarzania danych mogło w ogóle dojść. Nie jest zatem tak, że udostępnianie danych osobowych, gromadzenie ich i przetwarzanie stanowi naruszenie prywatności osób, od których pochodzą. Operacje wykonywane na danych osobowych nie stanowią nadmiernej ingerencji w prywatność właśnie dzięki spełnianiu wymienionych w niniejszym rozdziale przesłanek. Podmiot danych poprzez przewidziane prawem mechanizmy, jak zgoda na przetwarzanie czy sprzeciw wobec przetwarzania, ma prawo do decydowania, które dane pozostają prywatne, nieudostępnione, dysponuje swoimi danymi. Reforma ochrony danych osobowych zmierza w kierunku zapewnienia większej efektywności ochrony danych wobec niezwykle szybkiego postępu technologicznego i związanych z nim zmian w zakresie powstania nowych rodzajów podmiotów przetwarzających dane, nowych rodzajów danych. Należy ocenić pozytywnie wprowadzanie nowych mechanizmów ochrony danych, takich jak chociażby prawo do bycia zapomnianym, które mają odpowiadać na problemy przetwarzania danych związanych z ich skalą i nowymi wyzwaniami spowodowanymi głównie niezwykłym rozwojem sieci Internet od czasu wejścia w życie w 1995 r. dyrektywy 95/46/WE. Najlepszym dowodem na niezbędność takich rozwiązań jest liczba wniosków o usunięcie danych po przełomowym wyroku C-131/12 do Google, która na dzień 3 maj 2016 r. wynosiła 425872, w wyniku których usunięto 1483666 linków[180]. Dane te stanowią też dowód na coraz większą świadomość społeczną o tym, jak wielką wagę ma ochrona danych osobowych i ochrona prywatności.

[179] M. Krzysztofek, *op. cit.*, s. 169.

[180] Raport Google, https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en, [dostęp: 03.05.2016 r.].

3. Udostępnianie danych osobowych jako przejaw ograniczania prawa do prywatności

3.1. Skala zjawiska przetwarzania danych osobowych jako zwiększające się zagrożenie dla prywatności

3.1.1. Powszechność zjawiska związana z rozwojem nowych technologii i handlem międzynarodowym.

Od dnia uchwalenia dyrektywy 95/46/WE i później implementacji jej przez państwa członkowskie w odpowiednich przepisach prawa krajowego do dnia dzisiejszego można zaobserwować kluczowe dla poziomu ochrony danych osobowych wynikającego z dyrektywy zmiany. W szczególności niezwykłe upowszechnienie się sieci Internet stanowi wyzwanie dla ochrony danych osobowych. Dostęp do Internetu stworzył nowe środowisko do przetwarzania danych o szczególnej specyfice. Masowość dostępu powoduje liczne zagrożenia dla ochrony danych osobowych. Dość stwierdzić, że dyrektywa nie przewiduje rozwiązań dostosowanych do tej platformy przetwarzania danych osobowych, ponieważ uchwalenie jej miało miejsce jeszcze długo przed upowszechnieniem się Internetu. Punkt 9 motywów do rozporządzenia ogólnego o ochronie danych osobowych w tej kwestii informuje: „Cele i zasady dyrektywy 95/46/WE pozostają aktualne, jednak wdrażając ochronę danych w Unii, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w Internecie”[181]. Sama powszechność Internetu, liczba podmiotów z niego korzystających i wciąż powiększająca się ilość treści, jakie w sieci można znaleźć, powoduje zasadnicze zagrożenia dla ochrony danych osobowych i prywatności z tym związanej. Wśród zagrożeń należy wymienić wielopłaszczyznowość przetwarzania danych, zbieranie i przetwarzanie danych w braku wiedzy podmiotów danych o tych operacjach, trudności z wyegzekwowaniem usunięcia danych z sieci, uwidocznienie się nowych informacji, które powinny zostać uznane za dane osobowe (jak np. dane geolokalizacyjne, adresy IP), problem profilowania, przetwarzania danych w chmurze czy na portalach społecznościowych[182]. Rozwój technologii spowodował także dezaktualizację podstawowych dla ochrony danych definicji, czego przykładem jest sprawa C-131/12 i związane z nią wątpliwości co do pojęcia administratora danych[183]. Tego typu zagrożenia niewątpliwie stanowią niebezpieczeństwo dla prawa do prywatności. Brak wiedzy o dokonywanych na danych operacjach, a co za tym idzie – brak kontroli nad przetwarzaniem wynikający z wielości podmiotów przetwarzających dane w sieci, powielanie danych i tym samym ich ogromna ilość, wymuszone względami technicznymi jako prewencja przed utratą danych to negatywne aspekty przetwarzania danych w świetle rozwoju technologii[184]. Skalę zjawiska zaznaczono w motywach do rozporządzenia ogólnego o ochronie danych osobowych: „Szybki

[181] Rozporządzenie ogólne, motywy, pkt 9.
[182] M. Krzysztofek, *op. cit.*, s. 355.
[183] Wyrok Trybunału C-131/12 *Google Spain*…
[184] M. Krzysztofek, *op. cit.*, s. 357.

postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych"[185]. Tak dynamiczny rozwój systemów technologicznych często nie pozwala na określenie kto, w jakim zakresie i w jakim celu dysponuje danymi osobowymi. Wydaje się jednak, że nie sama okoliczność wykorzystywania systemów informatycznych przez powszechne oswojenie się z nimi i umiejętności korzystania z nich, ale skala zjawiska powoduje zagrożenie dla prywatności[186]. Masowość usług komunikacyjnych w sieci powoduje także wiele wątpliwości związanych z prywatnością, coraz większa ilość rozmaitych informacji udostępnianych przez podmioty danych, informacji związanych z prywatnością, często o coraz większym stopniu intymności, powoduje powstanie wątpliwości, czy informacje te udostępniane są w świadomie oraz czy podmiot danych ma wiedzę o konsekwencjach upubliczniania tego typu informacji[187]. Niezbędne jest wypracowanie nowych, odpowiednich pojęć i zapewnienie właściwej kontroli nad procesami przetwarzania danych[188]. Postęp technologiczny jest zatem dużym zagrożeniem dla prywatności w sferze danych osobowych i nie tylko. Odpowiedzią na te zagrożenia ma być właśnie reforma ochrony danych dostosowana do nowo powstałych wyzwań w czasie obowiązywania dyrektywy.

