

ŁUKASZ NASIADKA*

Prawo do bycia zapomnianym w perspektywie przetwarzania danych osobowych

Wprowadzenie

Aktualnie prawo do ochrony danych osobowych stanowi jedno z praw podmiotowych jednostki w demokratycznym państwie prawnym. Jak wskazuje się w literaturze przedmiotu, jest to prawo każdej jednostki do prywatności, poprzez umożliwienie jej kontroli sposobów przetwarzania, tworzenia i zbierania danych osobowych jej dotyczących¹.

Potrzeba zmiany prawa odnoszącego się do ochrony danych osobowych nie wynika z braku regulacji w tym zakresie, lecz bardziej z potrzeby ujednoczenia prawa we wszystkich państwach członkowskich Unii Europejskiej. Wcześniejsze próby nie przyniosły oczekiwanego rezultatu. Za przykład posłużyć może dyrektywa 95/46/WE z 24 października 1995 roku². Przepisy tego aktu normatywnego nie uwzględniały skali przetwarzania danych, która zaistniała w ciągu kilku lat po jego przyjęciu – za sprawą bardzo dynamicznego rozwoju Internetu, nowych technologii oraz ich dostępności. Ponadto, w wyniku implementacji do krajowych porządków prawnych pojawiły się istotne różnice w zakresie stosowania przepisów dyrektywy 95/46/WE przez poszczególne państwa

* Łukasz Nasiadka, mgr, Uniwersytet w Białymstoku, e-mail: lukasz_nasiadka@o2.pl, <https://orcid.org/0000-0001-6909-3899>.

¹ M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 217.

² Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 X 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. UE.L.1995.281.31), dalej „dyrektywa 95/46/WE”.

członkowskie Unii Europejskiej. W takich okolicznościach ustawodawca unijny postanowił uregulować kwestię ochrony danych osobowych za pomocą norm prawnych, z których treści wynikałoby wprost prawo każdej jednostki do weryfikowania dotyczących jej danych osobowych. Przy tym nowe przepisy obowiązywałyby bezpośrednio w każdym z państw członkowskich. Takie przekształcenie prawa unijnego, biorąc pod uwagę czynniki gospodarcze, prawne, społeczne i technologiczne, wydało się niezbędne. Wiele z tych motywów zmian, jak chociażby postęp technologiczny i globalizacja oraz masowe przekazywanie danych w wymiarze globalnym (motyw 6 preambuły) czy funkcjonowanie tak zwanej e-administracji³, finalnie znalazło się w preambule do rozporządzenia o ochronie danych osobowych⁴. Zgodnie ze stanowiskiem doktryny harmonizacja przepisów odnoszących się do ochrony danych osobowych może znacząco przyczynić się do usunięcia niepewności w zakresie stosowania wykładni prawa z uwagi na cel rozporządzenia, jakim jest zapewnienie równorzędnego poziomu ochrony danych, bezpieczeństwa przetwarzania informacji oraz transparentności dokonywanych działań⁵ we wszystkich państwach Unii Europejskiej, w tym również w Polsce.

Zgodnie z rozporządzeniem o ochronie danych osobowych dane osobowe mogą być zbierane i przetwarzane jedynie w konkretnych, uzasadnionych i zgodnych z prawem celach⁶. Podmioty zbierające i przetwarzające dane osobowe zobowiązane są natomiast do poszanowania praw osób, których te dane dotyczą, oraz niedopuszczenia do sytuacji, w której dane byłyby bezprawnie wykorzystywane. W związku z tym, aby wzmocnić ochronę danych osobowych i zapewnić jej skuteczną realizację, na mocy ogólnego rozporządzenia z 2016 r., ustanowiono mechanizm umożliwiający jednostce usunięcie danych osobowych, czyli tak zwane prawo do bycia zapomnianym.

Celem artykułu jest wskazanie zmian prawnych wynikających z rozporządzenia o ochronie danych osobowych, ze szczególnym uwzględnieniem praw osób, których dane dotyczą, a następnie analiza regulacji

³ A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018, s. 17–18.

⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 IV 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), dalej: „rozporządzenie 2016/679” lub „rozporządzenie o ochronie danych osobowych”.

⁵ K. Jastrzębska, *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*, Warszawa 2018, s. 35–37.

⁶ Por. art. 5 ust. 1 lit. a i b rozporządzenia 2016/679.

tw. prawa do bycia zapomnianym. Pierwsza część artykułu zwraca uwagę na sposób przetwarzania danych osobowych i zakres obowiązków ciążących na administratorach danych. Administratorzy danych są bowiem, wraz z inspektorem ochrony danych osobowych, odpowiedzialni za rejestrowanie czynności przetwarzania danych, w tym bieżącą kontrolę i reagowanie na sytuacje ich nieprawidłowego przetwarzania. Część druga skupia się na prawie do bycia zapomnianym oraz na ocenie tego uprawnienia w perspektywie rozporządzenia 2016/679. Metodami badawczymi, którymi posłużono się przy pracy nad artykułem, są: metoda analityczna zastosowana do analizy literatury przedmiotu i metoda dogmatyczno-prawna sprowadzająca się do analizy aktów prawnych oraz analizy orzecznictwa.

1. Prawa osób, których dane dotyczą, a obowiązki administratorów

Mając na uwadze informatyzację życia publicznego, jak również prywatnego, która wiąże się z przetwarzaniem danych na masową skalę, ustawodawca nakłada wiele obowiązków na administratorów danych. Stąd też konieczna stała się intensyfikacja działań na polu zmian regulacji prawnych, przyjętych przez organy krajowe i międzynarodowe, dotyczących danych osobowych.

