

BEATA BARAN

UNIwersytet Jagielloński
Wydział Prawa i Administracji
Zakład Prawa Karnego Wykonawczego
E-MAIL: BEATA.BARAN@GMAIL.COM

KATARZYNA POŁUDNIAK-GIERZ

UNIwersytet Jagielloński
Wydział Prawa i Administracji
Katedra Prawa Cywilnego
E-MAIL: K.POLUDNIAK-GIERZ@DOCTORAL.UJ.EDU.PL

Perspektywa regulacji prawa do bycia „zapomnianym” w Internecie. Zarys problematyki

STRESZCZENIE

W dobie postępującej cyfryzacji oraz gromadzenia coraz większych zasobów danych istotną kwestią staje się ochrona prywatności użytkowników sieci Web przy jednoczesnym zagwarantowaniu należytej swobody wypowiedzi. W artykule przedłożona została problematyka podjęta w Rezolucji Rady Praw Człowieka Organizacji Narodów Zjednoczonych w sprawie promowania, ochrony i korzystania z praw człowieka w Internecie w kontekście poszanowania prawa do prywatności. Jednym z instrumentów, które mogą przyczynić się do realizacji powyższych celów, jest prawo do bycia zapomnianym. Przedstawiona została ewolucja koncepcji prawa do bycia zapomnianym w prawie Unii Europejskiej oraz orzecznictwie unijnym i krajowym. Analizie poddano regulację prawa do bycia zapomnianym zawartą w rozporządzeniu Parlamentu Europejskiego i Rady 2016/679. Na tej podstawie wskazane zostały główne wyzwania oraz ryzyka związane z wejściem w życie rozporządzenia.

SŁOWA KLUCZOWE

prawo do bycia zapomnianym, Internet, prawo do prywatności, ochrona danych osobowych

Potrzeba regulacji prawa do bycia „zapomnianym”

Zgodnie z prawem Unii Europejskiej¹ dane osobowe mogą być zbierane wyłącznie przy zachowaniu ściśle określonych warunków, w zgodnym z prawem celu. Ponadto podmioty, które zbierają dane osobowe i zarządzają nimi, zobowiązane są do tego, by nie dopuścić do ich bezprawnego wykorzystania oraz respektować prawa podmiotów, od których dane pochodzą bądź też których dotyczą. Kodyfikacja reguł dotyczących przetwarzania danych osobowych nie byłaby wystarczająca do realizacji celu regulacji, gdyby nie mechanizm pozwalający na usunięcie danych osobowych, które znalazły się w sieci wbrew woli osoby, której one dotyczą, a ich przetwarzanie nie jest dozwolone na podstawie norm szczególnych.

Informacja staje się walutą w Internecie². Rozwój środowiska internetowego i wzrost prędkości przepływu oraz ilości przetwarzanych danych sprawiają, że usunięcie czy skorygowanie informacji, która już znalazła się w sieci, jest znacząco utrudnione. Osoba umieszczająca treści w sieci³ nie jest w stanie kontrolować tego, co się z nimi stanie: nie może skutecznie uniemożliwić ich zwielokrotniania, wyszukiwania czy pozycjonowania.

Dostęp do strony internetowej zwykle nie jest ograniczony terytorialnie. Dane są przesyłane i pozyskiwane przez podmioty prywatne i publiczne ponad granicami państwowymi. Sprzeczne przepisy dotyczące ochrony danych w poszczególnych państwach członkowskich Unii Europejskiej utrudniają określenie granic prawa do prywatności oraz wolności wypowiedzi w przypadku informacji, które znalazły się w sieci.

Choć konkurencyjność zasad wolności wypowiedzi i prawa do prywatności nie jest w doktrynie prawa zjawiskiem nowym, rozwój technologii informacyjnej sprawia, że pojawiają się wciąż nowe dylematy związane z ochro-

¹ Lit. b, ust. 1, art. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (DzU UE L119/89, 4.05.2016).

² J. Ausloos, *The 'Right to be Forgotten' – Worth Remembering?*, "Computer Law & Security Review" 2012, No. 28 (2), s. 143–152.

³ Problem dotyczy informacji upublicznionych, ale także przesłanych za pośrednictwem sieci internetowej. Nawet jeśli informacja pojawi się na zastrzeżonym profilu, regulamin użytkownika narzędzia może zawierać postanowienia dotyczące możliwości użytkownika danych przez inny podmiot lub przejścia niektórych praw autorskich do danej treści.

ną istoty obu tych zasad⁴. Jednym z nich jest tak zwane prawo do bycia zapomnianym⁵.

W pierwszej części opracowania przedstawiono globalną perspektywę ochrony praw człowieka w świecie wirtualnym, z naciskiem na prezentację aktualnych tendencji normatywnych. Zaprezentowano kontekst, w ramach którego w systemie ONZ rodzą się mechanizmy i inicjatywy przyjmujące potrzebę regulacyjną prawa do bycia zapomnianym jako kolejnej gwarancji realizacji praw człowieka. W drugiej części pracy przedstawiony został dorobek orzecznictwa unijnego i krajowego, kluczowy w ocenie autorów z punktu widzenia kształtowania się koncepcji prawa do bycia zapomnianym. Podjęte inicjatywy, mające na celu ujednoczenie zasad dotyczących ochrony danych osobowych w ramach Unii Europejskiej, doprowadziły do uchwalenia dyrektywy (UE) 2016/680 oraz rozporządzenia (UE) 2016/679⁶, regulujących wyrażnie prawo do bycia zapomnianym. Konstrukcja ta została poddana ocenie w oparciu o *case study*. Poza zakresem prowadzonych badań pozostały geneza i aksjologia samego prawa do bycia zapomnianym.

Międzynarodowa ochrona praw człowieka w przestrzeni Internetu

Problematyka ochrony praw człowieka w Internecie stanowi zarazem konieczność i wyzwanie stojące przed systemami prawnymi XXI wieku. Zagadnienia te podnoszone są również w ramach zinstytucjonalizowanych działań Organizacji Narodów Zjednoczonych. Godna analizy pozostaje ewolucja podejścia ONZ do omawianych kwestii. Ochrona praw podstawowych, ze szczególnym uwzględnieniem prawa do prywatności, wolności wypowiedzi oraz prawa do nauki, stała się osią działań ONZ, które doprowadziły do

⁴ Potrzeba utworzenia jednolitych ram prawnych w Unii Europejskiej jest dostrzegana również wśród społeczeństw krajów unijnych. *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union*, s. 181, [online] http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf [dostęp: 13.08.2017].