3.1.2. Praktyczne przejawy ograniczania prawa do prywatności w sferze ochrony danych osobowych

3.1.2.1. Zwolnienia z wymogów przetwarzania danych

W praktyce ochrona prywatności w zakresie danych osobowych doznaje wielu ograniczeń. Dyrektywa 95/46/WE przewiduje w art. 13 możliwość przyjęcia przez państwa członkowskie środków ograniczających prawo do dostępu do danych, obowiązków informacyjnych administratora i zasad przetwarzania danych. Ograniczenie to musi być uzasadnione koniecznością zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, czynności w sprawach karnych, ważnego interesu ekonomicznego państwa, funkcji kontrolnych związanych z wykonywaniem władzy publicznej, ochrony podmiotu danych, praw i wolności innych osób[189]. Choć przesłanki przyjęcia środków ograniczających odnoszą się do wybranych uprawnień i obowiązków

[185] Rozporządzenie ogólne, motywy, pkt 6.

[186] M. Sakowska-Baryła, *op. cit.*, s. 44.

[187] *Ibidem*, s. 45.

[188] D. Głowacka, J. Lipowicz, *Uwagi do strategii poprawy skuteczności unijnych przepisów dotyczących ochrony danych osobowych, przedstawionej przez KE*, Warszawa 2011, s. 11.

[189] Dyrektywa 95/46/WE, art. 13.

związanych z danymi, a także mogą być stosowane jedynie w przypadku zajścia określonych okoliczności o kwalifikowanym znaczeniu, wydaje się, że mimo to ograniczenie takie stanowi naruszenie prywatności podmiotu danych. Są one bowiem w istocie przetwarzane z pominięciem uprawnień podmiotu danych, jest on pozbawiony pewnych aspektów gwarantujących zachowanie prawa do prywatności przy przetwarzaniu danych osobowych. W przypadkach przewidzianych przywołanym przepisem mamy do czynienia z konfliktem interesów: interes prywatny, ochrona prywatności podmiotu danych ściera się tu albo z interesem publicznym państwa, albo z interesem innej osoby. W przypadku opisanych zwolnień pierwszeństwo przydaje się interesowi publicznemu i interesowi innego podmiotu kosztem interesu podmiotu danych. Niewątpliwie, choć taka przewaga powinna mieć miejsce jedynie w uzasadnionych, koniecznych przypadkach, cierpi na tym prywatność podmiotu danych. Podobne rozwiązania przyjmuje ogólne rozporządzenie o ochronie danych osobowych. W motywach zaznaczone zostały warunki ograniczeń: „W prawie Unii lub w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz prawa do informacji, dostępu do danych osobowych i ich sprostowania lub usuwania lub prawa do przenoszenia danych, prawa do sprzeciwu, decyzji opartych na profilowaniu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych oraz określonych powiązanych obowiązków administratorów, o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, by zapewnić bezpieczeństwo publiczne, w tym ochronę życia ludzkiego – w szczególności w ramach reakcji na klęski żywiołowe lub katastrofy spowodowane przez człowieka – zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, ściganie czynów zabronionych lub wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom lub zapobieganie naruszeniom zasad etyki w zawodach regulowanych, ochronę innych ważnych celów leżących w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnego interesu gospodarczego lub finansowego Unii lub państwa członkowskiego, prowadzenie rejestrów publicznych z uwagi na względy ogólnego interesu publicznego, dalsze przetwarzanie zarchiwizowanych danych osobowych w celu dostarczenia konkretnych informacji o postawie politycznej w ramach dawnych systemów państw totalitarnych lub ochronę osoby, której dane dotyczą, lub praw i wolności innych osób, w tym cele w dziedzinie ochrony socjalnej, zdrowia publicznego i cele humanitarne”[190]. Szczegółowe warunki ograniczeń przewiduje art. 23 rozporządzenia. Wydaje się, że wprowadzenie ograniczeń powinno uwzględniać zarówno charakter interesu publicznego i konieczny poziom jego ochrony, jak i charakter prawa do prywatności podmiotu danych. W szczególności zachowana powinna zostać odpowiednia proporcja w realizacji konfliktu interesu publicznego z prywatnym i odpowiedni stopień ingerencji w prawo do prywatności[191].

[190] Rozporządzenie ogólne, motywy, pkt 73.
[191] M. Sakowska-Baryła, *op. cit.*, s. 293.

3.1.2.2. Przetwarzanie danych przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze

Artykuł 3 dyrektywy 95/46/WE określa zakres obowiązywania dyrektywy. Wymogami przewidzianymi dyrektywą według tego przepisu nie jest objęte przetwarzanie danych osobowych przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze[192]. Problemem może okazać się określenie, jakie przetwarzanie ma charakter „czysto osobisty lub domowy". Preambuła dyrektywy przynosi podpowiedź w punkcie 12, gdzie znajdujemy informację o tym, że zasady dyrektywy mają zastosowanie do każdego przetwarzania, należy jednak z zakresu „wyłączyć przetwarzanie danych dokonywane przez osobę fizyczną w wykonywaniu działań o charakterze wyłącznie osobistym lub domowym, jak np. korespondencja i przechowywanie spisów adresów"[193]. Jak pokazuje orzecznictwo, wyłączenie to powoduje wiele wątpliwości interpretacyjnych. I tak w sprawie C-101/01 *Lindqvist* powstało pytanie, czy przetwarzanie danych przez osobę fizyczną polegające na udostępnieniu ich nieograniczonej liczbie osób za pomocą Internetu wyłącznie w celach związanych z wolnością wypowiedzi, bez związku z działalnością handlową czy zawodową stanowi przetwarzanie danych w ramach wyłączenia. W odpowiedzi na powyższe wątpliwości Trybunał orzekł, że: „wyłączenie powinno być interpretowane jako obejmujące wyłącznie działania wchodzące w zakres życia prywatnego lub rodzinnego jednostki, co w sposób oczywisty nie ma miejsca w przypadku przetwarzania danych osobowych polegającego na ich opublikowaniu w Internecie w taki sposób, że staną się one dostępne dla nieograniczonej liczby osób"[194]. Wątpliwości powstały także przy okazji wspominanej już sprawy C-212/13, w której Trybunał rozstrzygał, czy działanie systemu monitoringu w celu ochrony własności, zdrowia i życia właścicieli domu może być uznane za przetwarzanie o czysto osobistym lub domowym charakterze, nawet jeżeli wychodzi częściowo na przestrzeń publiczną. Trybunał uznał, że: „O ile nadzór kamer wideo, taki jak ten w postępowaniu głównym, rozciąga się choćby częściowo na przestrzeń publiczną i tym samym jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, o tyle nie powinien on być rozumiany jako czynność o czysto «osobistym lub domowym charakterze» w rozumieniu art. 3 ust. 2 tiret drugie dyrektywy 95/46"[195]. Przetwarzanie danych o charakterze czysto osobistym lub domowym jest zatem różnie interpretowane i nastręcza wielu problemów. Przetwarzanie w takich warunkach jest wyłączone z zakresu stosowania dyrektywy, a zatem nie stosuje się do niego wymogów przewidzianych przepisami dyrektywy, które to mają zapewniać poszanowanie prywatności w sferze danych osobowych. Wydaje się zatem, że przetwarzanie pozbawione zgody podmiotu danych, w warunkach zwolnienia z zasad rzetelności, jawności, adekwatności, nawet jeśli dokonywane ma być w szczególnym wypadku czynności o wyłącznie osobistym charakterze, w świetle wielu wątpliwości odnośnie