Istota zmian polega na dopasowaniu uregulowań prawnych do wciąż zmieniającego się rynku, rozwoju nowych technologii i Internetu, a uogólniając – do rozwoju procesów globalizacyjnych. Informatyzacja wiąże się nie tylko z łatwością wykonywania pewnych czynności (komunikacji) na znaczne odległości, lecz także z gromadzeniem i dalszym przetwarzaniem danych – co może stanowić istotne zagrożenie w postaci ich swobodnego przepływu (zwłaszcza danych wrażliwych). Tutaj najważniejszym zagadnieniem wydaje się być bezpieczeństwo informacji systemowych. Istnieje również potrzeba harmonizacji prawa w materii ochrony danych osobowych w kompletny, zapewniający możliwie jak najszerszy przepływ informacji sposób – przy jednoczesnym zapewnieniu jednolitego poziomu ich ochrony. Ujednolicenie prawa w państwach członkowskich Unii Europejskiej ma na celu powszechną akceptację ich przestrzegania w ramach harmonizacji systemowej⁷.

⁷ A. Krasuski, *Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy*, Warszawa 2012, s. 205–207.

W unijnym rozporządzeniu o ochronie danych osobowych na pierwszy plan wysuwają się dwie kwestie. Pierwszą z nich jest wskazanie definicji legalnej **przetwarzania danych osobowych**, drugą – dotyczących tego podstawowych zasad. Do operacji zachodzących (w ramach przetwarzania) na danych osobowych dodano między innymi takie czynności, jak: organizowanie, porządkowanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, ujawnianie (np. przez przesyłanie), dopasowywanie, ograniczanie, usuwanie, niszczenie. Wyliczenie tych operacji ma charakter przykładowy i otwarty. Zaznaczono przy tym, że przetwarzanie danych może mieć charakter zautomatyzowany lub niezautomatyzowany⁸.

Biorąc pod uwagę fakt, że dane osobowe są poddawane przetwarzaniu w systemach nie tylko tradycyjnych, lecz także elektronicznych, rozporządzenie rozbudowuje katalog danych osobowych zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, określając je jako identyfikatory bądź czynniki wspomagające identyfikację. Do identyfikatorów osoby fizycznej oprócz imienia i nazwiska, numeru identyfikacyjnego zaliczono przy tym identyfikatory internetowe, takie jak chociażby adres IP⁹.

Jak niejednokrotnie zostało przedstawione w literaturze przedmiotu, obowiązki administratorów i prawa osób, których dane osobowe dotyczą, są ściśle związane z zasadami ochrony danych osobowych. Standardy, zgodnie z którym mają być przetwarzane dane osobowe, to:

a) legalność, przejrzystość i rzetelność – przetwarzanie danych zgodnie z przepisami prawa, konieczność oparcia przetwarzania na jednej z podstaw dopuszczalności oraz informowanie podmiotów o wszelkich okolicznościach mających wpływ na przetwarzanie ich danych osobowych;

b) minimalizacja danych – zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz ich dalsze nieprzetwarzanie w sposób niezgodny z tymi celami;

c) prawidłowość – aktualizowanie danych, usuwanie i korygowanie błędów oraz zapewnienie zgodności zgromadzonych danych ze stanem faktycznym;

⁸ Art. 4 pkt 2 rozporządzenia 2016/679.

⁹ Art. 4 pkt 1 rozporządzenia 2016/679.

d) ograniczenie przechowywania – gromadzenie danych przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

e) integralność i poufność – przetwarzanie danych w sposób zapewniający odpowiednie ich bezpieczeństwo za pomocą odpowiednich środków technicznych lub organizacyjnych, w tym ochronę przed niepożądanym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;

f) rozliczalność administratora danych za prawidłową ochronę danych osobowych¹⁰.

Administrator, którym jest osoba fizyczna lub prawna, jednostka czy inny podmiot, może samodzielnie albo wspólnie z innym podmiotem określać cel oraz sposób przetwarzania danych¹¹. Wskazane powyżej zasady oraz ich wpływ na prawidłowość procedur odzwierciedlają podstawowe obowiązki administratorów, które można podzielić na trzy kategorie.

W pierwszej kolejności są to obowiązki informacyjne. Dzięki nim osoba ma prawo do uzyskania informacji o tym, jak jej dane są przechowywane, kim jest administrator danych, jaki jest cel, podstawa prawna i czas ich przetwarzania, a także o przysługujących jej prawach (dostępu, sprostowania, usunięcia, przenoszenia, sprzeciwu), charakterze przetwarzania danych (dobrowolnym, wynikającym z ustawy, umowy) oraz o ewentualnych sankcjach wynikających z ich niepodania¹². Funkcja informacyjna daje osobie, której dane dotyczą, możliwość sprawdzenia, czy administrator ma odpowiednie predyspozycje, aby zarządzać jej danymi osobowymi.

Drugą kategorią obowiązków ciążących na administratorze danych osobowych są czynności bezpośrednio związane z wykorzystywaniem danych osobowych. Sprowadzają się one do rejestrowania czynności przetwarzania danych, a więc administrator musi skrupulatnie prowadzić bieżącą rejestrację wszystkich działań polegających na użyciu danych osobowych. Prowadzona dokumentacja stanowi podstawowy dowód na to, w jaki sposób administrator zarządza danymi osobowymi, a przede wszystkim na to, czy ochronę danych można uznać za

¹⁰ D. Lubasz, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów, praktyczne uwagi*, Warszawa 2018, s. 26–28.

¹¹ Art. 4 pkt 7 rozporządzenia 2016/679.

