ZESZYT NAUKOWY
Wyższa Szkoła Zarządzania i Bankowości w Krakowie

Weronika Wojturska
Wydział Prawa i Administracji Uniwersytetu Warszawskiego
wwojturska@op.pl

E-PRYWATNOŚĆ W PERSPEKTYWIE USTAWODAWCY UNIJNEGO

Wprowadzenie

W obliczu zaawansowanych możliwości technicznych współczesnej cywilizacji prywatność staje się dobrem powszechnie pożądanym, a konieczność jej ochrony osiąga walor prawny, znajdując odzwierciedlenie w porządkach normatywnych na poziomie krajowym i międzynarodowym. Uzasadnieniem dla wprowadzania skutecznych gwarancji jest przede wszystkim dysponowanie przez każdego indywidualnym prawem do wyłącznej kontroli tej sfery, która nie dotyczy innych, a w której wolność od ciekawości z zewnątrz jest swoistą *conditio sine qua non* swobodnego rozwoju jednostki[1]. W obliczu wyzwań jakie pociąga za sobą rozbudowana infrastruktura informatyczna i postępujący rynek nowych technologii autorka podejmuje się oceny prawnej kondycji prawa do prywatności w łączności elektronicznej w perspektywie dotychczasowych regulacji unijnych i orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. Analizie na tle orzecznictwa poddane zostanie funkcjonowanie prawa do bycia zapomnianym, a także wybrane zagadnienia wdrażanych rozwiązań rozporządzenia 2016/679[2]. Ponadto rezultaty badań nad zjawiskiem możliwych zagrożeń wynikających z eksploatacji wzrastającej ilości gromadzonych danych użytkowników sieci Web, pozwolą w sposób krytyczny odpowiedzieć na pytanie – na ile kapitalne hasło orwellowskiego fikcji "Wielki Brat Patrzy"[3] znajduje oddźwięk w rzeczywistości?

1. Prywatność użytkowników sieci w aspekcie międzynarodowych gwarancji ochrony praw podstawowych

Od czasów zakończenia II wojny światowej sztandarową domeną dynamicznie formującego się systemu prawa międzynarodowego stała się ochrona podstawowych praw i

[1] M. Safjana, *Prawo do ochrony życia prywatnego* [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, pod red. L. Wiśniewskiego, Warszawa 1997, s. 127-128.
[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – dalej RODO.
[3] G. Orwell: *Rok 1984*, Warszawa 2003, s. 7-8.

wolności człowieka[4]. Wraz z wzrastającym trendem eksponowania poczucia indywidualności, odrębności i niepowtarzalności jednostki dostrzeżono konieczność zagwarantowania prawa do prywatności jako elementu praw obywatelskich. Został mu nadany status równoprawny z innymi fundamentalnymi gwarancjami jak godność, wolność sumienia, swoboda wyznania czy wypowiedzi. Prawo do prywatności otrzymało ochronę zarówno na gruncie regulacji o charakterze ogólnoświatowym, jak i regionalnym[5]. Na potrzeby niniejszej pracy poddany rozwadze zostanie jeden z elementów prywatności rozumiany jako autonomia informacyjna, czyli swoboda dysponowania i decydowania przez jednostkę o zakresie ujawnianych na jej temat informacji.

W kontekście problematyki ochrony praw człowieka w Internecie na szczególną uwagę zasługują przede wszystkim zinstytucjonalizowane działania Organizacji Narodów Zjednoczonych. Zasadniczym krokiem milowym stało się powołanie na mocy rezolucji nr 60/251[6] przyjętej w dniu 15 marca 2006 r. nowego organu pomocniczego Zgromadzenia Ogólnego ONZ – Rady Praw Człowieka. Pierwszym reformatorskim aktem okazała się rezolucja z dnia 5 lipca 2012 roku pt. „Promowanie, ochrona i korzystanie z praw człowieka w Internecie", która podkreśla wagę i zależność pomiędzy ochroną praw człowieka oraz swobodą przepływu informacji w sieci[7]. Jej głównym przesłaniem jest to, aby prawa i wolności chronione w świecie rzeczywistym, były adekwatnie zabezpieczone także *on-line*. W sposób szczególny zwrócono uwagę na poszanowania zasad wolności słowa bez względu na granice administracyjne i używane w tym celu środki przekazu masowej informacji, przy jednoczesnym respektowaniu art. 19 Powszechnej Deklaracji Praw Człowieka[8] oraz postanowień art. 19 Międzynarodowego Paktu Praw Obywatelskich i Politycznych[9]. Choć akt nie jest prawnie wiążący, to w sposób prekursorski zachęcił 47 państw członkowskich Rady Praw Człowieka (w tym także Polskę) do promocji oraz usprawnienia dostępu do Internetu przy

