Agnieszka Demczuk*

„Prawo do bycia zapomnianym" jako szczególne prawo jednostki do kontroli informacji o sobie w społeczeństwie informacyjnym w kontekście RODO

„Prywatność umarła – pogódźcie się z tym"
Scott McNealy, Sun Microsystems

Wstęp

Rewolucja informacyjna, która dokonuje się od blisko dwóch dekad, wynikająca z gwałtownego rozwoju sieci komputerowych, przebudowuje i zmienia społeczeństwo w informacyjne, coraz bardziej zglobalizowane i usieciowione. Powszechna staje się praktyka naruszająca własność intelektualną w cyberprzestrzeni, zagrożone jest prawo do prywatności, tajemnica elektronicznej korespondencji; zwiększa się ingerencja w życie prywatne, inwigilacja, coraz częstsze jest zakładanie fałszywych kont czy przywłaszczanie cudzych dóbr osobistych. Od lat dostawcy usług elektronicznych stosują algorytmy prognostyczne, korzystając z już otrzymanych danych osobowych; występuje powszechne zjawisko ich profilowania. Prawo do prywatności, tak jak i inne prawa podstawowe, są gwarantowane przez międzynarodowe dokumenty prawne z zakresu ochrony praw człowieka. Jednak ich faktyczna realizacja w ramach komunikacji elektronicznej wciąż wydaje się być daleka od założonych standardów przyjętych dla społeczeństwa demokratycznego. Brak regulacji w wielu kwestiach związanych z ICT sprawia, że na sądach krajowych i międzynarodowych spoczywa obowiązek kształtowania ram odpowiedzialności za naruszenia praw człowieka w cyberprzestrzeni. Przed władzami, ale także przed samymi użytkownikami sieci, stoją nowe wyzwania i szanse na zmianę zarówno w zakresie prawa, jak i praktyki. Zgłaszane są postulaty o większy i bardziej aktywny udział władz publicznych w zakresie tworzenia prawnych ram odpowiedzialności w celu efektywnej ochrony prawa do prywatności i innych praw podstawowych. Nową regulacją, która weszła w życie w państwach Unii Europejskiej w maju 2018 r., jest rozporządzenie PE i RE z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu

* Dr, Zakład Praw Człowieka, Wydział Politologii, Uniwersytet Marii Curie-Skłodowskiej w Lublinie, pl. Litewski 3, 20-802 Lublin, ademczuk@hektor.umcs.lublin.pl

takich danych, zwane RODO. Powszechny jest pogląd, iż przyjęte zapisy prawne RODO wprowadzają swoistą „rewolucję w dziedzinie ochrony danych osobowych", przewidują znaczne ograniczenia w profilowaniu danych, „prawo do bycia zapomnianym" czy rodotykę, tj. ocenę skutków dla ochrony danych w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

Celem autorki jest przybliżenie aktualnych refleksji, a także wątpliwości natury prawnej i praktycznej związanych z wdrożeniem nowych, wręcz nowatorskich rozwiązań prawnych dotyczących prawa do żądania usunięcia danych osobowych przez administratorów dotyczących użytkownika sieci oraz próba oceny skutków wynikających z realizacji tego prawa. „Prawa do bycia zapomnianym" zostanie omówione z perspektywy doktryny praw człowieka. Dokonana zostanie analiza wybranych przepisów RODO dotyczących prawa do usunięcia danych osobowych w cyberprzestrzeni oraz próba oceny ich skuteczności w przyszłości. Omówione zostanie „prawo do bycia zapomnianym", tj. podstawowy instrument prawny służący jednostce do większej kontroli informacji na swój temat udostępnionych w sieci, mając na celu zwiększenie ochrony danych o użytkownikach przed nadmiernym ich gromadzeniem i przetwarzaniem przez podmioty komercyjne. Do analizy powyższych kwestii wykorzystana zostanie metoda analizy prawnej tekstów prawnych oraz metoda studium przypadku, przedstawione zostaną wybrane kazusy z orzecznictwa międzynarodowego. Ponadto wykorzystane zostaną: metoda statystyczna pozwalająca na analizę wskaźników rozwoju społeczeństwa informacyjnego, metoda porównawcza, behawioralna i analizy systemowej.

1. Prawo do prywatności w społeczeństwie informacyjnym

Pod koniec XX w. Janusz Barta i Ryszard Markiewicz ostrzegali: „Globalne sieci komputerowe […] przyniosły ze sobą zwiększone niebezpieczeństwo ingerencji w prawo do prywatności i – spokrewnione z nim – prawo do tajemnicy korespondencji. Istnieje obawa naruszenia tej podstawowej, osadzonej w prawach osobistych […], kompetencji przynależnej człowiekowi, która pozwala mu samodzielnie decydować o tym, które informacje na jego temat […] zostaną podane do wiadomości publicznej względnie będą gromadzone bez wiedzy zainteresowanego" [Barta, Markiewicz, 2005, s. 366]. Rzeczywiście, dotychczasowy rozwój prawa do prywatności dowodzi, iż jego poszczególne elementy są niezwykle wrażliwe na zmiany wynikające z przeobrażeń warunków cywilizacyjnych związanych z szybkim postępem technologicznym. Także poglądy, postulaty i oczekiwania względem regulacji prawnych ewoluują w związku ze zmianami w sferze prywatnej. Prawo do prywatności różnie może być definiowane,

a także odmiennie mogą być wyróżniane jego składniki. Z pewnością w ramach prawa do prywatności mieści się prawo do bycia pozostawionym w spokoju, a także prawo do kontroli informacji na swój temat [więcej: Motyka, 2001]. Mają one szczególne znaczenie ponownie na początku XXI w. wraz z tak intensywnym rozwojem technologii przekazywania danych w cyberprzestrzeni.