⁵ Czym innym są prawo do zapomnienia (prawo do niepamięci) i prawo do bycia zapomnianym. Pierwsze z nich oznacza nieprzywoływanie danego historycznego wydarzenia z uwagi na upływ czasu od jego wystąpienia, drugie zaś odnosi się do prawa jednostki, by usunięto jej dane oraz zaprzestano ich przetwarzania, jeżeli przestały być potrzebne do zgodnych z prawem celów.

⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (DzU UE L 119/1 4.05.2016).

podjęcia rezolucji Zgromadzenia Ogólnego, wydania decyzji i publikacji raportów specjalnych Rady Praw Człowieka. W literaturze wskazuje się na wiodącą rolę państwa w obszarze przestrzegania, ochrony i realizacji praw człowieka⁷.

Pionierskim aktem okazała się rezolucja Rady Praw Człowieka z dnia 5 lipca 2012 roku⁸. Jest w niej wskazane wprost, iż prawa należne i chronione w świecie rzeczywistym powinny być także chronione *on-line*. W szczególności akcentowane jest tu swobodne korzystanie z wolności wypowiedzi oraz niezależność od granic administracyjnych, a także kanału komunikacji internetowej, z jednoczesnym poszanowaniem art. 19 Powszechnej Deklaracji Praw Człowieka oraz postanowień Międzynarodowego Paktu Praw Obywatelskich i Politycznych. Rezolucja wzywa wszystkie państwa do promocji oraz ułatwiania dostępu do Internetu przy jednoczesnej współpracy międzynarodowej ukierunkowanej na rozwój mediów i przepływ informacji⁹.

Kolejne akty prawne poświęcone ochronie praw człowieka w przestrzeni internetowej zostały wydane w formie rezolucji Rady Praw Człowieka w 2014¹⁰ oraz 2016 roku¹¹. Nowym aspektem ochrony, podniesionym w rezolucji z 2014 roku¹², była promocja dostępu do Internetu jako narzędzia wspierającego alfabetyzację cyfrową oraz dostęp do informacji. Państwa zostały także wezwane do rozwiązania problemów bezpieczeństwa oraz zapewnienia ochrony swobody wypowiedzi, wolności zgromadzeń, poszanowania prywatności i innych praw człowieka *on-line*. Postulowano powołanie państwowych, demokratycznych, transparentnych i działających w oparciu o zasadę praworządności instytucji, mogących zapewniać swobodę i bezpieczeństwo w sieci. Dzięki temu Internet mógłby stać się czynnikiem generującym rozwój gospodarczy, społeczny i kulturalny. Rezolucja wzywa państwa do stworzenia i przyjęcia – przy udziale partnerów społecznych i zastosowaniu transparentnych procedur krajowych – polityk publicznych zwią-

⁷ M. R. Bjarnadóttir, *Does the Internet Limit Human Rights Protection? The Case of Revenge Porn*, "JIPITEC" 2016, No. 7 (3), s. 204, [online] <https://www.jipitec.eu/issues/jipitec-7-3-2016/4509> [dostęp: 23.02.2017].

⁸ The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 29.06.2012, A/HRC/20/L.30.

⁹ Ibidem.

¹⁰ The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 20.06.2014, A/HRC/26/L.24.

¹¹ The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 27.06.2016, A/HRC/32/L.20.

¹² The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 20.06.2014, A/HRC/26/L.24.

zanych z Internetem, które potwierdzą globalny i otwarty charakter sieci Web. Ich podstawą winno być dążenie do realizacji praw człowieka, a celem – powszechny dostęp do zasobów sieciowych.

Rezolucja A/HRC/32/L.20 Rady Praw Człowieka ONZ¹³ w swoich tezach kładzie nacisk na walkę z wykluczeniem cyfrowym oraz zmniejszenie nierówności w dostępie do Internetu. W dokumencie potępiono podejmowanie jednoznacznych kroków ukierunkowanych na ograniczenie lub uniemożliwienie rozpowszechniania za pomocą Internetu informacji dotyczących naruszeń prawa człowieka. Wezwano państwa do powstrzymania się od takich działań lub ich zakończenia. Co istotne, w rezolucji położono nacisk na walkę z dyskryminacją oraz przemocą, a także promocję tolerancji i dialogu. Przeniesieniem na grunt praktyczny oraz weryfikacją zawartych w dokumencie tez będzie raport poświęcony sposobom niwelowania przepaści cyfrowej pomiędzy płciami z perspektywy praw człowieka¹⁴. Także Zgromadzenie Ogólne ONZ podjęło relewantne uchwały dotyczące ochrony praw podstawowych w erze cyfrowej, w szczególności zaś prawa do prywatności¹⁵.

Istnieje zgodność co do tego, iż w cyberprzestrzeni mają być chronione prawa człowieka, które gwarantowane są obecnie *off-line*. Teza ta została przyjęta nie tylko przez agendy Organizacji Narodów Zjednoczonych, ale również przez podmioty znajdujące się w otoczeniu społeczno-gospodarczym (na przykład podmioty działające w branży IT oraz organizacje pozarządowe). Takie wnioski zostały przedstawione w dokumencie podsumującym The Global Multistakeholder Meeting on the Future of Internet Governance, odbywający się w Sao Paulo w kwietniu 2014 roku¹⁶. Spotkanie to stanowiło forum debaty pomiędzy przedstawicielami poszczególnych państw, międzynarodowej społeczności internautów, Międzynarodowego Związku Telekomunikacyjnego, Departamentu ds. Społecznych i Ekonomicznych, Sekre-

¹³ The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 27.06.2016, A/HRC/32/L.20.

¹⁴ *Report of the Office of the United Nations High Commissioner for Human Rights on ways to bridge the gender digital divide from a human rights perspective*, [online] <http://www.ohchr.org/EN/Issues/Women/WRGS/Pages/WaystoBridgetheGenderDigital.aspx> [dostęp: 9.02.2017].

¹⁵ Por. General Assembly Resolution 68/167 on the right to privacy in the digital age, 18.12.2013; General Assembly Resolution 69/166 on the right to privacy in the digital age, 18.12.2014; General Assembly Resolution 71/199 on the right to privacy in the digital age, 16.11.2016.