¹² J. Łuczak, *Prawa osoby, której dane dotyczą*, w: *RODO – ogólne rozporządzenie o ochronie danych. Komentarz*, pod red. E. Bielak-Jomaa, D. Lubasza, Warszawa 2018, s. 479–482.

kompletną i prawidłową. W rejestrze powinny się znaleźć takie informacje, jak: imię i nazwisko lub nazwa oraz dane kontaktowe administratora, współadministratorów, inspektora ochrony danych; cel przetwarzania; wskazanie osób, których dane dotyczą i ich potencjalnych odbiorców; rodzaj danych osobowych i ewentualny czas ich usunięcia; informacje o przekazywaniu danych do państwa trzeciego czy organizacji międzynarodowej; opis środków zapewniających bezpieczeństwo danych¹³.

Z uwagi na zagrożenia występujące podczas przetwarzania danych w systemach teleinformatycznych na administratorze ciąży również obowiązek zabezpieczający. Zgodnie z nimi jest on zobligowany do zapewnienia zabezpieczenia technicznego, osobowego oraz rzeczowego danych osobowych, które przetwarza¹⁴. Jest to istotne w perspektywie komunikacji elektronicznej na masową skalę, w której informacje mogą być w łatwy sposób dostępne dla osób nieuprawnionych. Stąd też administrator powinien zwracać uwagę na zachowanie standardów poufności, integralności czy dostępności przetwarzania danych w systemach skutecznego reagowania w sytuacjach kryzysowych czy oceny skutków ochrony¹⁵.

Wszystkie te zmiany konkretyzują czynności związane z przetwarzaniem danych osobowych, wprowadzając regulacje mające przede wszystkim na celu skuteczniejszą ochronę informacji. Nakładają tym samym obowiązki, których realizacja obciąża głównie administratorów i podmioty przetwarzające dane osobowe.

2. Prawo do bycia zapomnianym w świetle rozporządzenia 2016/679

Uprawnienia osoby fizycznej związane z przetwarzaniem danych osobowych jej dotyczących składają się na szeroko rozumiane prawo podmiotowe. Oprócz uprawnień informacyjnych, związanych z dostępem do danych, obejmujących możliwość aktualizacji, sprostowania czy uzupełnienia informacji, warto zwrócić uwagę na prawo do bycia zapomnianym.

¹³ Art. 30 ust. 1 rozporządzenia 2016/679.

¹⁴ M. Ganczar, *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009, s. 171–172.

¹⁵ Zgodnie z art. 32 ust. 1 rozporządzenia 2016/679.

Zgodnie z art. 17 ust. 1 rozporządzenia 2016/679 osoby, których dane są przetwarzane, mają prawo żądania od administratora danych niezwłocznego ich usunięcia, a administrator ma wynikający z przepisów obowiązek usunąć je bez zbędnej zwłoki. Unijny prawodawca dodatkowo wymienia w art. 17 ust. 1 okoliczności, które powinny zachodzić, aby osoba mogła wysunąć względem administratora powyższe żądanie. Zalicza się do nich sytuacje, w których po pierwsze dane osobowe nie są niezbędne do celów, dla których zostały zebrane; po drugie osoba, której dane dotyczą, cofnęła zgodę lub wniosła sprzeciw na mocy art. 21 ust. 1 rozporządzenia; po trzecie dane były przetwarzane niezgodnie z prawem; po czwarte usunięcie danych jest implikowane nałożonym na administratora obowiązkiem prawnym; po piąte dane „zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego”¹⁶.

Zgodnie z powyższym prawo do bycia zapomnianym zależy od ściśle określonych w treści rozporządzenia przesłanek zarówno przedmiotowych, jak i podmiotowych. O ile zakres przedmiotowy nie budzi większych wątpliwości, o tyle zakres podmiotowy nieustannie staje się tematem ożywionej dyskusji. W świetle art. 17 rozporządzenia 2016/679 podmiotami uprawnionymi do żądania usunięcia danych są **osoby, których dane dotyczą**. W celu wyjaśnienia tego zwrotu należy się odwołać do terminologii zawartej w art. 4 pkt 1 rozporządzenia, w której dane osobowe oznaczają „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”¹⁷. Oznacza to, że prawo do bycia zapomnianym przysługuje wyłącznie osobie fizycznej, dlatego też można skonstatować, że katalog podmiotów uprawnionych do skorzystania z tego prawa jest na tyle ograniczony, że nie obejmuje swym zakresem ani osób prawnych, ani jednostek organizacyjnych nieposiadających osobowości prawnej. Nie jest to jednak jedyne ograniczenie prawa do bycia zapomnianym.

Warto zaznaczyć, że prawo do bycia zapomnianym nie działa wstecz. Oznacza to, że jeżeli osoba, której dane dotyczą, zażąda usunięcia pewnej informacji, to takie żądanie ma skutek prawny dopiero z momentem złożenia przez nią oświadczenia woli o wskazanej treści. Prawo do bycia zapomnianym nie rodzi zatem ewentualnych sankcji za wcześniejsze posługiwanie się danymi osobowymi, pod warunkiem że wcześniej było ono legalnym działaniem administratora. Należy przypomnieć, że

¹⁶ Przesłanki usunięcia danych osobowych zostały zawarte w art. 17 ust. 1 rozporządzenia 2016/679, pojawiły się także w treści motywu 65 tego rozporządzenia.

¹⁷ Por. art. 4 pkt 1 rozporządzenia 2016/679.

administrator powinien sam usunąć dane osobowe i zaprzestać dalszego ich przetwarzania, ale również poinformować innych administratorów o wniesieniu żądania usunięcia danych. Biorąc pod uwagę, że dane te mogły zostać udostępnione przez komunikatory elektroniczne, spoczywa na nim obowiązek usunięcia linków, odnośników do informacji o osobie, ewentualnych kopii. Zadanie to wydaje się nad wyraz istotne, gdy dotyczy informacji ujawnionych w sieci (na przykład do rejestracji na portalu społecznościowym). Tutaj prawo do bycia zapomnianym przysługuje zarówno dorosłemu, jak i osobie nieletniej¹⁸.