Od ponad dwóch dekad obserwowany jest proces intensywnie rozwijających się sieci nowoczesnych technologii komunikacyjnych i informacyjnych w skali globalnej. Nowy raport *Global Electronic 2018* z „We Are Social" i „Hootsuite" ujawnia, że w 2018 r. korzysta już z Internetu ponad 4 mld ludzi na całym świecie (tj. 4,021 mld, co stanowi wzrost o 7% w skali roku). Ponad połowa populacji na świecie jest online, a najnowsze dane pokazują, że prawie jedna czwarta miliarda nowych użytkowników pojawiła się online po raz pierwszy w 2017 r. Afryka odnotowała najszybsze tempo wzrostu, a liczba użytkowników Internetu na całym kontynencie rośnie o ponad 20% z roku na rok. Znaczna część wzrostu liczby użytkowników Internetu w 2018 r. wynika z bardziej przystępnych cenowo smartfonów (dwie trzecie, tj. 5,135 mld z 7,6 mld mieszkańców na świecie posiada telefon komórkowy). Ponad połowa używanych telefonów to urządzenia „inteligentne", więc coraz łatwiej jest ludziom korzystać z bogatego Internetu, gdziekolwiek się znajdują. Również korzystanie z mediów społecznościowych (*social media*) staje się coraz powszechniejsze, a liczba osób korzystających z platformy w każdym kraju wzrosła o prawie milion nowych użytkowników każdego dnia w ciągu ostatnich 12 miesięcy. Ponad 3 mld ludzi (tj. 3,196 mld, co stanowi wzrost o 13% w skali roku) na całym świecie korzysta obecnie z mediów społecznościowych co miesiąc, a 9 na 10 użytkowników uzyskuje dostęp do wybranych platform za pośrednictwem urządzeń mobilnych [*We are social*…, 2018, s. 7–8]. Powyższe dane wskazują na coraz intensywniejszy rozwój infrastruktury i skłaniają do sformułowania wniosku, iż rzeczywiście ludzkość wkroczyła w nowy etap rozwoju społeczeństwa globalnie informacyjnego i usieciowionego. W literaturze przedmiotu pojawiło się wiele określeń na współczesne społeczeństwo. Z jednej strony jest to społeczeństwo, w którym gwałtownie rozwijają się trzy sektory infrastruktury: telekomunikacyjny, informatyczny i mediów elektronicznych, z drugiej zaś – jest to także społeczeństwo niepewności i ryzyka[1].

[1] Wiele jest definicji społeczeństwa informacyjnego. Przykładowo jedna została zaproponowana przez Luca Soete, eksperta UE już w 2001 r., tj. społeczeństwem informacyjnym jest takie społeczeństwo, które właśnie się kształtuje, gdzie technologie gromadzenia i transmisji informacji i danych są powszechnie dostępne po niskich kosztach, a powszechnemu użyciu informacji i danych towarzyszą organizacyjne, komercyjne, społeczne i prawne zmiany, które głęboko zmieniają życie, pracę i społeczeństwo jako takie [za: Doktorowicz, 2005,

Społeczeństwo informacyjne jest efektem postępu technicznego, rozwoju ICT i w sposób istotny wpływa na wszystkie aspekty życia społecznego, gospodarczego i politycznego. Stąd trudno jest stworzyć jedną precyzyjną definicję. Podstawowym problemem jest konieczność uwzględnienia wszystkich zmian i zjawisk, jakie zachodzą w społeczeństwie informacyjnym pod wpływem zastosowania i wykorzystywania technologii informacyjnych i komunikacyjnych. Obserwowany jest rozwój masowej komunikacji zindywidualizowanej, stanowiącej platformę technologiczną, która pozwala konstruować autonomię aktora społecznego – jednostki i zbiorowości [Castells, 2013, s. 19]. Najczęściej zarówno jednostki, jak i zbiorowości realizują i zaspokajają swoje potrzeby, pragnienia i emocje w mediach społecznościowych, w których od lat obserwowany jest powszechny proces profilowania danych osobowych użytkowników sieci. Podmioty komercyjne, umieszczając na platformach społecznościowych reklamy, stosują powszechnie psychografię konsumentów (metoda badania stylu życia konsumentów w oparciu o sposoby spędzania wolnego czasu, zainteresowań i osobowości) i wykorzystują algorytmy prognostyczne. W oparciu o wspomniane algorytmy tworzą się tzw. bańki informacyjne, w których „zamknięci" odbiorcy informacji mają podobne preferencje, poglądy i zainteresowania. Jak zauważa Luciano Floridi, obecnie dokonuje się czwarta rewolucja społeczna (po odkryciach Kopernika, Darwina i Freuda), w której im bardziej społeczeństwo zmienia się w infosferę, czyli mieszankę fizycznych i wirtualnych doświadczeń, tym bardziej jednostki i zarazem użytkownicy sieci zdobywają „osobowość onlife" – różną od tego, kim z natury są tylko w „prawdziwym świecie" (offline) [Floridi, 2014].