¹⁶ *NETmundial Multistakeholder Statement*, Sao Paulo 2014, s. 4, [online] <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf> [dostęp: 9.02.2017].

tariatu ONZ oraz Komisji Europejskiej. Po raz pierwszy opracowano dokument *soft law* dotyczący zasad ładu internetowego¹⁷. Na pierwszym planie znalazły się kwestie dotyczące poszanowania i ochrony praw człowieka w oparciu o wspólne i podstawowe wartości prezentowane w Powszechnej Deklaracji Praw Człowieka. Wiodącą tezę zawartą w dokumencie podsumowującym jest teza o uniwersalności praw człowieka. Obowiązują one w porządku internetowym oraz są podstawą ładu internetowego. Wskazano, iż ochronę praw przynależnych *off-line* należy przenieść także na grunt rzeczywistości *on-line* zgodnie z wynikającymi z Międzynarodowych Paktów Praw Człowieka zobowiązaniami.

W ramach ochrony praw człowieka w przestrzeni internetowej na pierwszy plan wysuwa się gwarancja poszanowania dwóch kwestii szczególnie narażonych na naruszenia i silnie z sobą związanych: prawa do wolności wypowiedzi oraz prawa do prywatności. Zarówno wolność wypowiedzi, jak i prawo do prywatności w kontekście działań w sieci uznawane są za należące do tak zwanej kategorii praw cyfrowych (*digital rights*)¹⁸.

Prawo do bycia zapomnianym – zarys kontekstu

Konieczność wdrożenia mechanizmów ochrony prawa do prywatności wymuszona przez rozwój technologiczny została zauważona już w 1890 roku¹⁹. Wiek XX i początek wieku XXI, niosąc z sobą gwałtowny rozwój technologii informacyjnej, usunęły bariery techniczne i instytucjonalne w rozpowszechnianiu oraz odbiorze informacji, umożliwiając natychmiastowe i trwałe udostępnianie wszelkich treści w formacie cyfrowym niemal nieograniczonej liczbie podmiotów. Widoczna stała się potrzeba ochrony osób, których dane osobowe znalazły się w sieci Web i ulegają trwałemu upublicznieniu wbrew ich woli. Jednym z mechanizmów ochronnych miało być prawo do bycia zapomnianym.

Z uwagi na budowę sieci internetowej problem w praktyce obejmował trzy kwestie:

¹⁷ Ibidem.

¹⁸ W. H. Dutton, A. Dopatka, G. Law, V. Nash, *Freedom of Connection, Freedom of Expression, UNESCO Series on Internet Freedom*, [online] <http://unesdoc.unesco.org/images/0019/001915/191594e.pdf> [dostęp: 13.08.2017].

¹⁹ S. D. Warren, L. D. Brandeis, *The Right to Privacy*, "Harvard Law Review" 1890, No. 4, s. 195.

- I. publikowanie elementów danych osobowych na jakiegokolwiek stronie www w Internecie (strona źródłowa),
- II. przedstawianie przez wyszukiwarkę internetową wyników wyszukiwania, które kierują użytkownika Internetu do źródłowej strony internetowej,
- III. automatyczne przesyłanie do dostawcy usług wyszukiwania danych osobowych wyszukującego.

Kształtowanie się prawa do bycia zapomnianym w prawie unijnym²⁰

Dotychczas kwestie dotyczące prawa do bycia zapomnianym były regulowane przez dyrektywę 95/46/WE²¹, implementowaną do polskiego porządku prawnego ustawą o ochronie danych osobowych²². Zgodnie z art. 32 ust. 1 pkt 6 ustawy każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane, jak również (pkt 7) żądania zaprzestania przetwarzania danych ze względu na jej szczególną sytuację.

W dyrektywie, a następnie w prawie krajowym zabrakło jednoznacznego wskazania, czy owo roszczenie o uzupełnienie, uaktualnienie, sprostowanie czy usunięcie danych może być kierowane wyłącznie do podmiotu odpowiedzialnego za stronę źródłową, czy również do podmiotu odpowiedzialnego za narzędzie wyszukiujące. Wątpliwości może też budzić zakres informacji, które zostały objęte ochroną. Chronione są dane osobowe rozumiane jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej²³. Tymczasem informacje o użytkowniku sieci

²⁰ O kształtowaniu się koncepcji prawa do bycia zapomnianym zob. J. Żak, *Koncepcja „prawa do bycia zapomnianym”*, [w:] *Aktualne wyzwania ochrony wolności i praw jednostki*, red. M. Jabłoński, S. Jarosz-Żukowska, Wrocław 2014, passim.

²¹ 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 (DzU UE L z dnia 23 listopada 1995 r.).

²² Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 1997, nr 133, poz. 883 ze zm.).

²³ Termin „dane osobowe” użyty w art. 3 ust. 1 dyrektywy 95/46 został zdefiniowany w art. 2 lit. a) tej dyrektywy.

zbierane przez inne podmioty nie zawsze stanowią dane osobowe – istnieją także dane, na podstawie których można wnioskować o sytuacji, cechach, potrzebach i zainteresowaniach osoby lub grupy osób (na przykład korzystających z danego komputera), nie muszą one jednak pozwalać na zidentyfikowanie konkretnej osoby i odkrycie jej tożsamości. Tym samym wydaje się, że poza zastosowaniem regulacji mogą się znaleźć mechanizmy zbierające dane oparte na profilowaniu grupowym.

Ocena możliwości powołania się przez osobę, której dane osobowe zostały opublikowane na stronie www, na ochronę gwarantowaną przez dyrektywę 95/46/WE nie nastęrczała trudności. Trybunał już w wyroku w sprawie Lindqvist wskazał, że „przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany”²⁴ w rozumieniu art. 3 ust. 1 dyrektywy 95/46 obejmuje „każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych”²⁵, jako przykłady wskazując ich ujawnianie poprzez transmisję i rozpowszechnianie lub udostępnianie w inny sposób. Umieszczenie na stronie internetowej danych osobowych, pozwalające na dostęp do nich nieoznaczonej liczbie osób, jest wystarczające do realizacji przesłanki przetwarzania. Wątpliwy pozostaje natomiast automatyzm tegoż przetwarzania, gdyż dane muszą zostać wpisane lub załadowane na stronę źródłową przez osobę. Jednak nawet w takim przypadku, według aktualnie stosowanych procedur technicznych i informatycznych, czynności niezautomatyzowane użytkownika sieci będą połączone z procesami zautomatyzowanymi – załadowaniem strony źródłowej na serwer oraz przeprowadzeniem operacji, które uczynią tę stronę dostępną dla osób mających połączenie z Internetem. Tym samym umieszczenie na stronie www danych osobowych podmiotu będzie oceniane ze względu na zgodność z przepisami dyrektywy.