Co do zasady na każdorazowe żądanie podmiotu administrator powinien usunąć dane osobowe. Istnieje jednak kilka kategorii spraw, kiedy to prawo do bycia zapomnianym nie ma zastosowania. Otóż uprawnienie osoby nie działa, gdy przetwarzanie danych dotyczy wolności wypowiedzi i informacji, jest wymagane do ustalenia, dochodzenia lub obrony roszczeń, do celów archiwalnych, statystycznych, badań naukowych lub historycznych, ze względu na interes publiczny w zakresie zdrowia publicznego oraz kiedy ma zastosowanie przepis prawa, który wymaga przetwarzania określonych danych osobowych¹⁹.

Warto przyrzeć się dokładniej pierwszej przesłance, która stanowić może przeszkodę w skorzystaniu przez jednostkę z prawa do bycia zapomnianym: wolności wypowiedzi i dostępu do informacji. W tym kontekście wypada zaznaczyć, że wprowadzenie RODO w Unii Europejskiej budziło skrajne emocje oraz stanowiło przedmiot sporów już na etapie konsultacji²⁰. Z jednej strony podnoszono obawy, że takie rozwiązanie może być zagrożeniem dla stanu równowagi między wolnością wypowiedzi i dostępem do informacji a prawem do prywatności; z drugiej strony głoszono, że będzie ono skuteczniej gwarantować prywatność jednostek w świecie wirtualnym. Konkurencyjność prawa do prywatności oraz prawa do wolności wypowiedzi i dostępu do informacji niejednokrotnie była poruszana w literaturze przedmiotu²¹.

¹⁸ M. Czerniawski, *Sprostowanie i usuwanie danych*, w: *RODO – ogólne rozporządzenie...*, s. 526–528.

¹⁹ Por. art. 17 ust. 3 rozporządzenia 2016/679.

²⁰ D. Keller, *The new, worse 'right to be forgotten'*, Politico, 27 I 2016, <https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/> (dostęp: 2 III 2023).

²¹ M. Pryciak, *Prawo do prywatności*, „*Studia Erasmiانا Wratislaviensia*” 2010, nr 4, <https://www.bibliotekacyfrowa.pl/Content/37379/011.pdf> (dostęp: 2 III 2023); A. Gonschior, *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej*, w: *Aktualne*

W świetle powyższego, a także uwzględniając treść art. 17 RODO, warto podkreślić, że w Unii prawo do bycia zapomnianym ma ograniczony zasięg oddziaływania w stosunku do osób publicznych. Żądanie osoby, odgrywającej w życiu publicznym ważną rolę, dotyczące usunięcia niechcianych przez nią informacji zamieszczonych w Internecie, nie zawsze spotyka się z aprobatą administratora danych. Zawężenie zakresu ochrony prywatności osób publicznych wynika głównie z chęci utrzymania transparentności ich działań, co jest elementem prawidłowego funkcjonowania systemów demokratycznych²². Kolejną i równie istotną cechą współczesnych demokracji jest efektywne funkcjonowanie kontroli społecznej, co znow wiąże się z większą dostępnością do informacji na temat pełnionych funkcji i poczynań osób publicznych²³. Precyzyjne określenie, jaką funkcję powinna pełnić konkretna osoba, aby można było zaliczyć ją do osób publicznych, co pozwoliłoby administratorowi prawidłowo uzasadnić dostęp ogółu społeczeństwa do informacji na jej temat, może sprawiać trudności. Przykładowa lista takich osób obejmować może między innymi polityków, biznesmenów, urzędników państwowych czy osoby wykonujące zawody regulowane prawnie, to jest lekarzy czy prawników²⁴.

Stwierdzenie, że prawo do bycia zapomnianym to prawo osobiste, jest niezaprzeczone, jednak nie może być uznane za niepodważalne. Ponadto prawo do bycia zapomnianym umożliwia skuteczną

problemy prawa Unii Europejskiej i prawa międzynarodowego. Aspekty teoretyczne i praktyczne, pod red. D. Kornobis-Romanowskiej, Wrocław 2017, s. 239–288.

²² B. Banaszak, K. Wygoda, *Pojęcie funkcji publicznej jako przesłanka modyfikująca zakres ochrony danych osobowych*, w: Biuro Generalnego Inspektora Danych Osobowych, *Ochrona danych osobowych wczoraj, dziś, jutro. Personal data protection yesterday, today, tomorrow*, Warszawa 2006, s. 59 i n.

²³ J. Sieńczyło-Chlabicz, *Ochrona prywatności i wizerunku osób powszechnie znanych w świetle orzeczenia Europejskiego Trybunału Praw Człowieka – von Hannover v. Niemcy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” 2007, nr 4, <https://sip.lex.pl/komentarze-i-publicacje/artykuly/ochrona-prywatnosci-i-wizerunku-osob-powszechnie-znanych-w-swietle-151083435> (dostęp: 2 III 2023); M. Safjan, K. Berwid-Wilińska, *Prawo do prywatności osób publicznych*, w: Biuro Generalnego Inspektora Danych Osobowych, *Ochrona danych osobowych...*, s. 373.