[4] M. Wujczyk, *Prawo pracownika do ochrony prywatności*, Warszawa 2012, s. 36.
[5] M. Wujczyk, *op cit.*, s. 36.
[6] Rezolucja Zgromadzenia Ogólnego ONZ A/RES/60/251 z dnia 15 marca 2006 r. Rada Praw Człowieka rozpoczęła pracę 19 czerwca 2006 r.
[7] 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.
[8] Art. 19 – "Każdy człowiek ma prawo wolności opinii i wyrażania jej; prawo to obejmuje swobodę posiadania niezależnej opinii, poszukiwania, otrzymywania i rozpowszechniania informacji i poglądów wszelkimi środkami, bez względu na granice." Powszechnej Deklaracji Praw Człowieka z 10 grudnia 1948 r. Powszechna Deklaracja Praw Człowieka, http://ms.gov.pl/prawa_czl_onz/prawa_czlow_12.doc, Dostęp: 20.03.2018r.
[9] Art. 19 ust. 1 – "Każdy człowiek ma prawo do posiadania bez przeszkód własnych poglądów."; ust. 2 – "Każdy człowiek ma prawo do swobodnego wyrażania opinii; prawo to obejmuje swobodę poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób według własnego wyboru." Międzynarodowego Paktu Praw Obywatelskich i Politycznych z dnia 19 grudnia 1966 r. (Dz.U.1977.38.167).

jednoczesnej współpracy na polu międzynarodowym zorientowanej na przepływ informacji przy pomocy nowoczesnych technik komunikacyjnych[10]. Szerszy dyskurs w tym aspekcie podjęły kolejne rezolucje z 2014[11] i 2016[12] roku. Pierwsza ze wskazanych zwróciła uwagę na konieczność budowania zaufania w Internecie, aby w sposób efektywny wykorzystać jego potencjał do stwarzania warunków rozwoju i innowacji, w szczególności jako narzędzie promujące prawa do edukacji[13]. Państwa zostały zachęcone do wyjścia naprzeciw analfabetyzmowi cyfrowemu oraz rozwiązywania problemów z zakresu bezpieczeństwa w odniesieniu do wolności słowa, swobody stowarzyszania się, poszanowania prywatności. Rezolucja postulowała o stworzenie i przyjęcie w sposób transparentny oraz przy współudziale grup interesariuszy odpowiednich polityk krajowych, które dążą do urzeczywistniania praw człowieka w przestrzeni internetowej oraz popularyzowania globalnego i ogólnodostępnego charakteru zasobów sieciowych[14]. Z kolei drugi ze wskazanych aktów poczynił decydujące kroki w kierunku przeciwdziałania działaniom państw ukierunkowanych na dyskryminację, przemoc i wykluczenie cyfrowe w dostępie do Internetu[15]. Zaapelowano o konieczność projektowania, dystrybucji i rozwoju systemów teleinformatycznych przy udziale osób niepełnosprawnych oraz zlikwidowania wielu form cyfrowych podziałów za względu na płeć[16].

W obliczu rozbudowanej infrastruktury informatycznej potrzebę ochrony prawa do prywatności dostrzeżono również w Unii Europejskiej, która wielokrotnie w licznych aktach prawa, jak i na kanwie orzecznictwa Trybunału Sprawiedliwości, porusza kwestię prawa do prywatności, w szczególności w kontekście ochrony danych osobowych[17]. Sięgając u źródeł prawa pierwotnego, podstawy takie stwarza art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którym: "Każda osoba ma prawo do ochrony danych osobowych jej dotyczących". Kolejnym z gwarantów jest art. 6 ust 1 Traktatu o Unii Europejskiej, który zawiera deklarację uznania przez Unię praw, wolności i zasad określonych w Karcie Praw

[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] Ibidem.
[15] 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.
[16] Ibidem.
[17] H. Szewczyk, *Ochrona dóbr osobistych w zatrudnieniu*, Kraków 2007, s. 53–113; J. Braciak, *Prawo do prywatności*, Warszawa 2004, s. 61–111.