[192] Dyrektywa 95/46/WE, art. 3.
[193] *Ibidem*, motywy, pkt 12.
[194] Wyrok Trybunału C-101/01 Göta hovrätt, pkt 47.
[195] Wyrok Trybunału C-212/13, *František Ryneš*, pkt 33.

do definicji tego charakteru może stanowić w wielu wypadkach naruszenie prywatności osoby, od której dane pochodzą.

3.1.2.3. Przetwarzanie danych osobowych i wolność wypowiedzi

Dyrektywa przewiduje możliwość wyłączenia lub ograniczenia przez państwa członkowskie jej przepisów o kryteriach legalności przetwarzania, obowiązkach informacyjnych i warunkach przetwarzania danych wrażliwych „w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego”[196]. Taka możliwość powstaje jedynie w razie konieczności uzasadnionej zachowaniem przepisów dotyczących wolności wypowiedzi i pogodzenia ich z prawem do prywatności. Wolność wypowiedzi obejmuje także wolność pozyskiwania informacji, której nie towarzyszą obowiązki innych podmiotów związane z udostępnieniem, dostarczeniem informacji[197]. Autonomia jednostki w zakresie określania, które z informacji, danych osobowych o niej mogą zostać udostępnione, może w tym zakresie wywoływać kolizję z wolnością pozyskiwania informacji. Niewątpliwie kolizja taka powoduje zagrożenie dla prywatności podmiotu takich informacji. Dyrektywa nakazuje odpowiednie zachowanie prawa do prywatności, pogodzenie go z wolnością wypowiedzi. Motywy do dyrektywy stwierdzają: „Przetwarzanie danych osobowych dla potrzeb dziennikarstwa lub wypowiedzi o charakterze literackim lub artystycznym, zwłaszcza w dziedzinie techniki audiowizualnej, powinno kwalifikować się do zwolnienia z wymagań niektórych przepisów niniejszej dyrektywy, o ile jest to konieczne, aby pogodzić prawa podstawowe osób fizycznych z wolnością informacji, a zwłaszcza prawem do uzyskiwania i udzielania informacji”[198]. Dalej motywy podkreślają, że takie wyłączenia mają jednak zapewniać równowagę pomiędzy wolnością wypowiedzi a prawami podstawowymi, w tym prawem do prywatności. W tej kwestii problemem może okazać się każdorazowo wyznaczanie granicy, faktyczne zachowanie równowagi pomiędzy tymi prawami[199]. Innym aspektem wolności wypowiedzi, stanowiącym większe jeszcze zagrożenie dla prywatności podmiotów danych, jest wolność rozpowszechniania informacji. Stoi ono w konflikcie z prawem podmiotu danych do kontrolowania, kto posiada konkretne dane. Dlatego też wolność rozpowszechniania informacji powinna być ograniczona odnośnie do sfery prywatności podmiotu informacji jako potencjalnie najgłębiej ingerująca w prawo do prywatności. Ograniczenia tego aspektu wolności wypowiedzi powinny odnosić się do rozpowszechniania informacji tylko konkretnym, określonym osobom, w określonym celu[200]. Rozporządzenie ogólne o ochronie danych osobowych i motywy do niego podobnie zaznaczają konieczność pogodzenia ochrony danych osobowych z wolnością wypowiedzi, dodatkowo zaznaczając: „Aby uwzględnić, jak ważna dla każdego demokratycznego społeczeństwa jest wolność wypowiedzi, pojęcia dotyczące tej wolności, takie jak

[196] Dyrektywa 95/46/WE, art. 9.
[197] M. Sakowska-Baryła, *op. cit.*, s. 307.
[198] Dyrektywa 95/46/WE, motywy, pkt 37.
[199] M. Sakowska-Baryła, *op. cit.*, s. 308.
[200] *Ibidem*, s. 309.

dziennikarstwo, należy interpretować szeroko"[201]. Ze względu na zagrożenie dla prywatności, jakie niesie ze sobą wolność wypowiedzi, rozporządzenie także zaznacza, jak ważna jest równowaga pomiędzy wolnością wypowiedzi a prawami podmiotowymi podmiotów danych. Równowaga ta ma być zapewniana przez konieczność wprowadzenia odpowiednich aktów i przepisów prawnych na poziomie krajowym w państwach członkowskich[202].

3.1.2.4. Wyłączenia od obowiązku informacyjnego

Jednym z warunków zapewniających zachowanie i przestrzeganie prawa do prywatności w zakresie przetwarzania danych osobowych są uprawnienia informacyjne podmiotu danych i odpowiadające im obowiązki informacyjne administratora danych. Przepisy dyrektywy przewidują jednak wyjątki od zachowania obowiązków informacyjnych. Art. 11 dyrektywy traktuje o konieczności dostarczenia informacji o tożsamości administratora, celach przetwarzania i wszelkich dalszych informacji osobie, której dane dotyczą, w przypadku uzyskania ich z innych źródeł. Paragraf 2 tego przepisu zawiera wyłączenie tego obowiązku informacyjnego w przypadku przetwarzania, gdy udzielenie takiej informacji wymagałoby nadmiernych wysiłków lub w przypadku, gdy gromadzenie tych danych jest przewidziane przez prawo[203]. Przepis wskazuje, że takie wyłączenie miałoby w szczególności zastosowanie odnośnie do przetwarzania danych dla celów statystycznych, naukowych lub historycznych. Rozporządzenie ogólne o ochronie danych osobowych wskazuje wśród przesłanek takiego wyłączenia sytuacje, gdy podmiot danych dysponuje już informacjami objętymi obowiązkiem, gdy udzielenie informacji wiązałoby się z niewspółmiernymi wysiłkami, pozyskiwanie i ujawnianie informacji jest wyraźnie uregulowane prawem, które chroni uzasadnione interesy podmiotu danych lub dane muszą pozostać poufne ze względu na tajemnicę zawodową[204]. Katalog przesłanek w rozporządzeniu jest zatem nieco szerszy w stosunku do katalogu z dyrektywy. Choć zwolnienie z obowiązku informacyjnego ma mieć charakter wyjątkowy, usprawiedliwiony określonymi okolicznościami, należy stwierdzić, że może stanowić to naruszenie prywatności. Podmiot danych pozbawiony jest bowiem informacji o przetwarzaniu danych, a co za tym idzie – informacji o celu przetwarzania, zakresie, czasie oraz tożsamości administratora. Uniemożliwiona jest zatem kontrola przetwarzania danych przez podmiot danych i korzystanie z przysługujących na mocy przepisów uprawnień[205].