²⁴ W raporcie *The Advisory Council to Google on the Right to be forgotten* Google w celu wykonania wyroku TSUE z 13 V 2014 r. zobowiązał się do usuwania danych osobowych osób, które zgłaszają takie żądania, aczkolwiek Google odrzuca wnioski składane przez osoby, których działalność nosi znamiona pełnienia funkcji publicznych – zob. *The Advisory Council to Google on the Right to be Forgotten*, February 2015, <https://static.googleusercontent.com/media/archive.google.com/pl//advisorycouncil/advisement/advisory-report.pdf> (dostęp: 2 III 2023).

ochronę danych osobowych, ponieważ podkreśla znaczenie prawa do prywatności jako dobra osobistego przysługującego każdemu człowiekowi. Dobra osobiste, takie jak zdrowie, nazwisko, pseudonim czy wizerunek, chronione przepisami prawa cywilnego²⁵, na mocy rozporządzenia o ochronie danych osobowych uzyskały dodatkową ochronę prawną.

3. Prawo do bycia zapomnianym w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej

Zasadniczą rolę, z perspektywy prawa do bycia zapomnianym, odegrało w Unii orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Kompetencje Trybunału określa art. 19 Traktatu o Unii Europejskiej²⁶ w sposób, który daje Trybunałowi możliwość twórczej interpretacji prawa unijnego²⁷. Dzięki temu sędziowie luksemburscy zastosowali wykładnię postanowień dyrektywy 95/46/WE, na podstawie której przyznano obywatelom Unii prawo do bycia zapomnianym w Internecie²⁸ oraz zobowiązano operatorów wyszukiwarek internetowych, jako administratorów danych, do przestrzegania tego prawa.

Wątpliwości co do uznania wyszukiwarek internetowych za administratorów danych w świetle uprzednio obowiązującej dyrektywy 95/46/WE²⁹ były przedmiotem rozpatrywanej przez Trybunał sprawy *Google Spain i Google Inc. przeciwko Agencia Espanola de Protección de Datos (AEPD) i Mario Costeja González*³⁰. Hiszpański obywatel Mario Costeja González

²⁵ Zgodnie z art. 23 Ustawy z dnia 23 IV 1964 r. – Kodeks cywilny (Dz.U. 2018, poz. 1025).

²⁶ Traktat o funkcjonowaniu Unii Europejskiej, Dz.U. UE 26 X 2012, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:12012E/TXT&from=PL> (dostęp: 2 III 2023).

²⁷ T.T. Koncewicz, *Zasada jurysdykcji powierzonej Trybunału Sprawiedliwości Wspólnot Europejskich. O jurysdykcyjnych granicach i wyborach w dynamicznej „wspólnocie prawa”*, Warszawa 2009.

²⁸ Prawo do bycia zapomnianym zostało wyprowadzone z treści prawa do usunięcia i zablokowania danych (art. 12 dyrektywy 95/46/WE) oraz prawa sprzeciwu (art. 14 dyrektywy 95/46/WE).

²⁹ Dyrektywa 95/46/WE została zastąpiona w 2016 r. ogólnym rozporządzeniem o ochronie danych 2016/679.

³⁰ Wyrok TSUE z 13 V 2014 r. w sprawie C 131/12 *Google Spain i Google Inc. v. Agencia Espanola de Protección de Datos (AEPD) i Mario Costeja Gonzalez*, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=5478974> (dostęp: 2 III 2023).

w postępowaniu prejudycjalnym domagał się od Google usunięcia jego danych osobowych tak, aby po wpisaniu w wyszukiwarce internetowej jego imienia i nazwiska nie ukazywały się linki odsyłające do dwóch stron katalońskiego dziennika „La Vanguardia”, w treści których znajdowało się ogłoszenie informujące o licytacji nieruchomości skarżącego w związku z niespłaconymi przez niego należnościami na rzecz zakładu zabezpieczeń społecznych³¹. Swoje żądanie argumentował tym, że sprawa licytacji nieruchomości została dawno zakończona i nie ma aktualnie żadnego znaczenia³². Trybunał przychylił się do żądania skarżącego, a jednocześnie dokonał na tyle obszernej interpretacji pojęcia „administrator danych”, aby objąć jego zakresem operatorów wyszukiwarek internetowych, co w konsekwencji miało potwierdzić znaczenie aktywności Google w przetwarzaniu danych osobowych obywateli państw członkowskich UE³³.

W wyroku Trybunał Sprawiedliwości UE stwierdził też, że wyszukiwarki internetowe, przetwarzając dane osobowe, znacznie ułatwiają swoim użytkownikom pozyskiwanie informacji na temat życia prywatnego innych osób³⁴. Ponadto, tworzenie przez wyszukiwarkę internetową szczegółowego profilu konkretnej jednostki uzyskanego na podstawie porządkowania i łączenia w całość rozproszonych i niejednorodnych informacji opublikowanych w Internecie, może również okazać się zagrożeniem dla prywatności użytkowników sieci. Opieranie się na niewiarygodnych i niepełnych informacjach przy tworzeniu takich profili może też przyczynić się do naruszenia prawa tych osób do życia prywatnego czy rodzinnego³⁵.

Zakwalifikowanie przez Trybunał wyszukiwarki internetowej Google do katalogu administratorów danych spotkało się też z głosami krytycznymi. Przykładem może być opinia rzecznika generalnego N. Jääskinena, który stwierdził, że za administratora danych należałoby uznać jedynie wydawców źródłowych stron internetowych, posiadających należyte

³¹ Ibidem, pkt 14.

³² Ibidem, pkt 15.

³³ Por. M. Czerniawski, *Prawo do bycia zapomnianym w internecie. Glosa do wyroku TS z dnia 13 maja 2014 r. C-131/12*, LEX/el. 2015, <https://sip.lex.pl/komentarze-i-publicacje/glosy/prawo-do-bycia-zapomnianym-w-internecie-glosa-do-wyroku-ts-z-dnia-13-386107074> (dostęp: 2 III 2023).