Podstawowych Unii Europejskiej z 7 grudnia 2000 roku, a także potwierdza przystąpienie Unii do europejskiej Konwencji praw człowieka i podstawowych wolności.

Kwestie dotyczące ochrony prywatności informacyjnej uregulowane w Karcie, której nadano moc wiążącą wobec wszystkich krajów Unii Europejskiej na mocy traktatu podpisanego w Lizbonie z 13 grudnia 2007 r.[18], należy uznać za kluczowe z uwagi na zebrane w akcie wszystkie fundamentalne dla współczesnej Europy prawa człowieka i obywatela[19]. Na szczególną uwagę w tym zakresie zasługuje art. 8 Karty – "Każdy ma prawo do ochrony danych osobowych, które go dotyczą, jak również (ust. 2) dane te muszą być przetwarzane rzetelnie, w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, oraz (ust. 3) każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Przestrzeganie tych zasad podlega kontroli niezależnego organu". Regulację tę, jako specyficzny rodzaj prawa pierwotnego, należy uznać za pożądaną, mając na względzie wzrost liczby gromadzonych danych przez poszczególne podmioty. Sięgając do prawa wtórnego, pierwszym bazowym *acquis communautaire* wydanym w ramach delegacji z art. 16 ust 2 TfUE jest przyjęta dnia 24 października 1995 r. przez Parlament Europejski i Radę dyrektywa 95/46/WE (dyrektywa o e-prywatności) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[20]. Została ona implementowana do polskiego porządku prawnego ustawą o ochronie danych osobowych[21]. Należy zgodzić się z *M. Wulczykiem,* zdaniem którego, mamy do czynienia z pewną dychotomią celów na co wskazuje art. 1 dyrektywy, zgodnie z którym państwa członkowskie są z jednej strony zobowiązane do ochrony praw obywateli, w tym prawa do prywatności, z drugiej zaś do nieograniczania swobodnego przepływu danych. Przede wszystkim warto wskazać na zakres wynikającej z niej ochrony, definiując dane osobowe jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przetwarzanie danych osobowych zostało określone jako każda operacja lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie

[18] Dz. Urz. UE C 303 z 14.12.2007, s. 1 ze sprost.
[19] J. Sieńczyło-Chlabicz, *Ochrona prywatności osób powszechnie znanych w świetle Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności i Karty Praw Podstawowych* (w:) A. Wróbel (red.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009, s. 231–251.
[20] Dz. Urz. UE L 281 z 23.11.1995, s. 31 z późn. zm.
[21] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016.0.922 t.j.) – dalej UODO.

lub kompilowanie, blokowanie, usuwanie lub niszczenie (art. 2 lit. b dyrektywy 95/46/WE)[22]. Co istotne, dyrektywie podkreślono wymóg uzyskania zgody jako jednej z przesłanek legalności przetwarzania danych (art. 7 dyrektywy 95/46/WE). W końcu dyrektywa gwarantuje każdej osobie prawo dostępu do dotyczących jej danych, które są przetworzone (art. 12 dyrektywy 95/46/WE). W świetle wskazanych unormowań akt ten należy potraktować jako pierwszy fundament współczesnej ochrony prywatności w zakresie autonomii informacyjnej w państwach Unii Europejskiej[23]. Niezbędnym dopełnieniem, ze względu na specyfikę i zagrożenia dla prywatności wynikające z nieuprawnionego dostępu do danych w Internecie, są: dyrektywa **o handlu elektronicznym**[24], powołująca urząd Europejskiego Rzecznika Ochrony Danych oraz dyrektywa o ochronie prywatności i komunikacji elektronicznej[25]. Nie sposób pominąć także RODO w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, które z mocy prawa uchyla dyrektywę 95/46/WE. Akt będzie obowiązywać w pełni we wszystkich krajach członkowskich od 25 maja 2018 r., po dwuletnim okresie przejściowym. Jego podstawowym celem jest doprowadzenie do pełnej harmonizacji prawa materialnego w ramach UE, o czym będzie mowa będzie w dalszej części pracy.