3.2. Problem ochrony prywatności związany z transgranicznym przepływem danych

Rozwój gospodarczy i handlowy na poziomie międzynarodowym wymaga swobodnego przepływu danych osobowych w dziedzinach, w których dochodzi do przetwa-

[201] Rozporządzenie ogólne, motywy, pkt 153.
[202] *Ibidem*.
[203] Dyrektywa 95/46/WE, art. 11.
[204] Rozporządzenie ogólne, art. 14.
[205] M. Krzysztofek, *op. cit.*, s. 133.

rzania danych. Wyzwaniem i celem dla międzynarodowych porozumień stało się zatem ustalenie wspólnych standardów w tym zakresie. Przyjęcie międzynarodowych porozumień traktujących o ochronie danych osobowych miało na celu zbliżenie poziomu ochrony danych różnych państw, tak aby ułatwić ich transgraniczny przepływ. Transfer danych poza granice kraju powoduje zagrożenia dla ich ochrony, a przez to i dla zachowania prawa do prywatności podmiotu danych, bowiem ochrona w kraju przepływu danych może okazać się nieodpowiednia, niewystarczająca, niezapewniająca odpowiedniego zabezpieczenia danych.

Motywy dyrektywy 95/46/WE wskazują, że funkcjonowanie rynku wewnętrznego, czterech swobód wymaga zapewnienia swobodnego przepływu danych osobowych, a integracja wewnętrzna spowoduje zwiększenie się transferu danych między państwami[206]. Czynnikiem ułatwiającym międzynarodowy przepływ danych jest postęp technologiczny. Celem wprowadzenia dyrektywy była harmonizacja ustawodawstw państw członkowskich w zakresie ochrony danych osobowych, tak aby przy przepływie tych danych pomiędzy nimi poziom ich ochrony był zbliżony w każdym z państw UE[207]. Motywy wskazują także, że „Transgraniczny przepływ danych osobowych jest koniecznym warunkiem rozwoju handlu międzynarodowego; ochrona osób, jaką niniejsza dyrektywa gwarantuje we Wspólnocie, nie stanowi przeszkody dla przekazywania danych osobowych do państw trzecich, które zapewniają odpowiedni stopień ochrony"[208]. Preambuła do rozporządzenia ogólnego o ochronie danych osobowych wskazuje na upowszechnienie się transgranicznego przepływu danych: „Integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia transgranicznych przepływów danych osobowych. Wzrosła wymiana danych osobowych między podmiotami publicznymi i prywatnymi, w tym między osobami fizycznymi, zrzeszeniami i przedsiębiorstwami w Unii. Od organów krajowych państw członkowskich prawo Unii coraz częściej wymaga, by w celu wykonania swoich obowiązków lub w celu realizacji zadań w imieniu organu innego państwa członkowskiego współpracowały ze sobą i wymieniały się danymi osobowymi"[209]. Wydaje się zatem, że gwarantowany w państwach UE poziom ochrony i odpowiedni poziom ochrony w państwach trzecich zapewnia należyte poszanowanie dla prawa do prywatności. Jednak, po pierwsze, sam fakt harmonizacji prawa poprzez dyrektywę nie zakłada jednakowej ochrony we wszystkich państwach członkowskich. Pomiędzy regulacjami mogą istnieć różnice[210]. Inaczej będzie po wejściu ujednolicającego ustawodawstwa w tym zakresie rozporządzenia ogólnego o ochronie danych osobowych. W tej kwestii istotnie rozważania zawarte są w punkcie 13 motywów do rozporządzenia: „Aby zapewnić spójny stopień ochrony osób fizycznych w Unii oraz zapobiegać rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym –

[206] Dyrektywa 95/46/WE, motywy, pkt 3.
[207] *Ibidem*, pkt 8.
[208] *Ibidem*, pkt 56.
[209] Rozporządzenie ogólne, motywy, pkt 5.
[210] M. Jagielski, *Prawo do ochrony danych osobowych*…, s. 191.

w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom – pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten sam poziom prawnie egzekwowalnych praw oraz obowiązków i zadań administratorów i podmiotów przetwarzających, które pozwoli spójnie monitorować przetwarzanie danych osobowych, a także które zapewni równoważne kary we wszystkich państwach członkowskich oraz skuteczną współpracę organów nadzorczych z różnych państw członkowskich"[211]. Po drugie, powstaje problem przepływu danych do państw, które w istocie nie zapewniają odpowiedniego poziomu ich ochrony.

3.2.1. Wyjątki od zakazu transferu danych do państw trzecich niezapewniających odpowiedniego stopnia ochrony

Transfer danych do państw trzecich jest możliwy jedynie, gdy państwo to zapewnia odpowiedni stopień ochrony, który określany jest w świetle wszelkich okoliczności dotyczących operacji dokonywanych na danych[212]. W razie stwierdzenia, że stopień ochrony w państwie trzecim nie jest odpowiedni, państwo członkowskie ma obowiązek podjęcia wszelkich działań w celu nieprzekazania danych do tego państwa. Podobnie, choć bardziej szczegółowo, tę kwestię reguluje rozporządzenie, wymieniając dodatkowo katalog kryteriów brany przez Komisję pod uwagę przy ocenie, czy stopień ochrony danych osobowych w państwie trzecim jest odpowiedni[213]. Oba te akty wprowadzają jednak wyjątki od zasady zakazu transferu danych osobowych do państw trzecich niezapewniających odpowiedniego poziomu ochrony.