Jak zauważa Timothy Garton Ash, w Internecie o wiele łatwiej coś upublicznić, a o wiele trudniej zachować coś w sferze prywatnej, i dodaje: „Większość z nas dobrowolnie nosi przy sobie elektroniczne urządzenia śledzące. Nazywa się je telefonem komórkowym. Jeśli zebrać wszystkie dane i tak zwane metadane z naszych e-maili, połączeń telefonicznych, wyszukiwarek internetowych oraz innych urządzeń przesyłających informacje, takich jak inteligentna lodówka […], nie wspominając już o funkcjach

s. 100]. Druga zaś definicja została zaproponowana przez Leszka Porębskiego i akcentuje ona stopniowalność społeczeństwa informacyjnego. I tak, jest to społeczeństwo z jednej strony nasycone różnymi aspektami zastosowania ICT, z drugiej zaś próbujące świadomie wykorzystywać możliwości stwarzane przez nowe technologie dla wzrostu swego poziomu cywilizacyjnego i podnoszenia jakości życia. Im bardziej centralną pozycję w życiu społecznym zajmuje informacja i procesy z nią związane, tym bardziej uzasadnione jest operowanie pojęciem społeczeństwa informacyjnego w odniesieniu do konkretnej zbiorowości. Można więc mówić o stopniowalności kategorii społeczeństwa informacyjnego, większym lub mniejszym przeobrażeniu mechanizmów życia społecznego przez ICT [Porębski, 2001, s. 13].

rozpoznawania twarzy z nagrań monitoringu wizyjnego czy zdjęć trafiających do sieci – to obserwator może dowiedzieć się o nas więcej niż ornitolog o stadzie zaobrączkowanych elektronicznie ptaków. Dziś wszyscy jesteśmy zaobrączkowanymi gołębiami" [Ash, 2018, s. 453].

Fenomen Facebooka (i innych platform społecznościowych), tj. możliwość masowego rozpowszechniania informacji, którego inicjatorami są przede wszystkim zwykli ludzie, sprawia, że użytkownik, tworząc swój profil, z jednej strony promuje swoją osobę, z drugiej zaś – upubliczniając swoje dane, „sprzedaje" innym swoją osobę i informacje o sobie. Bez żadnych oporów i barier użytkownicy dzielą się (*share*) swoimi zainteresowaniami, osiągnięciami, znajomymi, nawet najintymniejszymi momentami swojego życia (np. zdjęcia USG z przebiegu ciąży – sic!). Cały system mediów społecznościowych oparty na kryterium polubień oraz udostępnianiu danych na życzenie dla firm komercyjnych w ramach wspomnianego powszechnego procesu profilowania danych sprawia, że powracają w świadomości wielu użytkowników (najczęściej starszych użytkowników) utopie Jeremy'ego Benthama czy Georga Orwella o wszechotaczającym człowieka systemie monitoringowym. Warto nadmienić, iż w Chinach od 2014 r. trwa wielki eksperyment, tj. budowa Systemu Zaufania Społecznego (*Social Credit System*), którego finalna wersja planowana jest na 2020 r. i docelowo ma dotyczyć wszystkich obywateli. To system, który ma pomóc w stworzeniu „idealnego społeczeństwa", funkcjonującego według konkretnych, oczekiwanych norm i zasad, inaczej określany jako system oceny obywateli, którego trzonem jest pięć czynników uwzględniających aktywność człowieka zarówno w sferze online, jak i offline[2]. Wciąż aktualne stają się pytania o zakres i granice ingerencji w prawo do prywatności systemów funkcjonujących w oparciu o dane i metadane użytkowników w cyberprzestrzeni zarówno w Chinach (gdzie dodatkowo w relacjach z władzą stosowany jest argument *ad baculum*), jak i w demokracjach liberalnych. Rachel Botsman zauważa, iż obecnie użytkownicy stoją przed wyborem pomiędzy jednokierunkowym panopticonem, a wzajemnym, przejrzystym rodzajem „nadzoru", który polega na obserwowaniu obserwatorów [Bosman, 2017][3].

[2] System oparty na pięciu kryteriach: historii kredytowej, zdolności finansowej, charakterystyce osobistej – danych osobowych, zachowaniach i preferencjach oraz relacjach osobistych z innymi użytkownikami.

[3] W 2013 r. skalę inwigilacji prowadzonej w Internecie przez amerykańskie służby ujawnił Edward Snowden, były współpracownik Agencji Bezpieczeństwa Narodowego USA. Twierdził on, iż władze amerykańskie stworzyły programy, np. PRISM, które umożliwiają monitorowanie ruchu w sieci na całym świecie. Ponadto służby bezpośrednio podłączały się do kanałów komunikacyjnych największych firm teleinformatycznych. Po tych doniesieniach na nowo odżyły debaty o granicach praw człowieka w społeczeństwie informacyjnym, szczególnie o ochronie prywatności w cyberprzestrzeni.