2. Wykładnia prawa do bycia zapomnianym na kanwie orzecznictwa unijnego

Jednym z podstawowych postulatów Komisji Europejskiej przy reformowaniu systemu ochrony danych w związku z dynamicznym rozwojem społeczeństwa informacyjnego było wzmocnienie tzw. prawa do bycia zapomnianym, tzn. "prawa osób fizycznych do swobodnego usunięcia ich danych oraz zaprzestania ich przetwarzania, jeżeli przestały być potrzebne do zgodnych z prawem celów"[26]. Zagadnienie sprawowania kontroli nad danymi osobowymi przez jednostkę pierwotnie zostało wprowadzone przy pomocy dyrektywy 95/46/WE, której postanowienia odzwierciedliła implementowana UODO w art. 32 ust. 1 pkt 6. Zgodnie z nim,

[22] M. Wujczyk, *op cit.,* s. 60.
[23] A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy o dyrektywie Unii Europejskiej*, PiP 1997, z. 6, s. 29 i n.
[24] **Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego, (***Dz. U. L 178 , 17/07/2000 P. 0001 - 0016).*
[25] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej, (*Dz*. Urz. WE L 201 z 2002 *r*., s. 37 ze zm.).
[26] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „*Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*", KOM(2010) 609, Bruksela 2010.

każdy ma 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. Ponadto za postępowe należy uznać wprowadzenie możliwości (pkt 7) wniesienia w szczególnych przypadkach umotywowanego żądania zaprzestania przetwarzania danych oraz (pkt 8) wniesienia sprzeciwu wobec przetwarzania danych w przypadkach, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych. Jak słusznie zauważa *A. Mednis*, analiza przepisów UODO wskazuje, że kontrola jednostki nad jej danymi, prowadząca w szczególności do ich usunięcia jest w gruncie rzeczy dość ograniczona. Składa się na to fakt, że administrator jest zobowiązany do usunięcia danych jeśli zebrano jest z naruszeniem przepisów, co uniemożliwia usunięcie danych zebranych na podstawie umowy lub w celu realizacji umowy. Za zasadnicze ograniczenie należy także uznać konieczność umotywowania szczególną sytuacją opartą wyłącznie na przesłance wykonywania zadań dla dobra publicznego lub usprawiedliwionego celu. Trudności nastręcza także brak gwarancji, że usunięcie informacji z jednego źródła nie pojawi się w innym miejscu, z uwagi na możliwość swobodnego ściągnięcia, utrwalenia i powielania treści na inne strony źródłowe. W tym miejscu warto zadać pytanie, czy uprawniona jednostka, której dane dotyczą, może domagać się, aby wyszukiwarka internetowa nie wyświetlała wyników wskazujących na powiązane strony źródłowe? W tym aspekcie za reformatorski dla formowania się prawa do bycia zapomnianym należy przyjąć wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google przeciwko AEPD[27]. W marcu 2010 r. strona postępowania – Mario Consteja Gonzalez – po bezskutecznej interwencji u wydawcy dziennika "La Vanguardia", wystąpił do firmy Google z żądaniem, aby wyniki wyszukiwania nie wskazywały linków do nieaktualnych informacji dotyczących licytacji nieruchomości w związku z niezapłaceniem przezeń należności z ubezpieczenia społecznego[28]. Skarżący interweniował, do Urzędu Ochrony Danych Osobowych, zaś ten przychylając się

[27] Wyrok TSUE w sprawie Google Spain SL i Google Inc. przeciwko Agencia Españo-la de Protección de Datos (AEPD) i Mario Costeja González z dnia 13 maja 2014 r., C131/12, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=43948. Dostęp: 23 marca 2018 r.