Wyjątki od tej zasady określone zostały w dyrektywie w art. 26 par. 2, który stanowi, że „Państwo Członkowskie może zezwolić na przekazanie lub przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2, jeżeli administrator danych zaleci odpowiednie zabezpieczenia odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw"[214]. Środki te mogą wynikać z umowy, dyrektywa nie zamyka jednak katalogu odpowiednich środków[215]. Rozporządzenie ogólne w art. 46 stwarza możliwość transferu danych w braku decyzji o odpowiednim poziomie ochrony w sytuacji, gdy administrator zapewni odpowiednie zabezpieczenia i egzekwowanie praw podmiotów danych. Rozporządzenie wymienia także katalog środków, za pomocą których można osiągnąć takie zabezpieczenia: prawnie wiążące i egzekwowalne instrumenty między organami lub podmiotami publicznymi; wiążące reguły korporacyjne zgodnie z art. 47; standardowe klauzule ochrony danych przyjętych przez Komisję; standardowe klauzule ochrony danych przyjęte przez organ nadzorczy i zatwierdzone przez Komisję; zatwierdzony kodeks postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwa-

[211] Rozporządzenie ogólne, pkt 13.
[212] Dyrektywa 95/46/WE, art. 25.
[213] Rozporządzenie ogólne, art. 45.
[214] Dyrektywa 95/46/WE, art. 26.
[215] M. Krzysztofek, *op. cit.*, s. 208.

rzającego; zatwierdzony mechanizm certyfikacji[216]. Możliwe jest zatem przekazanie danych do państw trzecich, wobec których nie stwierdzono odpowiedniego stopnia ochrony danych osobowych na podstawie zapewnienia administratora o wdrożeniu przed odbiorcę danych odpowiednich zabezpieczeń. Funkcjonowanie tego rozwiązania i praktyczne trudności kontroli nad zapewnianiem środków ochrony przez odbiorcę danych może stanowić poważne zagrożenie dla prawa do prywatności w zakresie przetwarzania danych osobowych.

3.2.2. Odstępstwa od zakazu transferu danych do państw trzecich niezapewniających odpowiedniego stopnia ochrony

Art. 26 par. 1 dyrektywy przewiduje także pewne odstępstwa od zakazu transferu danych do państw trzecich niezapewniających odpowiedniego stopnia ochrony. Rozróżnienie na odstępstwa od zakazu transferu i wyjątki od tej zasady z poprzedzającego punktu opiera się na kryterium zapewnienia odpowiedniej ochrony. Wyjątki wyżej opisane to w istocie środki, które mają zmierzać do zapewnienia odpowiedniego poziomu ochrony poprzez przyjęcie odpowiednich środków przez odpowiednie podmioty w postaci administratora i odbiorcy danych. Odstępstwa od zasady zakazu przekazywania danych do państw niezapewniających odpowiedniego poziomu ochrony będące przedmiotem niniejszego punktu w żaden sposób nie mają na celu rekompensowania braku odpowiedniej ochrony. Są to jedynie przesłanki, które pozwalają na transfer danych nawet w sytuacji braku odpowiedniej ochrony. Wśród nich w art. 26 par. 1 dyrektywa wymienia: jednoznaczną zgodę na proponowany transfer osoby, której dane dotyczą; konieczność przekazania danych dla realizacji umowy; konieczność przekazania ze względu na cele publiczne; konieczność dla zapewnienia interesów osoby, której dane dotyczą; przekazanie danych z rejestru służącego za źródło informacji dla ogółu społeczeństwa[217]. Rozporządzenie do tego katalogu wprowadza pewne modyfikacje. Najważniejszą z nich jest modyfikacja zgody i wprowadzenie obowiązku informacyjnego – zgoda podmiotu danych ma być wyraźna, a podmiot ten ma zostać poinformowany o ryzyku związanym z brakiem decyzji o odpowiednim poziomie ochrony danych osobowych[218]. Odstępstwo od zasady zakazu transferu danych do państw niezapewniających odpowiedniego poziomu danych osobowych poważnie narusza prawo do prywatności osób, od których dane pochodzą. Dlatego powinno być ograniczone do przypadków o niskim ryzyku i do sytuacji wyjątkowych, nielicznych[219]. Jak podkreśla Grupa Robocza art. 29, odstępstwa te mają miejsce jedynie w sytuacjach, w których ryzyko naruszenia prywatności jest niewielkie bądź uzasadnione[220].

Przesłanka zgody osoby, od której dane pochodzą, zdaje się, że i w tym wypadku musi spełniać wymogi analogiczne do zgody na przetwarzanie danych w podstawowym

[216] Rozporządzenie ogólne, art. 46.
[217] Dyrektywa 95/46/WE, art. 26.
[218] Rozporządzenie ogólne, art. 49.
[219] M. Krzysztofek, *op. cit*., s. 268.
[220] Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive – WP 12 z dnia 24 lipca 1998 r.

wariancie[221]. Musi być jednoznaczna, co wprost wynika z przepisu zarówno dyrektywy, jak i rozporządzenia. Jej wyrażenie powinno zostać poprzedzone odpowiednim, poprawnym wykonaniem obowiązków informacyjnych. Podmiot danych musi mieć możliwość odmowy, a zgoda musi być dobrowolna[222].

Gdy odstępstwo wynika z konieczności transferu dla realizacji umowy lub działań poprzedzających zawarcie umowy, przesłankę stanowi tu niezbędność przetworzenia danych. Należy tłumaczyć ją jako brak możliwości realizacji umowy w przypadku nieprzetworzenia danych. Interpretacja tego pojęcia powinna być ścisła, należy wykazać ścisły związek pomiędzy realizacją umowy a przepływem i przetwarzaniem danych[223].

Gdy podstawą odstępstwa jest istotne dobro publiczne, należy zwrócić uwagę na niezbędność takiego przepływu danych dla realizacji interesu publicznego. Ta niezbędność podobnie – nie może być interpretowana rozszerzająco. Kolejną kwestią jest pojęcie istotnego dobra publicznego, czyli takiego, które ma stanowić wartość dla ogółu społeczeństwa[224].

Podstawą transferu mogą być także żywotne interesy podmiotu danych. W tym przypadku także niezbędność transferu dla ich ochrony jest kluczowa, a zdaje się, że to administrator jest uprawniony do określenia, które to z interesów podmiotów danych są żywotne i wymagają ochrony[225].

W sytuacji przepływu danych pochodzących z rejestru, który służy za źródło informacji dla ogółu społeczeństwa, niedopuszczalność odstępstwa byłaby bezprzedmiotowa z uwagi na ogólnodostępność zawartych w danym rejestrze informacji[226]. Wymogiem koniecznym dla transferu danych jest tu jednak spełnienie określonych prawem warunków wglądu do rejestru.