Usunięcie danych ze strony źródłowej nie jest wystarczające ze względu na realizację celu dyrektywy. Informacja, która znalazła się w sieci, może być dowolnie kopiowana i przenoszona na inne strony źródłowe. Stąd też, w celu zapewnienia ochrony prywatności, zasadne byłoby zablokowanie możliwości zlokalizowania tych danych przez serwis wyszukiwający. Czy zatem osoba, której dane osobowe znalazły się w Internecie, może domagać się, aby wyszukiwarka internetowa nie wyświetlała wyników wyszukiwa-

²⁴ Wyrok Trybunału Sprawiedliwości UE w sprawie Lindqvist z dnia 6 listopada 2003 r., C101/01, pkt 25, [online] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&page=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1361686> [dostęp: 15.10.2016].

²⁵ Ibidem.

nia, które mogłyby kierować użytkownika Internetu do stron źródłowych, na których umieszczone zostały te dane? Dla kształtowania się prawa do bycia zapomnianym kluczowy jest wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google przeciwko AEPD²⁶.

Funkcjonowanie wyszukiwarki polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w sieci przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie ich udostępnianiu internautom w sposób uporządkowany zgodnie z określonymi preferencjami. Czy w sytuacji, gdy takie informacje zawierają dane osobowe osób trzecich, należy uznać opisaną powyżej działalność za „przetwarzanie danych” w rozumieniu definicji zawartej w art. 2 lit. b) dyrektywy 95/46? Czy osoba, domagając się ochrony w świetle dyrektywy 95/46, może zażądać bezpośrednio od przedsiębiorstwa prowadzącego wyszukiwarkę, by usunięto z jej indeksów informacje opublikowane przez osoby trzecie, bez uprzedniego lub jednoczesnego zwrócenia się z takim żądaniem do podmiotu będącego właścicielem (edytora) strony internetowej, na której zamieszczona została informacja?

Po pierwsze, należy rozważyć, czy działalność wyszukiwarki internetowej jest „przetwarzaniem danych osobowych” w rozumieniu dyrektywy. Operator wyszukiwarki internetowej, przeszukując Internet w zautomatyzowany, stały i systematyczny sposób w poszukiwaniu opublikowanych w nim informacji, gromadzi dane²⁷, które są następnie przez niego odzyskiwane, zapisywane i porządkowane za pomocą oprogramowania indeksującego. Operator wyszukiwarki przechowuje te informacje na swych serwerach oraz w odpowiednim przypadku ujawnia je i udostępnia użytkownikom w postaci listy wyników wyszukiwania, co w ocenie Trybunału realizuje przesłankę „przetwarzanie”. Fakt, że dane już zostały opublikowane przez inny podmiot, nie zmienia ich charakteru i nie stanowi podstawy do wyłączenia tych danych spod zakresu zastosowania dyrektywy²⁸. Podobnie irre-

²⁶ Wyrok TSUE w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González z dnia 13 maja 2014 r., C131/12, [online] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1353218> [dostęp: 15.10.2016].

²⁷ Brak dyferencjacji pomiędzy danymi osobowymi i danymi innego typu. Klasyfikacja danych ze względu na treść nie ma znaczenia dla funkcjonowania algorytmów wyszukiwania.

²⁸ Wyrok Trybunału Sprawiedliwości w sprawie Satakunnan Markkinapörssi i Sata-media z dnia 16 grudnia 2008 r., C73/07, pkt 48, 49, [online] <http://curia.europa.eu/juris/liste.jsf?language=pl&num=C-73/07> [dostęp: 16.10.2016].

lewantna jest okoliczność, że dane nie ulegają przekształceniu – pojęcie przetwarzania danych ani nie jest równoznaczne z ich modyfikowaniem, ani nie zakłada modyfikacji danych jako jednego z elementów koniecznych przetwarzania.

Okoliczność, że przedsiębiorstwo prowadzące wyszukiwarkę, posiłkując się zautomatyzowanymi narzędziami informatycznymi, nie posiada wiedzy o treści przetwarzanych danych i nie sprawuje nad nimi kontroli, jest irrelewantna w kontekście uznania przedsiębiorstwa za administratora danych w rozumieniu ustawy²⁹. Tylko przyjęcie szerokiej definicji pojęcia „administrator” umożliwia zapewnienie skutecznej i pełnej ochrony osobom, których dotyczą dane.

Ocena możliwości skutecznego żądania od operatora wyszukiwarki usunięcia danych przez osobę, której owe dane dotyczą, uzależniona jest od charakteru tychże danych.

Trybunał orzekł, że operator wyszukiwarki internetowej jest zobowiązany do usunięcia z wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby oraz linków do publikowanych przez osoby trzecie stron internetowych zawierających informacje dotyczące tej osoby, również w przypadku, gdy imię lub nazwisko czy inne dane nie zostały uprzednio czy jednocześnie usunięte z tych stron internetowych i – w odpowiednim przypadku – nawet jeśli ich publikacja na tych stronach jest zgodna z prawem.

Jest to uzasadnione ze względu na fakt, że przetwarzanie danych osobowych dokonywane przez operatora wyszukiwarki internetowej może znacząco oddziaływać na prawa podstawowe osoby – w szczególności prawo do poszanowania prywatności i ochrony danych osobowych. Jeśli hasłem wyszukiwanym jest imię i nazwisko, przeszukiwanie zasobów internetowych umożliwia wszystkim internautom otrzymanie ustrukturyzowanego przeglądu informacji dotyczących danej osoby i rozmaitych aspektów jej życia prywatnego. Zgromadzenie takich informacji za pośrednictwem innych narzędzi byłoby znacząco utrudnione lub w ogóle niemożliwe. „Ponadto skutki tej ingerencji w prawa osoby, której dane dotyczą, zostają zwielokrotnione ze względu na istotną rolę, jaką odgrywają Internet i wyszukiwarki internetowe we współczesnym społeczeństwie, nadając zawartej na takiej liście informacji wszechobecny charakter”³⁰.

²⁹ Wyrok w sprawie C131/12, pkt 34. Podobnie wyrok Trybunału Sprawiedliwości w sprawie eDate Advertising i in. z dnia 25 października 2011 r., C509/09 i C161/10, pkt 45.

³⁰ Ibidem, pkt 80.