[28] I.C. Kamiński, Z. Warso, *Czy można zniknąć z Google'a? Orzeczenie Trybunału 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)*, w: D. Bychawska-Siniarska, D. Głowacka, "Wirtualne media – realne problemy", Warszawa 2014, s. 51-52.

częściowo do skargi zażądał wycofania danych od operatora wyszukiwarki Google z jej indeksów z racji podlegania odpowiedzialności za przetwarzanie danych[29]. Trybunał w sprawie wystosowanej przez firmy Google Spain i Google Inc. posiłkował się już wcześniejszą definicją wypracowaną w wyroku w sprawie Lindqvist, gdzie wskazał, że „przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany"[30] 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"[31]. Orzeczenie oparł o wykładnie prawa do usunięcia danych z art. 12 lit. b dyrektywy 95/46/WE oraz prawa sprzeciwu wynikającego z art. 14 lit. a dyrektywy 95/46/WE. W uzasadnieniu wskazał, że przetwarzanie imienia i nazwiska może znacząco oddziaływać na uprawnienie do poszanowania prywatności i ochrony danych osobowych, jeżeli to przetwarzanie umożliwia każdemu internaucie otrzymanie ustrukturyzowanej listy wyników wyszukiwania dotyczących konkretnej osoby[32]. Ponadto, stwierdził, że podmiot danych ma prawo do zwracania się do wyszukiwarek internetowych w celu uniemożliwienia indeksowania dotyczącej go informacji, opublikowanej na stronach internetowych osób trzecich[33]. Orzeczenie to podkreśla rolę wyszukiwarek jako płaszczyzny rozpowszechniania informacji, które mogą prowadzić do naruszenia prawa do prywatności, co bez wątpienia miało wpływ na postanowienia nowego rozporządzenia o ochronie danych osobowych w Unii Europejskiej.

3. Analiza wybranych zagadnień u progu unijnej reformy ochrony danych osobowych

Długo wyczekiwany owoc unijnej debaty nad reformą ochrony danych osobowy – RODO – zacznie być stosowane od 25 maja 2018 r. Jako wyraz próby sprostania realiom współczesnego społeczeństwa informacyjnego po ponad 22 latach obowiązywania, zastąpi ono dyrektywę o e-prywatności. Jak słusznie wskazuje *E. Bielak-Jomaa* i *D. Lubasz*, data ta stanowi specyficzną cezurę w rozwoju prawa ochrony danych osobowych i jest to związane nie tylko z

[29] I.C. Kamiński, Z. Warso, *op. cit.*, s. 52.
[30] Wyrok Trybunału Sprawiedliwości UE w sprawie Lindqvist z dnia 6 listopada 2003 r., C101/01, pkt 25, http://curia.europa.eu/juris/document/document. jsf? text=&docid=48382&page Index=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid= 1361686. Dostęp: 24 marca 2018r.
[31] Ibidem.
[32] M. Czerniawski, *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych*, "Europejski Przegląd Sądowy" 05/2015, s. 4-5.
[33] Ibidem.

materią regulacyjną, ale także z wyborem środka legislacyjnego dla realizacji celów regulacji, ponieważ rozporządzenie jako akt prawa unijnego będzie obowiązywało we wszystkich państwach członkowskich w sposób bezpośredni, co z kolei ma w istotny sposób ograniczyć negatywny efekt harmonizacji minimalnej dokonywanej dyrektywą 95/46/WE[34]. Skala nadchodzących zmian jest na tyle rozległa, iż a potrzeby pracy przeanalizowano kwestie, zdaniem autorki, najbardziej zasadnicze z perspektywy użytkowników sieci Web.

Nowe przepisy dotyczyć będą znacznie szerszej grupy podmiotów niż dotychczas – także przedsiębiorstw, które oferują usługi na terenie UE, mając jednocześnie siedzibę poza jej granicami. Przede wszystkim regulacja wymusza, a by wszystkie przedsiębiorstwa chcące oferować swoje usługi na terenie Unii Europejskiej – bez względu na to, czy mają swoją siedzibę w kraju członkowskim, czy nie – stosowały europejskie prawo ochrony danych osobowych, czyli tzw. wyrównanie pola egzekwowania (*level playing field*)[35]. Kolejną z istotnych zmian będzie także obowiązek przeprowadzania przez przedsiębiorców oceny skutków operacji przetwarzania dla ochrony danych osobowych, a w pewnych sytuacjach konsultacje z Generalnym Inspektorem Ochrony Danych Osobowych (GIODO) jeszcze przed rozpoczęciem ich przetwarzania. Nowe rozporządzenie wymaga spełnienia kryterium przejrzystości, odpowiedzialności i rozliczalności wobec podmiotów zajmujących się komercjalizacją wielkich danych (*big data*). Wyklarowanie standardów ochrony w tych zakresie ma na celu zachęcić aktorów biznesowych do wprowadzania innowacyjnych rozwiązań środków technicznych i organizacyjnych, które skutecznie i wydajnie będą chronić dane osobowe przed incydentami związanymi z ryzykiem wykorzystania ich w sposób bezprawny.