³⁴ Ibidem.

³⁵ Wyrok TSUE z 13 V 2014 r. w sprawie C 131/12 *Google Spain i Google Inc. v. Agencia Espanola de Protección de Datos (AEPD) i Mario Costeja Gonzalez*, pkt 37.

uprawnienia do stosowania tzw. kodów wyłączenia znacznie ograniczających indeksowanie³⁶.

Wydaje się, że za zasadne należy uznać przyjęte przez Trybunał stanowisko, w którym operatorzy wyszukiwarek internetowych są traktowani jak administratorzy danych. Pozwala to, w celu zapewnienia jednostkom prawa do prywatności i ochrony danych osobowych w cyfrowej rzeczywistości, nałożyć na nich stosowne obowiązki. Warto też pamiętać, że wyrok prejudycjalny w sprawie *Google Spain* wywołuje skutki prawne nie tylko *inter partes*, lecz także skutki *erga omnes*, w konsekwencji czego ma zastosowanie wobec Google, a także wobec innych operatorów wyszukiwarek internetowych udostępniających swoje usługi obywatelom UE.

4. Ocena regulacji prawa do bycia zapomnianym

Aktualna regulacja prawa do bycia zapomnianym zawarta w art. 17 rozporządzenia 2016/679 budzi wątpliwości. Wskazuje się, że wykonywanie obowiązków związanych z zapewnieniem jego realizacji przez administratora wiąże się z dodatkowymi obciążeniami dla przedsiębiorców. Dodatkowo z uwagi na barierę technologiczną i społeczną³⁷ podważana jest skuteczność tak określonego uprawnienia³⁸. Ponadto sam jego kształt pozostaje kontrowersyjny w świetle fundamentalnych praw i wolności, w szczególności wolności wypowiedzi i dostępu do informacji.

W art. 17 rozporządzenia uprawnienie do bycia zapomnianym pozostaje niedookreślone – na przykład nie zostały wyznaczone procedury usuwania danych oraz informowania podmiotów trzecich o skorzystaniu przez podmiot uprawniony z tego żądania. Samo zobowiązanie administratora do usunięcia danych nie jest wystarczające. Taka redakcja

³⁶ Opinia rzecznika generalnego Niila Jääskinena przedstawiona 25 VI 2013 r. w sprawie C-131/12 *Google Spain i Google Inc. v. Agencia Española de Protección de Datos (AEPD) Mario Costeja González*, <https://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=pl> (dostęp: 2 III 2023).

³⁷ A.H. Stuart, *Google Search Results: Buried if Not Forgotten*, „North Carolina Journal of Law and Technology” 2014, nr 15(3), s. 465–517; R.H. Weber, *The Right to Be Forgotten: More Than a Pandora’s Box?*, „Journal of Intellectual Property, Information Technology and E-Commerce Law” 2011, nr 2, s. 122–123.

³⁸ M. Krzysztofek, „Prawo do bycia zapomnianym” i inne aspekty prywatności w epoce Internetu w prawie UE, „Europejski Przegląd Sądowy” 2012, nr 8, s. 33–34.

przepisu nastęcza sporo problemów interpretacyjnych. W orzecznictwie nie doszło do tej pory do pozytywnego określenia czynności, które mogłyby być adekwatne podczas usuwania skutków naruszenia. Ciężar udowodnienia faktu naruszenia oraz złożenia skonkretyzowanego żądania usunięcia danych spoczywa na osobie, której dane dotyczą. Z uwagi na brak ujednoczonych procedur, a także łatwość zwielokrotniania treści, bardziej skonkretyzowane ujęcie oświadczenia o woli skorzystania z prawa do bycia zapomnianym jest utrudnione.

Obowiązek poinformowania administratorów przetwarzających dane o żądaniu ich usunięcia powinien być miarkowany w zależności od możliwości technicznych i środków posiadanych przez zobowiązanego administratora. W ten sposób ustanowiony obowiązek okazuje się z jednej strony bardzo szeroko zakreślony i zdaje się wymagać znacznych nakładów, a z drugiej strony w związku z tym, że został wyznaczony w sposób nieostry, może okazać się niemożliwy do wyegzekwowania w praktyce.

Przede wszystkim pojawia się szereg problemów technicznych – skąd administrator ma wiedzieć, że dane przez niego udostępnione zostały skopiowane przez inny podmiot? Niedorzeczne wydaje się założenie, że aby zapewnić kontrolę nad danymi, powinien tak zmienić procedury, by kopiowanie danych każdorazowo wymagało jego zgody. Z uwagi na liczne sposoby powielania treści (na przykład kopiowanie przy użyciu urządzeń elektronicznych lub fotograficznych, ręczne przepisywanie treści) kontrola nad zwielokrotnianiem informacji wydaje się wysoce utrudniona, praktycznie niemożliwa. Z tego powodu taka wykładnia art. 17 ust. 2 rozporządzenia 2016/679 nie daje się pogodzić z założeniem racjonalności ustawodawcy.

Właściwe wydaje się przyjęcie, że administrator powinien poszukiwać pozostałych podmiotów, które przetwarzają dane. Jakie więc czynności musi podjąć, aby można było uznać, że dopełnił obowiązku określonego w art. 17 ust. 2 rozporządzenia? Zakres przedmiotowy obowiązku powinien być wyznaczony przy uwzględnieniu możliwości technologicznych, kosztów i postulatu proporcjonalności³⁹. Przy tym im bardziej dotkliwe mogą być skutki przetwarzania danych poza zakresem

³⁹ Art. 19 rozporządzenia 2016/679 stanowi, że administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

działalności administratora, tym bardziej rygorystyczne powinny być standardy staranności po jego stronie.