W przypadku odstępstwa ze względu na interes administratora danych należy zwrócić uwagę na istotną kwestię: ponieważ pojęcie istotnego, uzasadnionego interesu administratora danych nie jest zdefiniowane, nie powinno dochodzić do sytuacji, w których interes ten jest nadmiernie przedkładany ponad prawa podmiotowe – w tym prawo do prywatności – osób, od których dane pochodzą. Administrator bowiem może zapewnić odpowiednie środki ochrony danych osobowych[227].

3.3. Konkluzje

Mimo ustanawiania szeregu wymogów i przesłanek gromadzenia, przetwarzania i udostępniania danych osobowych istnieje wiele zagrożeń dla prywatności osób, od których dane pochodzą. Począwszy od rozwoju technologicznego, którego dynamika wciąż wzrasta, zakończywszy na transgranicznym przepływie danych. Zmiany społeczne związane z powszechnością sieci Internet oraz nowe środki i warunki techniczne

[221] M. Krzysztofek, *op. cit.*, s. 269.
[222] *Ibidem*, s. 272.
[223] *Ibidem*, s. 276.
[224] *Ibidem*, s. 278.
[225] *Ibidem*, s. 280.
[226] *Ibidem*, s. 281.
[227] *Ibidem*, s. 282.

przetwarzania danych powodują szybką dezaktualizację zastanych rozwiązań ochronnych i przez to narażanie na brak należytych, odpowiednich zabezpieczeń dla prywatności w sferze informacji o danej osobie. Z kolei rosnące znaczenie współpracy międzynarodowej, handlu międzynarodowego powoduje konieczność i potrzebę coraz częstszego i szerszego przepływu danych pomiędzy państwami. Transfer taki może powodować utratę kontroli nad danymi przez podmiot danych, niepewność co do przysługujących uprawnień i wreszcie wątpliwości co do stopnia ochrony danych i – co z tego wynika – prywatności w systemach prawnych państw odbierających dane. Z uwagi na to, że przepływ danych dokonywany jest nie tylko pomiędzy państwami członkowskimi UE, gdzie istnieją wspólne regulacje prawne dotyczące ochrony danych osobowych zbliżające ustawodawstwa państw członkowskich, ale też i do państw trzecich, temat zagrożeń dla prywatności jest szczególnie ważny i żywy. Poprzedzający rozdział miał na celu ukazanie mechanizmów chroniących prywatność w przetwarzaniu danych osobowych. W tym rozdziale uwidocznione zostały rozwiązania, które mogą stanowić naruszenie lub zagrożenie dla prywatności w sferze ochrony danych osobowych. Choć niewątpliwie przepisy dyrektywy i nowego rozporządzenia mającego zastąpić dyrektywę zmierzają do jak najszerszej ochrony prywatności podmiotów danych, uzasadnione wydają się być wątpliwości co do zakresu ochrony prywatności związane z nieostrością pojęć takich jak chociażby „uzasadniony interes"; nieświadomością osób, których dane dotyczą o kształcie i przebiegu procesu przetwarzania danych; nieświadomością o przysługujących uprawnieniach czy też wreszcie – związaną z funkcjami Internetu, funkcjonowaniem portali społecznościowych czy chociażby z funkcjonowaniem najprostszych nawet aplikacji mobilnych – niewiedzą o tym, ze w ogóle ma miejsce zgoda na przetwarzanie danych, gromadzenie danych i ich przetwarzanie. Podsumowując, należy zatem stwierdzić, że szybkość postępu technologicznego i złożoność procesów przetwarzania danych i ich udostępniania powodują ogromne zagrożenia dla prywatności osób fizycznych w zakresie ich danych osobowych.

Zakończenie

Problematyka ochrony danych osobowych i ochrony prywatności jest niezwykle złożona. W szczególności wpływa na to szybkość zmian technologicznych i wzrost znaczenia handlu międzynarodowego. Po pierwsze, powoduje to szybką dezaktualizację pojęć z dziedziny danych osobowych, pojawianie się coraz to nowych kategorii, których przyporządkowanie pod obecnie obowiązujące definicje okazuje się trudne bądź niemożliwe. Choć dane osobowe i wiele pojęć kluczowych dla tej dziedziny mają swoje definicje legalne, to często nie odpowiadają one potrzebom praktyki, aktualnej rzeczywistości, zaszłym zmianom i obecnym potrzebom. Problem ten ma rozwiązać nowe rozporządzenie ogólne o ochronie danych osobowych, którego rozwiązania mają być dostosowane do zaszłych przez ponad 20 lat po wejściu w życie dyrektywy 95/46/WE zmian. Z kolei, odnosząc się do prywatności, samo stworzenie definicji prywatności okazuje się

niemożliwe ze względu na specyfikę i szerokość tego pojęcia, a z drugiej strony – na zmiany zakresu tego, co prywatne wynikające z przemian społecznych, technologicznych. Niewątpliwie zarówno prywatność, jak i dane osobowe wymagają ochrony, co też znajduje odzwierciedlenie w prawodawstwach zarówno krajowych, jak i międzynarodowych czy wreszcie unijnych.

Problem ochrony danych osobowych w świetle prawa do prywatności szczególnie uwidacznia się podczas dokonywania operacji na danych osobowych, takich jak ich przetwarzanie czy udostępnianie. Operacje te mogą wkraczać w sferę prywatności, naruszać prywatność podmiotu danych. Dlatego też, aby zachować prawo do prywatności, w prawie UE przewidziano szereg wymogów, które mają na celu zminimalizowanie ingerencji w prywatność podmiotu danych. Zachowywanie tych wymogów ma gwarantować zapewnienie poszanowania prywatności. Wraz z narastaniem nowych zagrożeń powstały także nowe mechanizmy zapewniania prywatności w sferze ochrony danych osobowych. Przykładem może być prawo do bycia zapomnianym, które to wywiedzione zostało z obowiązującej jeszcze dyrektywy przez TSUE w orzecznictwie. Kluczowe jednak dla zachowywania prywatności przy okazji dokonywania operacji na danych osobowych jest dostosowywanie wymogów przetwarzania do zmian spowodowanych postępem technologicznym. Tu znowu rozwiązaniem ma stać się reforma ochrony danych i rozporządzenie będące jej efektem. Ma ono zapewniać szersze stosowanie wymogów ochronnych, dostosowanie ich, zaostrzenie. Przewiduje wprost już prawo do bycia zapomnianym. Samo podjęcie reformy w tej kwestii należy ocenić pozytywnie. Próba aktualizacji pojęć, precyzyjne określenie przesłanek i wymogów przetwarzania, uprawnień podmiotu danych i obowiązków administratora danych ma wychodzić naprzeciw problemom ochrony danych powstałych wraz z postępem technologicznym, a szczególnie upowszechnieniem sieci Internet i przetwarzaniem danych w Internecie, co nie miało miejsca w czasach powstawania dyrektywy. Ostateczny efekt reformy i jej realizację w praktyce, to, czy poziom ochrony danych osobowych i co za tym idzie – prywatności – podniósł się, będzie można oceniać po wejściu w życie rozporządzenia ogólnego. Nadal pozostaje jednak pytanie, czy reforma okaże się wystarczająca, jak szybko i czy w ogóle się zdezaktualizuje.