Na uznanie w aspekcie dbałości o bezpieczeństwo danych zasługuje propagowane przez RODO usuwanie wszelkich danych pozwalających na identyfikację użytkownika (o ile nie są one niezbędne), zastępowanie danych indywidualizujących sztucznie wygenerowanymi identyfikatorami oraz szyfrowanie danych tak, by tylko osoba upoważniona mogła je odczytać[36]. W kontekście profilowania, które współcześnie przybierają coraz bardziej inwazyjne formy, kluczowe znaczenie ma fakt, iż w przepisach pojawia się definicja legalna jako „dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na

[34] E. Bielak-Jomaa (red.), D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, LEX/el. 2018.
[35] K. Szymielewicz, W. Adamska, *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?*, Warszawa 2017, s. 20-22.
[36] Ibidem, s.22.

wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się" (art. 4 pkt 4 RODO). Uprawniony będzie miał możliwość zbierania danych wyłącznie w (z góry) określonych celach, a po zebraniu nie mogą być przetwarzane w innym celu bez dodatkowej zgody podmiotu danych, co w praktyce oznacza, że administrator nie może gromadzić więcej, niż faktycznie potrzebuje[37]. Z uwagi na główny cel RODO, jakim jest ochrona autonomii informacyjnej, administratorzy zostaną zmuszeni informować podmioty, których dane dotyczą, w sposób klarowny i zrozumiały o celach, czasie i sposobie przetwarzania. Co istotne z punktu zapewnienia realnej kontroli, administratorzy zostaną zobligowani do umożliwienia osobom uprawnionym realizacji ich prawa dostępu do informacji (wglądu w dane), sprostowania danych, ograniczenia przetwarzania, ale także prawo do usunięcia danych (tj. „prawo do bycia zapomnianym). Jak wskazuje art. 4 pkt 32: "Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia." Nie sposób nie zgodzić się z *K. Szymielewicz,* zdaniem której unormowanie w aspekcie zgody należy uznać za niższe aniżeli obowiązujące aktualnie w Polsce, ponieważ RODO nie nakazuje, by była ona wyrażona w sposób literalny[38].

Reasumując, na rzeczywiste osiągnięcie projektowanego ujednolicenia poziomu ochrony danych osobowych wpływać będzie jednak nie tylko stosowanie nowego prawa przez administratorów, organy nadzorcze i sądy, ale również zakres aktywności prawodawców krajowych[39]. Z uwagi na rozległy obszar wprowadzanych zmian zarówno ustawodawca krajowy, jak i administratorzy powinni jak najszybciej przeanalizować nowe mechanizmy ochrony danych i rozpocząć przygotowania do zapewnienia zgodności z unijnym aktem prawnym[40].

Podsumowanie

[37] K. Szymielewicz, W. Adamska, *op. cit.,* s. 20-22.
[38] Ibidem.
[39] Ibidem.
[40] E. Bielak-Jomaa (red.), D. Lubasz (red.), *op. cit.*, LEX/el.

Rozwój rynku nowych technologii polegający w dużej mierze na zbieraniu danych i dokonywaniu na nich operacji, szczególnie komercyjnych może stanowić istotne zagrożenie dla prawa dla prywatności użytkowników sieci. Europejski regulator dostrzegł wszechobecność i zasadne zagrożenia gromadzenia danych o użytkownikach Internetu poza ich kontrolą. Dotychczasowe regulację ochrony e-prywatności, choć miały wymiar fundamentalny, to powstały w diametralnie innych warunkach technologicznych, stąd wymóg aktualizacji, która przywróci im skuteczność na miarę współczesnych standardów społeczeństwa informacyjnego. Próbą odpowiedzi na wyzwanie w sposób zrównoważony, szanując różne modele biznesowe i tworząc równe warunki dla wszystkich przedsiębiorców jest RODO, aby skutecznie wypełnić w szerszej perspektywie lukę pomiędzy rzeczywistym, a przysługującym poziomem ochrony danych osobowych. W odpowiedzi na zaakcentowane na wstępie widmo orwellowskiej wizji, które sugeruje pogodzić się z końcem prywatności w świecie cyfrowym, autorka pragnie zaakcentować, iż szczególna ochrona prywatności jest dotąd celowa, dokąd jest ona warunkiem wolności.