W przypadku żądania usunięcia innych danych niż imię i nazwisko czy numer PESEL – na przykład miejsca zamieszkania, numeru IP, numeru telefonu, adresu e-mail czy innych informacji, które obecnie nie są postrzegane jako dane osobowe, bowiem nie wystarczają do identyfikacji osoby – wskazane byłoby podejście *ad casu*. Czy w danym stanie faktycznym konkretny zbiór informacji może umożliwiać identyfikację osoby? Wraz z postępem technologicznym i wzrostem skuteczności mechanizmów wyszukiwujących kategoria danych osobowych będzie się rozszerzać.

Obowiązujący stan prawny ulegnie zmianie wraz z wejściem w życie rozporządzenia (UE) 2016/679 oraz implementacją dyrektywy (UE) 2016/680 w maju 2018 roku³¹. Celem nowych aktów ma być dostosowanie regulacji poświęconych ochronie danych osobowych do realiów technologicznych i potrzeb społeczeństwa informacyjnego. Zakresem przedmiotowym dyrektywy 2016/680 objęta zostanie ochrona osób w związku z przetwarzaniem danych osobowych na potrzeby zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych.

Prawo do bycia zapomnianym zostało *explicite* określone w rozporządzeniu 2016/679³². W motywach rozporządzenia zarysowane zostały trzy główne kwestie, związane z funkcjonowaniem prawa do bycia zapomnianym w społeczeństwie informacyjnym. Jeśli osoba udzielająca zgody na przetwarzanie danych nie była w pełni świadoma ryzyka z nim związanego, powinna być uprawniona do cofnięcia tej zgody i domagania się, by usunięto zamieszczone informacje (kazu zgody udzielonej przez dziecko na przetwarzanie jego danych osobowych). W ocenie ustawodawcy łatwość zwielokrotniania raz upublicznionej informacji sprawia, że prawo do żądania usunięcia danych przez ich administratora jest niewystarczające dla ochrony osoby, której one dotyczą. Stąd też prawodawca rozszerzył prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił owe dane, do poinformowania administratorów, którzy je przetwarzają, o usunięciu wszelkich łączy do nich, kopii tych danych osobowych lub ich replikacji³³.

Równocześnie, z uwagi na ryzyko wycieku danych osobowych przetwarzanych zgodnie z obowiązującymi przepisami, podmioty administrujące danymi powinny być zobowiązane do zabezpieczenia praw i wolności osoby, której przetwarzane dane dotyczą. Przykładowo powinny zostać wdrożone

³¹ Wejście w życie rozporządzenia nastąpi 24 maja 2018 roku. Państwa członkowskie są zobowiązane do implementacji dyrektywy w terminie do 6 maja 2018 roku.

³² Motywy 65, 66, 156 oraz artykuł 17 rozporządzenia 2016/679.

³³ Granice obowiązku wyznaczają dostępne administratorowi technologie i środki.

środki techniczne i organizacyjne zapewniające poszanowanie zasady minimalizacji danych³⁴. Zauważona została potrzeba wagi ryzyka naruszenia³⁵. W przypadku zawodności mechanizmów ochronnych lub niespektowania przepisów prawa krajowego lub unijnego ustawodawca przyznaje osobie, której dane dotyczą, uprawnienie do żądania niezwłocznego usunięcia dotyczących jej danych osobowych, zwane powszechnie prawem do bycia zapomnianym.

Osoba może domagać się od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, jeśli:

- a) dane nie są już niezbędne do celów, dla których zostały zebrane,
- b) osoba, której dane dotyczą, cofnęła zgodę lub wniosła sprzeciw³⁶,
- c) dane te były przetwarzane niezgodnie z prawem,
- d) usunięcie tych danych wynika z obowiązku prawnego,
- e) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Jeżeli administrator upublicznił dane osobowe, to zobowiązany jest poinformować przetwarzających je administratorów, że osoba, której one dotyczą, żąda usunięcia: wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji.

Ocena regulacji w oparciu o *case study*

Obecnie 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.

³⁴ W myśl motywu 53 dyrektywy 2016/680 ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych. Wdrożenie takich środków nie powinno zależeć wyłącznie od względów gospodarczych. Aby móc wykazać przestrzeganie przepisów niniejszej dyrektywy, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz zasadą domyślnej ochrony danych.

³⁵ Zgodnie z motywem 52 dyrektywy 2016/680 prawdopodobieństwo i wagę ryzyka naruszenia należy określić poprzez uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy operacje przetwarzania danych niosą poważne zagrożenie.

³⁶ Art. 21 ust. 2 rozporządzenia 2016/679.

niami dla przedsiębiorców. Dodatkowo, z uwagi na barierę technologiczną³⁷ i społeczną³⁸, podważana jest skuteczność tak określonego uprawnienia³⁹. Ponadto, sam jego kształt pozostaje kontrowersyjny w świetle fundamentalnych praw i wolności, w szczególności wolności wypowiedzi i dostępu do informacji.

Artykuł 17 rozporządzenia 2016/679 pozostawia uprawnienie do bycia zapomnianym niedookreślone – na przykład nie zostały wyznaczone procedury usuwania danych oraz informowania podmiotów trzecich o skorzystaniu przez podmiot danych z prawa do bycia zapomnianym. Jak dalece może to utrudniać skorzystanie z prawa do bycia zapomnianym, obrazuje kazuś osoby, która zgłosiła na policję pożar „sterty siana”. Nagranie tego – specyficznego w formie i treści – zgłoszenia, w którym pojawiają się pełne dane personalne i adresowe kobiety, trafiło do satyrycznych serwisów internetowych, szybko stając się „virałem”. Powódka, której dobra osobiste w postaci dobrego imienia, godności, czci, prawa do prywatności, poszanowania jej kalectwa i wolności od drwin i szykan zostały naruszone wskutek ujawnienia i rozpowszechniania nagrania, żądała jego usunięcia z portali internetowych.

W toku postępowania sądowego wyraźnie ujawniły się główne problemy związane z dochodzeniem usunięcia treści umieszczonych w sieci internetowej na podstawie art. 24 k.c.⁴⁰ Dotyczyły one: precyzyjności żądania pozwu oraz precyzyjności i samodzielności rozstrzygnięcia o tym żądaniu; redakcji sentencji wyroku w sposób wykluczający jej konkretyzację przez którąkolwiek ze stron; zasadności uznania zachowań osób trzecich, niekontrolowanych przez osobę pozwaną, za skutek naruszenia dobra przez tę ostatnią; określenia czynności, których dopełnienia może domagać się powód w granicach środków zmierzających do usunięcia skutków naruszenia w rozumieniu art. 24 k.c. oraz wyjątku od odpowiedzialności cywilnoprawnej podmiotów pośredniczących w udostępnianiu treści w ramach art. 12–15 u.ś.u.d.e.