Zachowywanie prywatności w sferze ochrony danych osobowych doznaje też wielu zagrożeń. Przepisy obowiązującego prawa przewidują wiele odstępstw od zachowywania wymogów przetwarzania, a także zwolnienia z nich. Problemem w tej kwestii jest także skala zjawiska przetwarzania, która to wciąż się poszerza. Jak już wielokrotnie zaznaczono, podstawowym zagrożeniem dla ochrony danych osobowych i prywatności w tej sferze jest upowszechnienie się sieci Internet i wzrost znaczenia handlu międzynarodowego i co za tym idzie – przetwarzanie danych w Internecie na niespotykaną dotąd skalę oraz transgraniczny przepływ danych. Powoduje to brak kontroli nad danymi, brak gwarancji ich odpowiedniej kontroli, a jest to z całą pewnością zagrożenie dla prywatności podmiotu danych. Rozwiązaniem w tej kwestii jest wzrost współpracy międzynarodowej również w kwestii aktów regulujących poziom ochrony, a także reforma dostosowana do zmian wynikających z przetwarzania danych w sieci. Taką refor-

mę ma zapewniać rozporządzenie ogólne, a współpraca międzynarodowa odbywa się także poprzez porozumienia międzynarodowe zezwalające na transgraniczny przepływ danych, jak np. zezwolenia na przepływ danych wydawane przez Komisję. Nie zawsze jednak pomimo uzgodnień odpowiedniego poziomu ochrony danych ten poziom jest w praktyce zapewniany, czego przykładem może być porozumienie z USA nazywane *Safe Harbor*, które to miało gwarantować odpowiedni poziom ochrony danych, a które jest negatywnie oceniane jako niespełniające swoich założeń w praktyce. Jak widać na tym przykładzie, nawet próby porozumień co do odpowiedniego poziomu ochrony nie gwarantują jego wprowadzenia i zachowania, co niewątpliwie ma wpływ na zachowywanie albo jego brak prawa do prywatności.

Istnieje zatem bardzo wiele mechanizmów ochronnych mających zapewnić prywatność w sferze danych osobowych, a także wiele zagrożeń dla prywatności w tej dziedzinie. Niewątpliwie można zaobserwować próby podwyższania poziomu ochrony, dostosowywania jej do aktualnych wymogów, dążenie do tego, aby dane osobowe były chronione w odpowiedni sposób, a przez to zapewnienie poszanowania dla prywatności. Przetwarzanie danych w Internecie, próba kontroli i regulacji tego zjawiska nawet w podstawowym stopniu może okazać się dużym wyzwaniem ze względu na powszechność tego zjawiska i ogromną jego skalę. Aktualne zatem wydają się być nadal wątpliwości, czy podjęte w tym kierunku kroki okażą się być wystarczające, czy zapewnią należytą kontrolę nad danymi, co pozwalałoby na zwiększenie poszanowania dla prywatności.

Bibliografia

Literatura

1. Barta J., Markiewicz R., *Ochrona danych osobowych, Komentarz*, Warszawa 2011.
2. Boni M., *Nowe ramy prawne ochrony danych osobowych w UE – Ważne wyzwanie dla Polski*, „Monitor Polski" 2013, nr 8.
3. Braciak J., *Prawo do prywatności*, Warszawa 2004.
4. Chrabonszczewski M., *Prywatność. Teoria i praktyka*, Warszawa 2012.
5. Dopierała R., *Prywatność w perspektywie zmiany społecznej*, Kraków 2013.
6. Fajgielski P., *Kontrola i audyt przetwarzania danych osobowych*, Wrocław 2010.
7. Fajgielski P., *Obowiązki związane z zabezpieczeniem danych osobowych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.
8. Fajgielski P., *Podstawy prawne dopuszczalności przetwarzania danych osobowych*, [w:] S. Fundowicz (red.), *Współczesne problemy prawa publicznego*, Studia z Prawa Publicznego, t. 1, Lublin 1999.
9. Fischer B., *Ponadgraniczne przekazywanie danych osobowych – charakter prawny regulacji z uwzględnieniem uzupełniającej roli soft law*, [w:] A. Mednis (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013.

10. Głowacka D., Lipowicz J., *Uwagi do strategii poprawy skuteczności unijnych przepisów dotyczących ochrony danych osobowych, przedstawionej przez KE*, Warszawa 2011.
11. Głowacka D., *Dostęp do mechanizmów ochrony danych osobowych w krajach UE. Wnioski z raportu Agencji Praw Podstawowych UE*, „Monitor Polski" 2014, nr 9.
12. Gołaczyński J., *Jednostka i państwo w dobie demokracji elektronicznej. Ochrona prywatności, życia osobistego i rodzinnego*, e-biuletyn CBKE, Kwiecień 2006.
13. Ilnicki M., *Prawo do bycia zapomnianym w kontekście „postzniesławiającej" informacji w sieci Internet*, „Palestra" 2014, nr 1/2.
14. Jabłoński M., *Prywatność jako przesłanka ograniczenia dostępu do informacji publicznej*, „Przegląd Prawa i Administracji" 2007, nr 86.
15. Jabłoński M. (red.), *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, Prawnicza i Ekonomiczna Biblioteka Cyfrowa WPAiE UWr, Wrocław 2014.
16. Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010.
17. Jatkiewicz P., *Ochrona danych osobowych. Teoria i praktyka*, Warszawa 2015.
18. Karwala D., Fajgielski P., Konarski X., Mednis A., Sibiga G., *Projekt rozporządzenia PE i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych – zagadnienia wybrane*, „Monitor Polski" 2013, nr 8.
19. Kamińska I., *Ochrona danych osobowych*, Warszawa 2007.
20. Kępa L., *Ochrona danych osobowych*, Warszawa 2014.
21. Kopff A., *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, [w:] Studia Cywilistyczne, t. XX, Kraków 1972.
22. Krzysztofek M., *Ochrona danych osobowych w UE*, Warszawa 2014.
23. Krzysztofek M., *Prawo do bycia zapomnianym i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy" 2012, nr 8.
24. Majchrzak K., *Wzmacnianie świadomości obywateli Unii Europejskiej na temat gromadzenia i przetwarzania danych oraz ich ochrony*, [w] J. Jaskiernia (red.), *Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania*, tom 2, Wydawnictwo Sejmowe, Warszawa 2014.
25. Marcinkowski B., *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*, "Ohio State Law Journal" 2013, nr 6.
26. Mednis A., *Prawo do prywatności a interes publiczny*, Warszawa 2006.
27. Mednis A., *Prawna ochrona danych osobowych*, Warszawa 1995.
28. Mednis A. (red.), *Prywatność a ekonomia, ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013.
29. Safjan M., *Prawo do ochrony życia prywatnego*, [w:] *Szkoła Praw Człowieka*, Helsińska Fundacja Praw Człowieka, Warszawa 2006.
30. Sakowska-Baryła M., *Prawo do ochrony danych osobowych*, Wrocław 2015.
31. Sibiga G., Konarski X. (red.), *Ochrona danych osobowych. Aktualne problemy i wyzwania*, Warszawa 2007.