Literatura

[1] Bielak-Jomaa E. (red.), Lubasz D.(red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* LEX/el. 2018.
[2] Czerniawski M*., Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych,* "Europejski Przegląd Sądowy" 05/2015.
[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, (Dz. Urz. UE L 281 z 23.11.1995, s. 31 z późn. zm.).
[4] **Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego, (***Dz. U. L 178, 17/07/2000 P. 0001 - 0016).*
[5] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej, (*Dz.* Urz. WE L 201 z 2002 *r.*, s. 37 ze zm.).
[6] Kamiński I. C., Warso Z., *Czy można zniknąć z Google'a? Orzeczenie Trybunału 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),* w: D. Bychawska-Siniarska, D. Głowacka, "Wirtualne media – realne problemy", Warszawa 2014.
[7] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „*Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*", KOM(2010) 609, Bruksela 2010.

[8] Mednis A., *Ochrona danych osobowych w konwencji Rady Europy o dyrektywie Unii Europejskiej*, PiP 1997, z. 6.
[9] Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 19 grudnia 1966 r. (Dz.U.1977.38.167).
[10] Orwell G. *Rok 1984*, Warszawa 2003.
[11] Powszechna Deklaracja Praw Człowieka z 10 grudnia 1948 r. http://ms.gov.pl/prawa_czl_onz/prawa_czlow_12.doc.
[12] Rezolucja Zgromadzenia Ogólnego ONZ A/RES/60/251 z dnia 15 marca 2006 r.
[13] 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, (DzU UE L 119/1 4.05.2016).
[14] Safjana M., *Prawo do ochrony życia prywatnego* [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, pod red. L. Wiśniewskiego, Warszawa 1997.
[15] Sieńczyło-Chlabicz J., *Ochrona prywatności osób powszechnie znanych w świetle Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności i Karty Praw Podstawowych* (w:) A. Wróbel (red.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009.
[16] Szewczyk H., *Ochrona dóbr osobistych w zatrudnieniu*, Kraków 2007, s. 53–113; J. Braciak, *Prawo do prywatności*, Warszawa 2004.
[17] Szymielewicz K., Adamska W., *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?,* Warszawa 2017.
[18] 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.
[19] 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.
[20] 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.
[21] Traktat Lizboński z Lizbonie z 13 grudnia 2007 r. (Dz. Urz. UE C 303 z 14.12.2007, s. 1 ze sprost.).
[22] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016.0.922 t.j.).
[23] Wujczyk M., *Prawo pracownika do ochrony prywatności*, Warszawa 2012.
[24] Wyrok TSUE w sprawie Google Spain SL i Google Inc. przeciwko Agencia Españo-la de Protección de Datos (AEPD) i Mario Costeja González z dnia 13 maja 2014 r., C131/12,
[25] Wyrok TSUE w sprawie Lindqvist z dnia 6 listopada 2003 r., C101/01, pkt 25,

Streszczenie

Rozwój rynku nowych technologii polegający w dużej mierze na zbieraniu danych i dokonywaniu na nich operacji, szczególnie komercyjnych może stanowić istotne zagrożenie dla prawa dla prywatności użytkowników sieci. W obliczu wyzwań jakie pociąga za sobą rozbudowana infrastruktura informatyczna autorka podejmuje się oceny prawnej kondycji prawa do prywatności w łączności elektronicznej w perspektywie dotychczasowych regulacji unijnych i orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. Analizie na tle

orzecznictwa poddane zostanie funkcjonowanie prawa do bycia zapomnianym, a także wybrane zagadnienia wdrażanych rozwiązań rozporządzenia 2016/679 (RODO).