Jeszcze parę lat temu dość powszechne było przeświadczenie, iż korzystając z Internetu, użytkownicy pozostają anonimowi, prywatność zachowana, a identyfikacja w sieci prawie niemożliwa. Obecnie wiadomo, iż każdy ruch internauty pozostawia po sobie cyfrowy ślad. Od 2012 r. trwały w Unii Europejskiej prace inicjowane przez Komisję Europejską, nad stworzeniem nowego systemu zapewniającego ochronę danych osobowych. Dane osobowe użytkowników przetwarzane są przez administratorów na niespotykaną dotąd skalę, stwarzając tym samym ogromne ryzyko wykorzystywania tych danych w celach nieuprawnionych, a przede wszystkim mogących prowadzić do naruszenia fundamentalnego dla każdej jednostki jej prawa do prywatności.

2. Prawo do ochrony danych osobowych w świetle RODO – zarys problemu

Ochrona prywatności, w tym szczególnie prawo do ochrony danych osobowych, stały się w ostatniej dekadzie, szczególnie za sprawą wciąż szybko zmieniających się nowoczesnych technologii, bardzo ważnym problemem politycznym, wymagającym pilnego uregulowania na poziomie międzynarodowym. W świecie zglobalizowanym i mocno usieciowionym, w którym wielkie międzynarodowe korporacje komputerowe i internetowe są nowymi ważnymi aktorami życia publicznego, kwestie związane z przetwarzaniem danych osobowych stały się także kluczowymi zagadnieniami z zakresu cyberbezpieczeństwa. Powszechny i uzasadniony stał się pogląd o konieczności przyjęcia nowych i bardziej szczegółowych regulacji prawnych chroniących dane i metadane użytkowników, zwiększające poczucie bezpieczeństwa użytkowników w sieci.

Oprócz ogólnych przepisów dotyczących ochrony prywatności uregulowanych w Konstytucji RP z 2 kwietnia 1997 r.[4] istnieją także akty prawne, które regulują szczegółowe zasady przetwarzania danych osobowych czy przesyłania tych danych do krajów trzecich oraz prawa osób związane z wykorzystywaniem informacji o nich. Są także stosowne przepisy międzynarodowego prawa praw człowieka[5]. Do aktów prawnych

[4] Są to: art. 47 Konstytucji RP – podstawowe prawo do prywatności, w tym życia prywatnego, rodzinnego, dobrego imienia i prawa decydowania o swoim życiu osobistym, art. 76, zgodnie z którym władze publiczne są zobowiązane do ochrony konsumentów oraz użytkowników przed działaniami zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu, a także przed nieuczciwymi praktykami rynkowymi oraz art. 51 o zakazie ujawniania informacji o swojej osobie inaczej niż na podstawie ustawy,

[5] Są to m.in.: art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności z 1950 r. przyjętej w ramach Rady Europy, w którym zagwarantowano ochronę prawa do życia prywatnego i intymnego, czy art. 7 Karty Praw Podstawowych UE, zgodnie z którym każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, domu i komunikowania się.

o charakterze szczegółowym należy obecnie rozporządzenie PE i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Na gruncie zaś krajowym szczegółowymi aktami są: ustawa o ochronie danych osobowych z 2018 r. i ustawa o świadczeniu usług drogą elektroniczną z 2002 r. Nowa ustawa o ochronie danych osobowych z 10 maja 2018 r. jest aktem „przenoszącym" RODO. Rozporządzenie to ma stanowić istotny krok na drodze do większej ochrony praw podstawowych w UE w erze cyfrowej, a także ułatwienia działalności gospodarczej poprzez uproszczenie i ujednolicenie zasad dla administratorów rynku wspólnotowego. Przepisy dyrektywy 95/46/WE wymagały unowocześnienia ze względu na gwałtowny proces rozwoju usług internetowych i nowe wyzwania technologiczne, np. szczególnie intensywny rozwój social media, nowe możliwości, jakie dają usługi chmury obliczeniowej, usługi mobilne oparte na lokalizacji użytkowników.

W 2015 r. przeprowadzone zostały badania dotyczące ochrony danych na zlecenie Dyrekcji Generalnej ds. Sprawiedliwości i Konsumentów wśród prawie 28 tys. obywateli z 28 państw członkowskich UE (w okresie od 28 lutego do 9 marca 2015 r.). Badania te miały na celu wsparcie podjętej reformy ochrony danych poprzez przeanalizowanie poglądów obywateli UE na temat kwestii związanych z ochroną danych. Wyniki Eurobarometru jednoznacznie wskazały, iż zaufanie do środowisk cyfrowych pozostawało na niskim poziomie, tj. 67% respondentów wskazało, iż martwiło się faktem braku kontroli nad informacjami, które podawało w Internecie, a tylko 15% odpowiedziało, że miało nad nimi pełną kontrolę; 63% ankietowanych nie ufało firmom internetowym oraz firmom telefonicznym i internetowym dostawcom usług (62%). Połowa europejskich internautów obawiała się, że stanie się ofiarą oszustwa polegającego na niewłaściwym wykorzystaniu ich danych. Aż 89% badanych opowiedziało się za jednakową ochroną praw w całej UE, niezależnie od państwa, w którym ma siedzibę usługodawca [Eurobarometr, 2015].