W tym miejscu warto byłoby zwrócić uwagę na treści umieszczane w Internecie, które dotyczą danych osobowych, często tych wrażliwych. Dostrzegalna jest pewna specyficzna cecha występowania określonej treści w nowoczesnym medium – korelacja pomiędzy popularnością treści a jej wzmożonym przetwarzaniem. W prawie polskim zwykło się przyjmować, że jeśli jakaś treść naruszająca dobro osoby była udostępniana w sposób umożliwiający jej dotarcie do nieoznaczonego kręgu osób, to czynności mające na celu doprowadzenie do zaprzestania naruszeń powinny również móc dotrzeć do nieograniczonego kręgu osób. Zgodnie z tym ujęciem, jeśli osoba, której dane zostały udostępnione na stronie internetowej, skorzystała z prawa do bycia zapomnianą, wiadomość o skorzystaniu przez nią z tego prawa również powinna się znaleźć na przedmiotowej stronie. Taki sposób realizacji ustawowego obowiązku z art. 17 ust. 2 rozporządzenia mógłby być uznany za wystarczający w świetle zasady proporcjonalności. W orzecznictwie wskazuje się, że dotyczy to kwestii **nieograniczonego kręgu osób**.

Zgodnie z tym „[...] wymóg złożenia m.in. w odpowiedniej formie oświadczenia oznacza zachowanie adekwatności z uwzględnieniem m.in. miejsca i czasu dokonanego naruszenia dobra osobistego, a nie jest warunkowany oceną prawdopodobieństwa i szansy dotarcia do oświadczenia przez przeciętnego jego adresata oraz jego czasu i skłonności do lektury informacji niedostatecznie wyeksponowanych, choć opublikowanych w tożsamym miejscu, w którym doszło do publikacji inkryminowanych tekstów”⁴⁰.

Takie rozumienie prawa do bycia zapomnianym wydaje się nie do końca właściwe. Wskazana powyżej wykładnia wynika głównie z braku zrozumienia specyfiki funkcjonowania medium, jakim jest Internet. Liczba osób, które mogły zapoznać się z materiałem zawierającym dane osobowe, jest – racjonalnie rzecz oceniając – nieporównywalna z liczbą osób, do których dotrze informacja o skorzystaniu z prawa do bycia zapomnianym przez osobę będącą podmiotem danych.

Implementacja prawa do bycia zapomnianym w UE była podyktowana przede wszystkim chęcią wzmocnienia gwarancji realizacji praw człowieka w świecie cyfrowym, gdyż mają one charakter uniwersalny, stąd też zasięg ich ochrony nie może obejmować jedynie sfery offline

⁴⁰ Wyrok Sądu Najwyższego z 19 V 2011 r., sygn. akt I CSK 497/10, LEX nr 936483.

(baz danych prowadzonych przez administratorów), lecz również sferę online. Nie da się jednak ukryć, że ochrona praw człowieka w Internecie stanowi wyzwanie dla unijnego systemu prawnego, chociażby w związku ze wzrostem popularności i funkcjonalności portali społecznościowych.

Podsumowanie

Harmonizacja przepisów związanych z ochroną danych osobowych związana jest przede wszystkim ze wzrostem przekazywania informacji przy użyciu środków komunikacji elektronicznej. Rejestrowanie czynności w systemach z informatyzowanych ma bowiem zastosowanie ze względu na kwestie nie tylko społeczne, lecz także administracyjne, gospodarcze czy finansowe. Dlatego tak wiele obowiązków nałożono na administratorów. Ich działania obejmują identyfikację rodzaju przetwarzanych informacji, określenie podstawy prawnej ich wykorzystywania, w tym polityki bezpieczeństwa i oceny jej skutków, a także maksymalizację uprawnień osoby fizycznej.

Rozporządzenie o ochronie danych osobowych w znacznej mierze poszerza katalog praw osób, których dane dotyczą, jednocześnie wskazując obowiązki administratorów, co w założeniach ma zapewnić kompleksową ochronę w zakresie gromadzenia oraz przetwarzania danych. Poza tym akt ten zauważa problem, jakim jest zarządzanie danymi w systemach teleinformatycznych. Działania ustawodawcy w tym zakresie skupiają się na wyeliminowaniu korzystania przez administratora z metod i narzędzi, których celem jest ciągłe gromadzenie oraz przetwarzanie danych na masową skalę, niekoniecznie w jasnym i wiadomym celu.

Zadania o charakterze informacyjnym, dotyczące udostępniania czy bezpieczeństwa danych osobowych, są ściśle związane z uprawnieniami osób, których dane dotyczą. Ogólne rozporządzenie unijne wskazuje przesłanki prawa do bycia zapomnianym. Prawo to zapewnia jednostce kontrolę nad przetwarzaniem jej danych osobowych, umożliwiając żądanie ich usunięcia. Z tego prawa wynika też ewentualność szybkiego reagowania na sytuacje zagrażające prawidłowemu przetwarzaniu informacji oraz analizy celowości dalszego posługiwania się danymi osobowymi.

Regulacja prawa do bycia zapomnianym nakłada na administratorów danych szereg obowiązków, których realizacja przy obecnym stanie

technicznym wydaje się wysoce utrudniona. Pozytywnie należy ocenić objęcie zakresem zastosowania normy administratorów danych, a także nałożenie na nich obowiązku poinformowania innych podmiotów przetwarzających te dane o żądaniu ich usunięcia. Wpływ regulacji na wykształconą praktykę gospodarczą może być ograniczony przez użycie pojęć nieostrych i odwołanie do pozaprawnych kryteriów delimitujących zakres obowiązku (koszty, możliwości technologiczne). Choć z perspektywy dorobku orzeczniczego uregulowanie prawa do bycia zapomnianym w rozporządzeniu należy ocenić pozytywnie, to jednak trzeba podkreślić, że praktyczne znaczenie regulacji będzie w przeważającej mierze zależało od postawy administratorów oraz przyjętej w orzecznictwie wykładni przepisów.