W pierwszej kolejności uwidoczniła się konieczność precyzyjnego określenia żądania oraz redagowania sentencji wyroku w sposób kategori-

³⁷ A. H. Stuart, *Google Search Results: Buried if Not Forgotten*, „North Carolina Journal of Law and Technology” 2012, No. 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 Electronic Commerce Law” 2011, No. 2, s. 122.

³⁸ Ibidem, s. 122–123.

³⁹ 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.

³⁹ Wyrok Sądu Najwyższego z dnia 15.01.2015 r., sygn. akt II CSK 747/13.

wykluczający pozostawienie jej konkretyzacji którejkolwiek ze stron⁴¹. Zobowiązanie strony do podjęcia czynności mających na celu usunięcie danych z portali internetowych, w tym w szczególności zwrócenie się z odpowiednim żądaniem do właścicieli lub administratorów portali, nie czyni za- dość tym wymaganiom⁴². W orzecznictwie nie doszło do pozytywnego okre- ślenia czynności, które mogłyby być adekwatne w celu usunięcia skutków naruszenia dobra osobistego w Internecie. Ciężar precyzyjnego sformu- łowania żądania, wystarczająco konkretnego, by możliwa była jego realizacja, spoczywa na osobie zamierzającej skorzystać z uprawnienia do bycia za- pomnianą. Z uwagi na brak ujednoczonych procedur, a także łatwość zwie- lokrotniania treści, bardziej skonkretyzowane ujęcie oświadczenia o woli skorzystania z prawa do bycia zapomnianym jest utrudnione. W świetle art. 17 rozporządzenia 2016/679 ów brak regulacji procedury usuwania danych może okazać się determinantą przesądzającą o niskiej użyteczności prak- tycznej uprawnienia.

We wspomnianej sprawie rozważania Sądu Najwyższego objęły także kwe- stię zasadności uznania zachowań osób trzecich, niekontrolowanych przez osobę pozwaną, za skutek naruszenia dobra przez pozwaną w rozumieniu art. 24 k.c. Dostępność treści naruszającej dobra osobiste skarżącej nie jest wyłącznie następstwem bezprawnych działań strony pozwanej, ale również zachowań niekontrolowanych przez nią osób trzecich, które uzyskały do- stęp do treści wskutek jej pierwotnego ujawnienia. Czy te dalsze naruszenia dobra osobistego przez inne podmioty stanowią skutek naruszenia pierwot- nego? Sąd Najwyższy w wyroku o sygn. akt II CSK 747/13 przyjął, że nie można uznać zachowań anonimowych osób trzecich, korzystających z usług internetowych, za „skutek naruszenia” w rozumieniu art. 24 k.c. Przyjęty mo- del rozumowania, choć prawidłowy w świetle zasad przypisania, prowadzi do wniosku, że żądanie podjęcia czynności mających na celu usunięcie tre- ści z portali internetowych, na których nagranie zostało umieszczone, nie mieści się w granicach środków zmierzających do usunięcia skutków naru- szenia w rozumieniu art. 24 k.c.

Dopuszczalne jest natomiast domaganie się, by zobowiązać pozwanego do zawiadomienia określonych podmiotów zarządzających portalami inter- netowymi, że znajduje się na nich treść, która prawomocnym wyrokiem sądu została uznana za naruszającą dobra osobiste, a tym samym bezprawną. Po-

⁴¹ Wyrok Sądu Najwyższego z dnia 19.01.1982 r., sygn. akt IV CR 500/01, OSNCP 1982, nr 8–9, poz. 123; uchwała siedmiu sędziów Sądu Najwyższego z dnia 20.09.1988 r., sygn. akt III CZP 37/88, OSNCP 1989, nr 3, poz. 40.

⁴² Wyrok Sądu Najwyższego z dnia 15.01.2015 r., sygn. akt II CSK 747/13, *passim*.

wiadomienie to wyłączać będzie możliwość powoływania się przez usługodawcę (podmiot zarządzający portalem internetowym) na ograniczenie odpowiedzialności wynikające z art. 14 ust. 1 u.ś.u.d.e., jeśli nie uniemożliwi niezwłocznie dostępu do tych danych. Podobne rozwiązanie zostało przyjęte w rozporządzeniu 2016/679, przy czym z orzeczenia Sądu Najwyższego wynika, że to osoba dochodząca usunięcia treści ma wskazać portale, które powinny zostać powiadomione o tym, że znajduje się na nich dana informacja, natomiast ustawodawca unijny w ust. 2 art. 17 rozporządzenia 2016/679 obowiązkiem identyfikacji administratorów przetwarzających treści obarczył administratora, do którego zostało skierowane żądanie usunięcia treści w pierwszej kolejności.

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

Przed wszystkim pojawia się szereg problemów technicznych – skąd administrator ma wiedzieć, że dane przez niego udostępnione zostały skopiowane przez inny podmiot? *Ad absurdum*, czy aby zapewnić kontrolę nad danymi, powinien zmienić procedury, tak by kopiowanie danych każdorazowo wymagało jego zgody? Z uwagi na wielość sposobów powielania treści (od kopiowania przy użyciu narzędzi elektronicznych, przez użycie narzędzi zewnętrznych, na przykład aparatu fotograficznego i czytnika pozwalającego na konwertowanie zdjęć, po ręczne „przepisywanie” treści) kontrola nad zwielokrotnianiem informacji wydaje się wysoce utrudniona, praktycznie niemożliwa. Z tej przyczyny taka wykładnia ust. 2 art. 17 rozporządzenia 2016/679 nie daje się pogodzić z założeniem racjonalności ustawodawcy.

Czy zatem obowiązek administratora obejmuje tylko poinformowanie podmiotów, którym udzielił on zgody na skopiowanie danych? Wówczas znaczenie tego obowiązku byłoby znikome. Należałoby go traktować raczej jako konstrukcję propagującą pożądaną przez ustawodawcę model.