RODO wprowadza szereg nowych narzędzi ochrony danych osobowych osób, których informacje te dotyczą. Przede wszystkim narzędzia te mają na celu wzmocnienie ochrony tych danych poprzez:

- prawo do usunięcia danych (prawo do bycia zapomnianym – *right to be forgotten*) (art. 17);
- łatwiejszy dostęp do danych, gdyż osoby, których dane dotyczą, będą miały dostęp do szerszego zakresu informacji o przetwarzaniu ich danych, a prawo do przenoszenia danych pozwolić ma osobom

zainteresowanym na przenoszenie danych między usługodawcami internetowymi (art. 13 ust. 2 pkt b, art. 14 ust. 2 pkt c, art. 20);
- obowiązek informowania o naruszeniu danych, tj. administratorzy mają obowiązek powiadomienia organu nadzorczego i w stosownych przypadkach osoby, której dane dotyczą, o naruszeniu danych (art. 33–34);
- silniejszą ochronę praw dzieci w RODO słusznie przyjęto założenie, iż dzieci mogą być w mniejszym stopniu świadome zagrożeń, konsekwencji, gwarancji i swoich praw w odniesieniu do przetwarzania danych osobowych; stąd rozporządzenie przewiduje, że zgoda na przetwarzanie danych dziecka, które nie ukończyło 16 lat, musi być wyrażona albo zaaprobowana przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem i tylko w zakresie wyrażonej zgody (państwa członkowskie mogą obniżyć ten próg i ustanowić niższą granicę wiekową, która musi wynosić co najmniej 13 lat) (art. 4 pkt 25, art. 8, art. 12 ust. 1, art. 40 ust. 2 pkt g);
- lepszą i sprawniejsza egzekucję przestrzegania przepisów – polski organ ochrony danych będzie wyposażony w możliwość nakładania administracyjnych kar pieniężnych w wysokości nawet do 20 mln euro lub do 4% całkowitego rocznego światowego obrotu (art. 83 ust. 5);
- konieczność wdrożenia różnych mechanizmów ochrony danych już w fazie projektowania oraz domyślnej ochrony danych (ochrona danych osobowych ma zostać uwzględniona już na etapie tworzenia usługi internetowej, a domyślne ustawienia ochrony zapewniające minimalizację przetwarzanych danych powinny zostać normą w serwisach społecznościowych (art. 25).

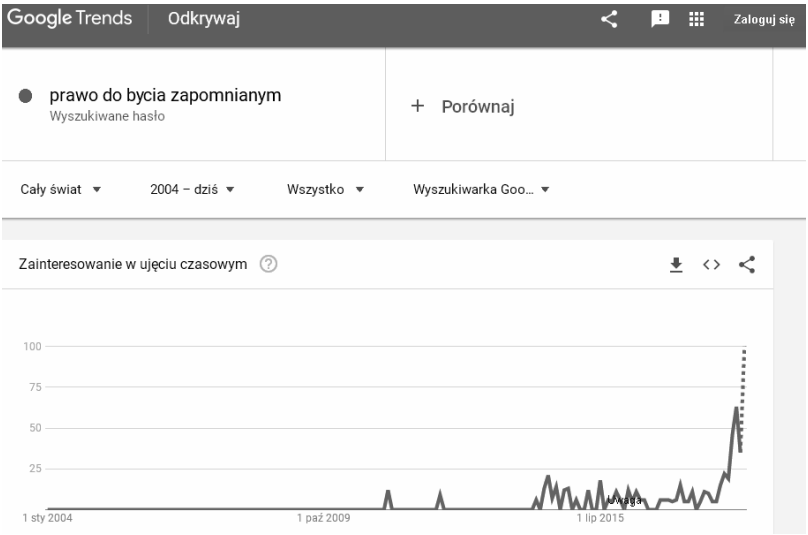
3. Prawo do usunięcia danych („prawo do bycia zapomnianym")

W przedstawionym przez Komisję Europejską w 2012 r. projekcie kompleksowej reformy unijnych przepisów w zakresie ochrony prywatności i danych osobowych znalazło się nowe rozwiązanie, które aż do maja 2018 r. nie było znane polskiemu porządkowi prawnemu, tj. prawo do usunięcia danych (tzw. prawo do bycia zapomnianym – zob. rys. 1 i 2). Rysunki te przedstawiają zainteresowanie użytkowników omawianymi hasłami, poprzez wpisywanie ich do wyszukiwarki Google. Jak widać, zainteresowanie znaczeniem tego prawa (w języku angielskim – rys. 1 i w języku polskim – rys. 2) nastąpiło dopiero w latach 2012–2013, przy czym największe zainteresowanie należy odnotować w przypadku hasła w języku polskim dopiero w 2018 (zrzut ekranu został zrobiony w lipcu 2018 r.).

Rysunek 1. Liczba zapytań dla hasła „right to be forgotten" z okresu 2004–2018

Źródło: [Google Trends, zrzut ekranu z dnia 3.07.2018].

Rysunek 2. Liczba zapytań dla hasła „prawo do bycia zapomnianym" z okresu 2004–2018



Źródło: [Google Trends, zrzut ekranu z dnia 3.07.2018].

Istotnym elementem omawianego prawa jest prawo żądania usunięcia z obiegu w Internecie danych osobowych umieszczonych w sieci przez osobę, której dotyczą, lub przez osoby trzecie. Do momentu wejścia w życie przepisów RODO w polskim porządku prawnym, zgodnie z art. 51 ust. 4 Konstytucji RP i poprzedniej ustawy z 1997 r. o ochronie danych osobowych (art. 35 ust. 1), każdy miał prawo do sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą, uszczegółowione w ten sposób, że prawo takie odnosiło się do sytuacji: po pierwsze – gdy zebrane dane były nieaktualne, niekompletne lub nieprawdziwe, albo zebrane z naruszeniem ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane. Brak było natomiast uprawnienia jednostki do usunięcia danych umieszczonych i przetwarzanych zgodnie z prawem, jednak na skutek upływu czasu dane te uległy dezaktualizacji. RODO poszerza katalog sytuacji, w których jednostki mają prawo żądania usunięcia danych. I co bardzo istotne, rozporządzenie wzmacnia ochronę danych osobowych dzieci umieszczanych i przetwarzanych w cyberprzestrzeni.