THE RIGHT TO BE FORGOTTEN FROM THE PERSPECTIVE OF PROCESSING PERSONAL DATA

Summary

Nowadays, effective protection of personal data is one of the fundamental issues of a democratic state under the rule of law. Therefore, the legislator should be very precise about the principles and standards of data processing. In the last few decades, in particular, the development of new technologies, digitalisation and the increase in the need for electronic communication has become evident, which leads to the adoption of appropriate regulations for the handling of personal data. In addition, the EU legislator has introduced the General Data Protection Regulation (GDPR) in order to harmonise the regulations of EU Member States regarding the protection of personal data. This provides a framework for the proper functioning of legal provisions across the European Union regarding the handling of personal data of its citizens.

The aim of the article is to identify the legal changes resulting from the Personal Data Protection Regulation, with a particular focus on the persons to which they apply and then to analyse the regulation of 'the right to be forgotten'. In the first part of the article, attention is drawn to the way personal data are processed and the scope of obligations incumbent on data controllers. This is because data controllers are, together with the personal data protection officer, responsible for recording data processing activities, including ongoing monitoring and responding to situations of inaccurate data processing. The second part focuses on the right to be forgotten and the assessment of this entitlement in the perspective of Regulation 2016/679. The research methods include an analysis of legal acts, at the same time using the subject literature.

Keywords: personal data processing – right to be forgotten – data protection

BIBLIOGRAFIA

- Banaszak B., Wygoda K., *Pojęcie funkcji publicznej jako przesłanka modyfikująca zakres ochrony danych osobowych*, w: Biuro Generalnego Inspektora Danych Osobowych, *Ochrona danych osobowych wczoraj, dziś, jutro. Personal data protection yesterday, today, tomorrow*, Warszawa 2006, s. 59–76.
- Czerniawski M., *Prawo do bycia zapomnianym w internecie. Glosa do wyroku TS z dnia 13 maja 2014 r. C-131/12*, <https://sip.lex.pl/komentarze-i-publikacje/glosy/prawo-do-bycia-zapomnianym-w-internecie-glosa-do-wyroku-ts-z-dnia-13-386107074> (dostęp: 2 III 2023).
- Czerniawski M., *Sprostowanie i usuwanie danych*, w: RODO – ogólne rozporządzenie o ochronie danych. Komentarz, pod red. E. Bielak-Jomaa, D. Lubasza, Warszawa 2018, s. 517–553.
- Ganczar M., *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009.
- Gonschior A., *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej*, w: *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego. Aspekty teoretyczne i praktyczne*, pod red. D. Kornobis-Romanowskiej, Wrocław 2017, s. 239–288.
- Jastrzębska K., *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*, Warszawa 2018.
- Keller D., *The new, worse 'right to be forgotten'*, Politico, 27 I 2016, <https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/> (dostęp: 2 III 2023).
- Koncewicz T.T., *Zasada jurysdykcji powierzonej Trybunału Sprawiedliwości Wspólnot Europejskich. O jurysdykcyjnych granicach i wyborach w dynamicznej „wspólnocie prawa”*, Warszawa 2009.
- Krasuski A., *Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy*, Warszawa 2012.
- Krasuski A., *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018.
- Krzysztofek M., *„Prawo do bycia zapomnianym” i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy” 2012, nr 8, s. 29–34.
- Lubasz D., *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów, praktyczne uwagi*, Warszawa 2018.
- Łuczak J., *Prawa osoby, której dane dotyczą*, w: RODO – ogólne rozporządzenie o ochronie danych. Komentarz, pod red. E. Bielak-Jomaa, D. Lubasza, Warszawa 2018, s. 464–584.
- Pryciak M., *Prawo do prywatności*, „Studia Erasmiana Wratislaviensia” 2010, nr 4, s. 211–229, <https://www.bibliotekacyfrowa.pl/Content/37379/011.pdf> (dostęp: 2 III 2023).
- Safjan M., Berwid-Wilińska K., *Prawo do prywatności osób publicznych*, w: Biuro Generalnego Inspektora Danych Osobowych, *Ochrona danych osobowych wczoraj, dziś, jutro. Personal data protection yesterday, today, tomorrow*, Warszawa 2006, s. 371–397.
- Sakowska-Baryła M., *Prawo do ochrony danych osobowych*, Wrocław 2015.

- Sieńczyło-Chlabicz J., *Ochrona prywatności i wizerunku osób powszechnie znanych w świetle orzeczenia Europejskiego Trybunału Praw Człowieka – von Hannover v. Niemcy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” 2007, nr 4, s. 399–416, <https://sip.lex.pl/komentarze-i-publicacje/artykuly/ochrona-prywatnosci-i-wizerunku-osob-powszechnie-znanych-w-swietle-151083435> (dostęp: 2 III 2023).
- Stuart A.H., *Google Search Results: Buried If Not Forgotten*, „North Carolina Journal of Law and Technology” 2014, nr 15(3), s. 463–517.
- The Advisory Council to Google on the Right to be Forgotten*, February 2015, <https://static.googleusercontent.com/media/archive.google.com/pl//advisorycouncil/advisement/advisory-report.pdf> (dostęp: 2 III 2023).
- Weber R.H., *The Right to Be Forgotten: More Than a Pandora’s Box?*, „Journal of Intellectual Property, Information Technology and E-Commerce Law” 2011, nr 2, s. 120–130.