Bardziej racjonalne wydaje się przyjęcie, że administrator powinien poszukiwać kopiujących. Jakich czynności będzie musiał dopełnić, aby można było uznać, że pomimo nieznalesienia podmiotów, które przetwarzają dane pobrane z jego strony, wykonał obowiązek określony w art. 17 ust. 2 rozporządzenia 2016/679? Zakres przedmiotowego obowiązku powinien być wy-

znaczony przy uwzględnieniu możliwości technologicznych, kosztów i postulatu proporcjonalności⁴³. W zależności od rodzaju danych osobowych dopuszczalne wydaje się różnicowanie poziomu ich ochrony i wymaganej aktywności administratora. Im bardziej dotkliwe mogą być skutki przetwarzania danych poza systemem administratora, tym wyższe powinny być standardy należytej staranności i aktywności.

W tym kontekście warto zauważyć także pewną specyficzną cechę występowania określonej treści w Internecie – korelację 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 znaleźć się na przedmiotowej stronie. Taki sposób realizacji ustawowego obowiązku mógłby być uznany za wystarczający w świetle zasady proporcjonalności. W orzecznictwie wskazuje się, że

[...] 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 tekstów⁴⁴.

Jednakże taka wykładnia wynika z braku zrozumienia specyfiki funkcjonowania medium. Liczba osób, które mogły zapoznać się z materiałem zawierającym dane osobowe, który stał się „virałem”, a liczba osób, do których, racjonalnie rzecz oceniając, dotrze informacja o skorzystaniu z prawa do bycia zapomnianą przez osobę będącą podmiotem danych, jest nieporównywalna.

Kolejnym problemem związanym ze skorzystaniem z prawa do bycia zapomnianym (obecnie – w myśl art. 32 ust. 6–8 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych – do kontroli przetwarzania da-

⁴³ 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.

⁴⁴ Wyrok Sądu Najwyższego z dnia 19 maja 2011 r., sygn. akt I CSK 497/10, LEX nr 936483.

nych osobowych) są kwestie proceduralne. W zależności od statusu administratora danych czynności, o których mowa w art. 32 u.o.d.o., można traktować jako czynności faktyczne lub – jeśli pochodzą od organu administracji publicznej – wydanie zaświadczenia potwierdzającego określone fakty w rozumieniu przepisów kodeksu postępowania administracyjnego (art. 217 i n. k.p.a.). Będzie to skutkowało zróżnicowaniem sytuacji prawnej osoby zainteresowanej w zależności od statusu administratora danych. Stąd też przyjmuje się⁴⁵, że oznaczone sprawy związane z ochroną danych osobowych powinny być rozstrzygane przez Generalnego Inspektora Danych Osobowych (por. art. 18 i 35 u.o.d.o.). Na wniosek zainteresowanego to Generalny Inspektor, w drodze decyzji administracyjnej, będzie mógł nakazać uzupełnienie, uaktualnienie, sprostowanie danych osobowych, ich usunięcie, a także czasowe lub stałe wstrzymanie przetwarzania. Dopuszczalne⁴⁶ jest także żądanie korekty danych, ich usunięcia czy wstrzymania przetwarzania w drodze postępowania cywilnego, w ramach roszczeń przewidzianych w art. 24 k.c.⁴⁷

Nierozwiązane zostają także niektóre kwestie dotyczące zakresu zastosowania przedmiotowego uprawnienia. Wątpliwe jest, czy przyjęte regulacje pozwalają na objęcie zakresem zastosowania rozporządzenia 2016/679 portali społecznościowych typu Facebook⁴⁸. Trzeba przyznać, że na gruncie polskim prawo do kontroli przetwarzania danych osobowych zostało określone dość wąsko, a mianowicie przysługuje jedynie osobom, których dane są przetwarzane w ramach zbioru danych. Uzależnienie przyznania uprawnień od faktu przetwarzania danych w zbiorze zostało poddane krytyce⁴⁹ – rozwiązanie takie nie pokrywa się z przepisami dyrektywy 95/46/WE (por.

⁴⁵ J. Barta, P. Fajgielski, R. Markiewicz, art. 32, pkt 10, [w:] *Ochrona danych osobowych. Komentarz*, red. J. Barta, P. Fajgielski, R. Markiewicz, LEX 2015; Wyrok Naczelnego Sądu Administracyjnego z dnia 19 kwietnia 2000 r., sygn. akt II SA 2619/99, „Wokanda” 2000, nr 7, poz. 43.

⁴⁶ Eidem, art. 32, pkt 11, [w:] *Ochrona danych osobowych...*, op. cit.

⁴⁷ Odmiennie: Sąd Apelacyjny w Poznaniu w wyroku z dnia 13 listopada 2001 r., sygn. akt I ACa 1140/01, „Wokanda” 2002, nr 11, poz. 46. Naruszenie sfery prywatności skutkuje odpowiedzialnością z tytułu ochrony dóbr osobistych, jednak żądanie usunięcia danych osobowych nie należy do kognicji sądów powszechnych.

⁴⁸ E. L. Carter, *The Right To Be Forgotten*, Oxford Research Encyclopedia of Communication, 2016, s. 8, [online] <http://communication.oxfordre.com/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189> [dostęp: 9.02.2017].

⁴⁹ J. Barta, P. Fajgielski, R. Markiewicz, art. 32, pkt 2, [w:] *Ochrona danych osobowych...*, op. cit.; Wyrok Wojewódzkiego Sądu Administracyjnego z dnia 26 lutego 2009 r., sygn. akt II SA/Wa 1685/08, LEX nr 519827.

art. 12). Z tej przyczyny wydaje się, że po wejściu w życie nowej regulacji szczególne znaczenie będzie odgrywała kontrola zgodności wykładni rozporządzenia 2016/679.

Wnioski

Prawo do prywatności i wolność wypowiedzi należą do tej samej grupy praw człowieka, chronią zaś różne dobra. Z tej przyczyny w europejskim porządku prawnym niemożliwe jest przyznanie któremukolwiek z nich prymatu, gdyż ich zakres ochrony nie podlega wartościowaniu. Konstrukcją pozwalającą na zachowanie istoty obu tych praw może być prawo do bycia zapomnianym. Pozwala ono określić, w jakim zakresie sektor prywatny jest odpowiedzialny za ochronę wolności wypowiedzi i prawa do prywatności. Obecnie w porządku globalnym można zaobserwować pewne inicjatywy poświęcone ochronie praw człowieka w Internecie, w szczególności prawa do prywatności. Rozwój technologii informacyjnej sprawia, że coraz bardziej widoczna staje się potrzeba zagwarantowania prawa do bycia zapomnianym. Brak jednak globalnych rozwiązań normatywnych regulujących istnienie owego prawa. Konstrukcja ta pojawia się natomiast w prawie unijnym, w art. 17 rozporządzenia 2016/679.