Inspiracją dla przyjęcia nowych rozwiązań dotyczących prawa do bycia zapomnianym było twierdzenie, iż w demokratycznych państwach prawnych, nawet w stosunku do sprawców poważnych przestępstw, stosuje się instytucję zatarcia skazania po upływie określonego czasu. Nie ma jednak przewidzianego regulacją prawną uprawnienia do „zatarcia" (usunięcia) danych jednostek w Internecie, a różne informacje o osobie stają się nieusuwalne, wpływając jednocześnie przez wiele lat i praktycznie bez ograniczeń czasowych na dalszą karierę polityczną czy zawodową osoby, której te informacje dotyczą [Lipowicz, 2011, s. 7].

Należy także wspomnieć o wyroku, który zapadł w dniu 13 maja 2014 r. wydanym przez Trybunał Sprawiedliwości Unii Europejskiej w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González (C-131/12). Trybunał wypowiedział się w nim co do nowego, proponowanego rozwiązania, jakim stało się prawo do bycia zapomnianym. W 2010 r. obywatel Hiszpanii M.C. González wystąpił do organu ochrony danych ze skargą dotyczącą informacji opublikowanej w 1998 r. przez dziennik „La Vanguardia", żądając jej usunięcia ze strony internetowej gazety i wyszukiwarki Google. Organ ochrony danych uznał, że gazeta nie musi usuwać pierwotnej publikacji, ponieważ ukazała się zgodnie z prawem, natomiast Google musiał usunąć prowadzące do niej linki. Google odwołał się do hiszpańskiego sądu krajowego najwyższej instancji, który przekazał sprawę do Trybunału Sprawiedliwości UE. TSUE orzekł, że firma obowiązana jest usunąć zaskarżony link z list wyników wyszukiwania wszystkich swoich wyszukiwarek na terenie UE

(np. google.es, google.de, google.co.uk). Międzynarodowe zainteresowanie ta sprawą sprawiło, że wystąpił efekt Streisend, zainteresowanie sprawą było tak duże, że np. brytyjski „Guardian" zarejestrował blisko 840 artykułów w największych światowych mediach w ciągu jednego dnia. Jak zauważa T.G. Ash: „Usiłując ochronić własną prywatność, González został nie tylko postacią publiczną, ale wręcz postacią historyczną. Na zawsze zostanie zapamiętany jako człowiek, który chciał, by o nim zapomniano" [Ash, 2018, s. 495–496].

Co ciekawe, firma Google została później „zalana" żądaniami dotyczącymi „delistingu" linków. Przez kolejne miesiące do 2015 r. firma otrzymała ponad 300 tys. takich wniosków i w związku z tym musiała przeanalizować ponad 1 mln adresów URL, usuwając z wyszukiwarek około 40% adresów.

Prawo do bycia zapomnianym *expressis verbis* wynika z art. 17 RODO. Po pierwsze, jak wynika z ust. 1, osoba, której dotyczą dane, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe. Obowiązek ten powstaje w sytuacjach, o których mowa w rozporządzeniu, tj. gdy dane osobowe nie są już niezbędne do celów, do których je zebrano, gdy podmiot danych wycofał zgodę i nie istnieje inna podstawa prawna dla przetwarzania tych danych, albo kiedy podmiot danych wniósł sprzeciw do dalszego przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania. Administrator powinien usunąć dane osobowe przetwarzane niezgodnie z prawem oraz kiedy zostały zebrane w celu świadczenia usług internetowych dziecku. Wreszcie, dane osobowe muszą być usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w unijnym bądź krajowym przepisie prawnym, tj. np. przepisach dotyczących niszczenia dokumentacji medycznej. Administrator, który upublicznił dane osobowe, a na mocy wspomnianego wyżej przepisu ma obowiązek usunąć dane osobowe, powinien być zobligowany do poinformowania innych administratorów, którzy przetwarzają te dane, do usunięcia linków, kopii i odniesień do tych danych osobowych (ust. 2). Stąd administrator powinien usunąć dane ze wszystkich miejsc, np. z serwera, poczty, plików tekstowych, arkuszy kalkulacyjnych, dysków zewnętrznych, przenośnych czy nawet papierowych kopii. Samo bowiem przechowywanie przez administratora danych nadal będzie kwalifikowane jako przetwarzanie tych danych[6]. Istotny jest

[6] Jak informuje Ministerstwo Cyfryzacji w swym Informatorze RODO, dane muszą być usuwane z kopii zapasowych, a jeżeli usuwanie z tych kopii pojedynczych rekordów stwarza ryzyko naruszenia integralności pozostałych gromadzonych danych – administrator może manualnie przywracać kopie do bazy głównej, a następnie usuwać z nich pojedyncze rekordy i tworzyć backupy bazy pomniejszone o te rekordy (choć jest to proces czasochłonny) [Ministerstwo Cyfryzacji, 2017, s. 7].

także obowiązek administratora do poinformowania podmiotów przetwarzających, aby stosowne dane również usunęli.