32. Sibiga G. (red), *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej*, wyd. I, CH Beck, Warszawa 2013.
33. Warren S., *The Right to Privacy*, "Harvard Law Review" 1890, vol. 4.
34. Wiewiórkowski W., *Nowe ramy ochrony danych osobowych w UE*, „Monitor Polski" 2012, nr 7.
35. 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.

Dokumenty

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. z 1997 r. Nr 78, poz. 483.
2. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., Dz. U. z 1997 r. Nr 133, poz. 883.
3. Traktat o funkcjonowaniu Unii Europejskiej, wersja skonsolidowana, Dz. Urz. UE C 326/01 z 26.10.2012 r.
4. Traktat o Unii Europejskiej, wersja skonsolidowana, Dz. Urz. UE C 326/01 z 26.10.2012 r.
5. Karta praw podstawowych Unii Europejskiej, Dz. U. UE C 326/391 z 26.10.2012 r.
6. Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r., Dz. U. z 1993 r. Nr 61, poz. 284.
7. Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu, Dz. U. z 2003 r. Nr 3, poz. 25.
8. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. WE L 281 z 23.11.1995 r.
9. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz. Urz. WE L 201 z 31.07.2002 r.
10. Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego, Dz. Urz. WE L 178 z 17.07.2000 r.
11. Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz. Urz. UE L 105 z 13.04.2006 r.
12. Rozporządzenie nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez insty-

tucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz. Urz. L 008 z 12.01.2001 r.

13. Rozporządzenie nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz. Urz. WE L 8 z 12.01.2001 r.
14. Rozporządzenie Komisji nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, Dz. Urz. L 173 z 26.06.2013 r.
15. Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA, Dz. Urz. WE L 215 z 25.08.2000 r.
16. Rozporządzenie Parlamentu Europejskiego i Rady – Wniosek Komisji w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) z dnia 25 stycznia 2012 r. COM(2012) 11 final.
17. Discussion document: First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy) – WP 4 Grupa robocza art. 29 z dnia 26 czerwca 1997 r.
18. Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995, (WP 114 z 25.11.2005).
19. Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive – WP 12 z 24.07.1998 r.
20. Raport The US Safe Harbor – Fact or Fiction? (December 2008), http://www.galexia.com/public/research/articles/research_articles-pa08.html, [dostęp: 10.01.2016 r.].
21. Raport Google INC., https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en, [dostęp: 03.05.2016 r.].

Orzecznictwo

1. Wyrok Trybunału 29/69 *Stauder przeciwko Ulm*, EU:C:1969:57.
2. Wyrok Trybunału C-155/79 z dnia 18 maja 1982 r. *AM & S Europe Limited przeciwko Komisji Wspólnot Europejskich*, EU:C:1982:157.
3. Wyrok Trybunału C-136/79 z dnia 26 czerwca 1980 r. *National Panasonic (UK) Limited przeciwko Komisji Wspólnot Europejskich*, EU:C:1980:169.
4. Wyrok Trybunału C-265/87 z dnia 11 lipca 1989 r. *Hermann Schräder HS Kraftfutter GmbH & Co. KG przeciwko Hauptzollamt Gronau*, EU:C:1989:303.
5. Wyrok Trybunału C-212/13 z dnia 11 grudnia 2014 r. *František Ryneš/Úřad pro ochranu osobních údajů*, EU:C:2014:2428.

6. Wyrok Trybunału C-446/12 do C-449/12 z dnia 16 kwietnia 2015 r. *W.P. Willems* (C-446/12) *przeciwko Burgemeester van Nuth*, *H.J. Kooistra* (C-447/12) *przeciwko Burgemeester van Skarsterlân*, *M. Roest* (C-448/12) *przeciwko Burgemeester van Amsterdam* i *L.J. A. van Luijk* (C-449/12) *przeciwko Burgemeester van Den Haag*, EU:C:2015:238.
7. Wyrok Trybunału C-524/06 z dnia 16 grudnia 2008 r. *Heinz Huber przeciwko Bundesrepublik Deutschland*, EU:C:2008:724.
8. Wyrok Trybunału C-362/14 z dnia 6 października 2015 r. *Maximillian Schrems przeciwko Data Protection Commissioner*, *przy udziale Digital Rights Ireland Ltd*, EU:C:2015:650.
9. Wyrok Trybunału C-28/08 z dnia 29 czerwca 2010 r. *The Bavarian Lager Co. Ltd przeciwko KWE*, EU:C:2010:378.
10. Wyrok Trybunału C-131/12 z dnia 13 maja 2014 r. *Google Spain, Google Inc vs Agencia de Proteccion de Datos, Mario Costeja Gonzalez*, EU:C:2014:317.
11. Wyrok Trybunału C-101/01 z dnia 6 listopada 2003 r. *Postępowanie karne przeciwko Bodil Lindqvist*, EU:C:2003:596.
12. Wyrok Trybunału C-101/01 z dnia 6 listopada 2003 r. *Göta hovrätt przeciwko Bodil Lindqvist*, EU:C:2003:596.
13. Wyrok Trybunału z dnia 20 maja 2003 r. *Rechnungshof* (C-465/00) *przeciwko Österreichischer Rundfunk i innym oraz Christa Neukomm* (C-138/01) i *Joseph Lauermann* (C-139/01) *przeciwko Österreichischer Rundfunk*, sprawy połączone, EU:C:2003:294.
14. Wyrok Trybunału C-73/07 z dnia 16 grudnia 2008 r. *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy, Satamedia Oy*, EU:C:2008:727.