Regulacja nakłada na podmioty administrujące i przetwarzające dane szereg obowiązków, których realizacja przy obecnym stanie technicznym wydaje się wysoce utrudniona. Pozytywnie należy ocenić objęcie zakresem zastosowania normy zarówno administratorów stron źródłowych, jak i administratorów wyszukiwarek internetowych, a także nałożenie na administratora danych obowiązku poinformowania administratorów 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 2016/679 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.

PERSPECTIVE OF REGULATION ON THE RIGHT TO BE “FORGOTTEN” ON THE INTERNET. OUTLINE OF THE PROBLEM

ABSTRACT

At the age of information technology, enabling collecting and processing vast amounts of data it is essential to protect the privacy of Internet users without restricting freedom of expression. It is claimed, that human rights protected in the real world should be respected also on the Internet. The UN Human Rights Council Resolution on the promotion, protection and enjoyment of human rights on the Internet was analyzed. One of the instruments that can contribute to achieve its goals is the right to be forgotten. The authors present the evolution of that concept in EU law and Polish and European jurisprudence. The new regulation of the right to be forgotten was introduced by the Regulation of the European Parliament and of the Council 2016/679. The main challenges and risks associated with its entry into force were indicated.

KEYWORDS

the right to be forgotten, the Internet, the right to privacy, protection of personal data

BIBLIOGRAFIA

1. Ausloos J., *The ‘Right to be Forgotten’ – Worth Remembering?*, “Computer Law & Security Review” 2012, No. 28 (2).
2. Bjarnadóttir M. R., *Does the Internet Limit Human Rights Protection? The Case of Revenge Porn*, “JIPITEC” 2016, No. 7 (3), [online] <https://www.jipitec.eu/issues/jipitec-7-3-2016/4509> [dostęp: 23.02.2017].
3. Carter E. L., *The Right To Be Forgotten*, Oxford Research Encyclopedia of Communication, 2016, [online] <http://communication.oxfordre.com/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189> [dostęp: 9.02.2017].
4. Dutton W. H., Dopatka A., Law G., Nash V., *Freedom of Connection, Freedom of Expression, UNESCO Series on Internet Freedom*, [online] <http://unesdoc.unesco.org/images/0019/001915/191594e.pdf> [dostęp: 13.08.2017].
5. 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 (DzU UE L z dnia 23 listopada 1995 r.).
6. General Assembly Resolution 68/167 on the right to privacy in the digital age, 18.12.2013.
7. General Assembly Resolution 69/166 on the right to privacy in the digital age, 18.12.2014.
8. General Assembly Resolution 71/199 on the right to privacy in the digital age, 16.11.2016.
9. Krzysztofek M., „Prawo do bycia zapomnianym” i inne aspekty prywatności w epoce Internetu w prawie UE, „Europejski Przegląd Sądowy” 2012, nr 8.
10. Lit. b, ust. 1, art. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r.

11. *NETmundial Multistakeholder Statement*, Sao Paulo 2014, s. 4, [online] <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf> [dostęp: 9.02.2017].
12. *Ochrona danych osobowych. Komentarz*, red. J. Barta, P. Fajgielski, R. Markiewicz, LEX 2015.
13. *Report of the Office of the United Nations High Commissioner for Human Rights on ways to bridge the gender digital divide from a human rights perspective*, [online] <http://www.ohchr.org/EN/Issues/Women/WRGS/Pages/WaystoBridgetheGenderDigital.aspx> [dostęp: 9.02.2017].
14. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (DzU UE L 119/1 4.5.2016).
15. Sąd Apelacyjny w Poznaniu w wyroku z dnia 13 listopada 2001 r., sygn. akt I ACa 1140/01, „Wokanda” 2002, nr 11, poz. 46.
16. *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union*, s. 181, [online] http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf [dostęp: 13.08.2017].
17. Stuart A. H., *Google Search Results: Buried if Not Forgotten*, „North Carolina Journal of Law and Technology” 2012, No. 15 (3).
18. Szymanek J., *Konstytucjonalizacja prawa do wolności myśli, sumienia, religii i przekonań*, „Studia z Prawa Wyznaniowego” 2007, nr 10.
19. The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 29.06.2012, A/HRC/20/L.30.
20. The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 20.06.2014, A/HRC/26/L.24.
21. The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 27.06.2016, A/HRC/32/L.20.
22. Uchwała siedmiu sędziów Sądu Najwyższego z dnia 20.09.1988 r., sygn. akt III CZP 37/88, OSNCP 1989, nr 3, poz. 40.
23. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 1997, nr 133, poz. 883 ze zm.).
24. Warren S. D., Brandeis L. D., *The Right to Privacy*, „Harvard Law Review” 1890, No. 4.
25. Weber R. H., *The Right to Be Forgotten: More Than a Pandora's Box?*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law” 2011, No. 2.
26. Williams C.R., *A Proposal for Protecting Privacy During the Information Age*, „Alaska Law Review” 1994, No. 11.
27. Wyrok Sądu Najwyższego z dnia 15.01.2015 r., sygn. akt II CSK 747/13.
28. Wyrok Sądu Najwyższego z dnia 19 maja 2011 r., sygn. akt I CSK 497/10, LEX nr 93 6483.
29. Wyrok Sądu Najwyższego z dnia 19.01.1982 r., sygn. akt IV CR 500/01, OSNCP 1982, nr 8–9, poz. 123.
30. Wyrok Trybunału Sprawiedliwości UE w sprawie Lindqvist z dnia 6 listopada 2003 r., C101/01, pkt 25, [online] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1361686> [dostęp: 15.10.2016].
31. Wyrok Trybunału Sprawiedliwości w sprawie eDate Advertising i in. z dnia 25 października 2011 r., C509/09 i C161/10, pkt 45.

32. Wyrok Trybunału Sprawiedliwości w sprawie Satakunnan Markkinapörssi i Satamedia z dnia 16 grudnia 2008 r., C73/07, pkt 48, 49, [online] <http://curia.europa.eu/juris/liste.jsf?language=pl&num=C-73/07> [dostęp: 16.10.2016].
33. Wyrok TSUE w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González z dnia 13 maja 2014 r., C131/12, [online] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1353218> [dostęp: 15.10.2016].
34. Żak J., *Koncepcja „prawa do bycia zapomnianym”*, [w:] *Aktualne wyzwania ochrony wolności i praw jednostki*, red. M. Jabłoński, S. Jarosz-Żukowska, Wrocław 2014.