Dane osób, które chciałyby być zapomniane, muszą być zatem usunięte w całości z systemu administratora. Jeśli dane opublikowane są w Internecie, to administrator musi upewnić się, że wszystkie linki do tych informacji także zostały skasowane, a kopie i repliki pousuwane, nawet jeżeli są w posiadaniu innych podmiotów przetwarzających te dane w imieniu administratora. Nie wystarczy dezaktywować lub ukryć profil danej osoby w wybranej platformie social media. Dane należy usunąć. Jest to jak dotąd największe wyzwanie dla systemów informatycznych, tj. opcja usuwania danych.

Omawiany przepis w ostatnim ustępie reguluje także sytuacje, kiedy administrator danych nie będzie musiał realizować tego prawa, tj. gdy przetwarzanie danych przez administratora jest wymagane przez prawo unijne albo krajowe lub gdy jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń (np. gromadzenia dokumentacji pracowniczej), do korzystania z prawa do wolności wypowiedzi i informacji, w celach archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych czy też celów statystycznych (o ile prawdopodobne jest, że prawo do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania). Wreszcie art. 17 ust. 3 przewiduje także brak zastosowania omawianego prawa z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego.

Zakończenie

Brak regulacji wielu zagadnień związanych z funkcjonowaniem Internetu sprawia, że wciąż to na sądach krajowych i trybunałach międzynarodowych spoczywa przede wszystkim obowiązek kształtowania standardów prawnych z zakresu prawa do prywatności. Do międzynarodowych trybunałów napływa wiele spraw dotyczących mediów, w tym elektronicznych, i samego Internetu. „Prawo do bycia zapomnianym", jako prawo do usunięcia danych osobowych, także stało się przedmiotem rozpatrywania przed TSUE w Luksemburgu. Pomimo wcześniejszych regulacji prawnych odnoszących się w pewnym zakresie do tego prawa dopiero RODO reguluje te kwestie w sposób nowy i pełniejszy. W literaturze przedmiotu wykazywano, iż przed wejściem w życie RODO egzekwowanie prawa do usunięcia danych było właściwie niemożliwe. Postulowano podjęcie działań legislacyjnych w tej sprawie, przy czym prognozowano częściową tylko jego skuteczność, twierdząc, że mogą ją zapewnić przede wszystkim działania edukacyjne i popularyzacja wiedzy dotyczącej zagrożeń, wynikających z przetwarzania danych w Internecie i praw osób, której dane dotyczą [Krzysztofek, 2012, s. 6].

Obecnie po wejściu w życie RODO perspektywy rozwoju i interpretacji tego szczególnego rodzaju prawa do prywatności zdają się otwierać na nowo. Wydaje się jednak, że tak jak w przypadku innych nowych rozwiązań prawnych, tak i w tym przypadku kluczowe staną się rozstrzygnięcia sądowe wyznaczające kierunek szczegółowej interpretacji omawianych przepisów z art. 17 RODO. Na szczególną uwagę zasługują także te rozwiązania, które dotyczą danych osobowych dzieci w sieci. Dla wielu młodych użytkowników istnienie w sieci jest koniecznym warunkiem ich egzystencji. Udostępniają dobrowolnie wiele informacji i zdjęć na swój temat, by móc „zaistnieć" w cyberprzestrzeni, nie zdając sobie sprawy z zagrożeń, ale i konsekwencji takich wyborów. Z pewnością w przyszłości prawo dostępu do treści swych danych, prawo do ich sprostowania, prawo do wniesienia sprzeciwu wobec przetwarzania danych, czy wreszcie prawo żądania do usunięcia danych pozwolą na realizację w większym zakresie prawa do kontroli informacji na swój temat. Być może też „gwarancje rodowskie" pozwolą w przyszłości na uniknięcie „nieprzyjemnego rozgłosu" z powodu dawno opublikowanych w sposób nieprzemyślany, potem „zapomnianych" – lecz nie przez Internet – zdjęć czy wpisów. Należy podkreślić, iż uwaga mediów – po wejściu w życie RODO – skoncentrowana była na negatywnych konsekwencjach braku realizacji wspomnianych obowiązków prawnych i możliwych, wielomilionowych karach. Jak się wydaje, bardzo mało uwagi poświęcono kwestii podniesienia świadomości prawnej w zakresie znajomości przyjętych nowych rozwiązań. W pierwszych miesiącach obowiązywania RODO pojawiło się wiele nieporozumień co do znaczenia wielu postanowień dyrektywy, np. te związane z rzekomym całkowitym zakazem umieszczania danych osobowych w przestrzeni publicznej offline (skrzynki pocztowe, szafki szkolne, wywoływanie po nazwisku pacjentów w szpitalach i przychodniach i inne). Stąd konieczny jest, jak się wydaje, postulat większej edukacji społecznej w tym zakresie.

Warto również zauważyć, że już w pierwszym dniu wejścia w życie przepisów RODO, 25 maja 2018 r., zostały złożone pozwy przeciwko Facebookowi i Google'owi. Zrobił to austriacki prawnik Max Schrems, prowadzący organizację None of Your Business, twierdząc, iż firmy te złamały nowe przepisy, tj. zarzuty dotyczą przestrzegania RODO w systemie operacyjnym Android (należącym do Google), oraz także tego, co z danymi robi Facebook i należące do niego Instagram i WhatsApp. Naruszanie prawa odbywa się bowiem zdaniem M. Schremsa poprzez niedopuszczalne pozyskiwanie danych wrażliwych swoich użytkowników bez ich zgody (Facebook), zaś w przypadku Androida problemem jest fakt, iż aby z niego korzystać, należy dać zgodę na przetwarzanie danych.

Literatura

Ash T.G. (2018), *Wolne słowo. Dziesięć zasad dla połączonego świata*, Kraków 2018.

Baran B., Południak-Gierz K., *Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki*, „Zeszyty Naukowe Towarzystwa Doktorantów UJ, Nauki Społeczne", nr 2, Kraków.

Barta J., Markiewicz R. (1999), *Prawo do prywatności w społeczeństwie informatycznym*, „Ethos", nr 1–2.

Botsman R. (2017), *Big data meets Big Brother as China moves to rate its citizens*, „Wired", 21 October.

Bychawska-Siniarska D., Głowacka D. (2014), *Wirtualne media – realne problemy*, Warszawa.

Castells M. (2013), *Sieci oburzenia i nadziei. Ruchy społeczne w Internecie*, Warszawa.

Doktorowicz K. (2005), *Europejski model społeczeństwa informacyjnego: polityczna strategia Unii Europejskiej w kontekście globalnych problemów w wieku informacyjnym*, Katowice.

Dubis W., Daćków M. (2015), *Prawo do bycia zapomnianym w Internecie – za życia i po śmierci?*, w: J. Kołaczyński, J. Mazurkiewicz, J. Turłukowski, D. Karkut (red.), *Non omnis moriar: osobiste i majątkowe aspekty prawne śmierci człowieka: zagadnienia wybrane*, Wrocław.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, Dz. Urz. WE L 281 z 23 listopada 1995

Eurobarometr, badanie specjalne 431 – Data Protection, czerwiec 2015 r., Europejska Komisja, http://ec.europa.eu, dostęp: 3.07.2018.

Floridi L. (2014), *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford.

Generalny Inspektor Ochrony Danych Osobowych, https://giodo.gov.pl, dostęp: 3.07.2018.

Karta Praw Podstawowych Unii Europejskiej z 7 grudnia 2000 (Dz. Urz. z 2012/C 326/02).

Konstytucja Rzeczpospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. Nr 78, poz. 483 z późn. zm.

Konwencja o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r., Dz. U. z 1993, Nr 61, poz. 284.

Krzysztofek M. (2012), *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy", sierpień.

Lipowicz I. (2011), *Prawo do zapomnienia*, w: *Uwagi do strategii poprawy skuteczności unijnych przepisów dotyczących ochrony danych osobowych, przedstawionej przez Komisję Europejską przygotowane przez Stowarzyszenie „Naukowe Centrum Prawno-Informatyczne"*, Warszawa.

Ministerstwo Cyfryzacji (2017), *Informator RODO*, Warszawa.

Ministerstwo Łączności (2001), *ePolska – Strategia rozwoju społeczeństwa informacyjnego na lata 2001–2006*, Warszawa.

Motyka K. (2001), *Prawo do prywatności. Aspekty prawne i psychologiczne*, Lublin.

Niklas J. (2014), *Prywatność w Internecie*, „Infos", nr 13.
Porębski L. (2001), *Elektroniczne oblicze polityki. Demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Kraków.
Rozporządzenie PE i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. WE L 119 z 4 maja 2016.
Świeboda H. (2013), *Problem prywatności w społeczeństwie informacyjnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego", nr 763, „Ekonomiczne Problemy Usług", nr 105.
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, t.j. Dz. U. z 2019 r., poz. 123.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. poz. 1000 z późn. zm.
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t.j. Dz. U. z 2016 r. poz. 922 z późn. zm.
We Are Social, Global Digital Report 2018, https://digitalreport.wearesocial.com/, dostęp: 12.06.2018.

Streszczenie

Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych znacząco wzrosła. W 2018 r. weszło w życie rozporządzenie o ochronie danych osobowych (RODO), które reguluje kwestie związane z przetwarzaniem danych osobowych i wprowadza po raz pierwszy do polskiego systemu prawnego prawo do bycia zapomnianym. Przed podmiotami komercyjnymi i instytucjami publicznymi stoją wyzwania o charakterze finansowym i organizacyjnym, a także edukacyjnym i kulturowym, tj. zmiany mentalności pracowników w zakresie większej ochrony danych osobowych w cyberprzestrzeni.

Słowa kluczowe

społeczeństwo informacyjne, Internet, prawo do prywatności, „prawo do bycia zapomnianym", RODO

„The right to be forgotten" as a special right of the individual to control information about himself in the information society in the General Data Protection Regulation (GDPR) context (Summary)

Rapid technical progress and globalization have brought new challenges in the field of personal data protection. The scale of collecting and exchanging data has increased significantly. The General Data Protection Regulation (GDPR/RODO) entered into force in 2018, which regulates issues related to the processing of personal data and introduces the right to be forgotten for the first time in the Polish legal system. Commercial and public institutions face challenges of a financial and organizational nature, as well as educational and cultural, i.e.

changes in the mentality of employees in the scope of greater protection of personal data in cyberspace.

Keywords
information society, Internet, right to privacy, right to be forgotten, GDPR/RODO