Zeszyty Naukowe KUL 60 (2018), nr 1 (241)

Katarzyna Chałubińska-Jentkiewicz*

Bezpieczeństwo prawne danych osobowych w nowych warunkach cyfrowych

Rozwój technik informacyjno-komunikacyjnych (TIK) oraz szybki postęp związany z zastępowaniem nimi tradycyjnych, manualnych metod gromadzenia i utrwalania informacji stwarza nowe zagrożenie związane z ochroną prywatności jednostki i danych osobowych. W okresie rozwoju nowych technologii dane są wytworzone, przechowywane, przetwarzane za pomocą środków elektronicznych. Stosowanie na skalę masową TIK w różnych dziedzinach życia pociąga za sobą zmiany, które określane są pojęciem „rewolucji informacyjnej". Powszechność w dostępie do narzędzi informatycznych oraz sieci teleinformatycznych prowadzi do wzrostu ilości danych, które są łatwo utrwalane, gromadzone, wykorzystywane, archiwizowane, przesyłane, czyli przetwarzane. Zgodnie z art. 7 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1] przez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się za pośrednictwem systemów informatycznych. Jednak łatwość wytworzenia oraz przechowywania danych osobowych stanowi poważne ryzyko związane z naruszeniem praw osób, których dane te dotyczą, wpływa bezpośrednio na ich bezpieczeństwo, a tym samym na bezpieczeństwo jednostki. Należy podkreślić, że potrzeba prywatności jest jedną z ważniejszych potrzeb, którą należy chronić.

Gromadzenie danych przez podmioty zarówno prywatne, jak i publiczne może obniżać realne koszty, zwiększać szybkość i efektywność wykonywa-

* Dr hab. Katarzyna Chałubińska-Jentkiewicz – prof. ASzWoj; e-mail: kasiachalubinska@gmail.com

[1] Tj. Dz.U. z 2016 r., poz. 922, dalej „u.o.d.o".

nych przez te podmioty działań, lecz nie ograniczy to, ani nie zminimalizuje niebezpieczeństw związanych z naruszeniem prywatności przez osoby do tego nieupoważnione. Rozwój systemów informatycznych powoduje również wzrost kontaktów społecznych, ekonomicznych, czy też handlowych dokonywanych za pośrednictwem sieci teleinformatycznych. Sam przepływ informacji stał się bardzo szybki, a informacja stała się produktem o dużej wartości ekonomicznej. Wobec wzmożonego rozwoju TIK można przyjąć stanowisko, iż wiedza o obywatelach stała się bardziej dostępna, bowiem pozostawione w globalnej sieci internetowej informacje mówią wiele o ich preferencjach związanych między innymi z życiem codziennym.

W takich warunkach niezbędne stały się odpowiednie regulacje prawne gwarantujące ochronę dóbr osobistych, prawa do prywatności i ochronę danych osobowych. Potrzeba taka powstaje zarówno na szczeblu krajowym jak i międzynarodowym.

Definicja danych osobowych

W polskim systemie prawnym pojęcie „dane osobowe" po raz pierwszy pojawiło się w ustawie z dnia 29 września 1994 r. o rachunkowości[2], natomiast pierwsza definicja o charakterze legalnym zawarta została w ustawie o ochronie danych osobowych. Nawiązuje ona do definicji tego pojęcia zawartej w dyrektywie 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[3], zgodnie z którą za dane osobowe należy uznać wszelkie informacje odnoszące się do oznaczonej lub możliwej do oznaczenia osoby fizycznej. W pierwotnym brzmieniu za dane osobowe uważano każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby[4]. Jednak taka redakcja definicji spotkała się z krytyką nauki prawa i uznano ją za niezgodną z zapisami dyrektywy 95/46/WE, ponieważ za dane osobowe uznawała wyłącznie dane identyfikacyjne[5]. Obecnie w doktrynie prawa uważa się, że za dane osobowe powinny zostać uznane wszelkie informacje, jeżeli tylko możliwe jest ich odniesienie do konkretnej osoby[6]. W rozumieniu obowiązującej

[2] Tj. Dz.U. z 2016 r., poz. 1047.

[3] Dyrektywa 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 Nr 281, poz. 31).

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

[5] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2016, s. 77.

[6] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 383-384.

ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy czym osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne[7]. Wymienione numery identyfikacyjne to przykładowo: numer powszechnego elektronicznego systemu ewidencji ludności (PESEL), numer identyfikacji podatkowej (NIP), numer dowodu osobistego, czy też posiadanego paszportu. Z kolei czynniki, które można uznać za określające cechy osoby to między innymi cechy fizyczne, w tym wizerunek oraz cechy związane bezpośrednio z wyglądem (np. kolor oczu, włosów), fizjologiczne, czyli grupa krwi, kod DNA oraz dotyczące cech umysłu, kultury, mówiące o pochodzeniu, poglądach politycznych bądź przekonaniach religijnych[8]. Definicja danych osobowych wyróżnia trzy elementy: a) musi to być informacja, b) dotycząca osoby fizycznej, c) która jest zidentyfikowana lub możliwa do zidentyfikowania.

Pierwszy z tych elementów to informacja. Jej cechami charakterystycznymi są łatwość przekazu, niematerialny charakter, a także wykorzystywanie przez wiele osób w tym samym czasie[9]. Informacja może się odnosić do tego, co istniało, istnieje lub może zaistnieć. Jednak w kontekście definicji ochrony danych osobowych i użytego sformułowania „wszelkie informacje" zakres znaczeniowy tego pojęcia powinien obejmować nie tylko znaki językowe, ale również pozajęzykowe, do których można zaliczyć, zdjęcia, filmy, zarejestrowane głosy, a także tzw. dane biometryczne, cechy źrenicy, linie papilarne[10].

Drugim elementem definicji *danych osobowych* jest cecha, zgodnie z którą informacja *taka* odnosi się do osoby fizycznej. Użycie tego zwrotu podkreśla, że pojęcie to odnosi się do informacji związanych z konkretną osobą, jej stosunków osobistych, rzeczowych, życia zawodowego, prywatnego, wykształcenia, wiedzy, a nawet cech charakteru[11]. Informacja wtedy dotyczy osoby fizycznej, gdy komunikuje coś na jej temat i umożliwia ustalenie jej tożsamości. Można ją ustalić na podstawie imienia, nazwiska oraz innych informacji na przykład w postaci adresu zamieszkania, bądź któregokolwiek z numerów identyfikacyjnych (PESEL). Wówczas informacje te stanowią dane służące identyfikacji tej osoby.

---

[7] Art. 6 ust. 1 i 2 u.o.d.o. CO TO WNOSI? *Przybliżenie przesłanki podmiotowej definicji danych osobowych*

[8] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, s. 331.

[9] M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego,* Warszawa 2015, s. 46.

[10] P. Barta, P. Litwiński, *Ustawa…*, s. 77.

[11] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…,* s. 304.

Na kolejny element *wskazanej powyżej* definicji składa się sformułowanie „osoba fizyczna musi być zidentyfikowana lub możliwa do zidentyfikowania". Osobą, którą można zidentyfikować jest osoba, której tożsamość może być określona w sposób bezpośredni lub pośredni, w szczególności – jak wyżej wspomniano – przez powołanie się na jeden z numerów identyfikacyjnych, bądź też jeden lub kilka czynników specyficznych, które określają cechy zarówno fizyczne, jak i fizjologiczne, umysłowe, czy ekonomiczne[12]. W ustawie zdefiniowano jedynie „osobę możliwą do zidentyfikowania".

Wydaje się, że w tym przypadku pomocne może okazać się rozróżnienie zawarte w art. 6 ust.2 u.o.d.o., zgodnie z którym jeśli osobą możliwą do zidentyfikowania jest osoba, której tożsamość można ustalić, to osobą zidentyfikowaną jest osoba o ustalonej już tożsamości. W art. 6 ust. 3 u.o.d.o. ustalono, iż informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Można zatem wnioskować, że nie mają charakteru danych osobowych informacje, przy których ustalenie tożsamości osoby wymaga nieproporcjonalnie dużego nakładu finansowego, czasu, czy pracy. Jednak na obecnym poziomie rozwoju TIK, kryterium kosztów może tracić na znaczeniu, a ustalenie czy mamy do czynienia z nadmiernymi kosztami, czasem bądź działaniami związanymi z pozyskiwaniem takich informacji powinno być rozpatrywane indywidualnie, w zależności od sytuacji związanej z przetwarzaniem określonej informacji. Bowiem ta sama informacja związana z ustaleniem tożsamości osoby, która dla jednego podmiotu jest szybka do uzyskania, dla innego podmiotu może wiązać się z działaniami nieproporcjonalnymi[13].

Dane osobowe dzielimy na dwie grupy: dane identyfikujące oraz dane wrażliwe – sensytywne. Według E. Kuleszy dane wrażliwe „są szczególnie chronione i ustawa o ochronie danych osobowych zezwala na ich ujawnienie tylko w szczególnych przypadkach"[14]. Zostały one wymienione enumeratywnie w u.o.d.o. w formie katalogu zamkniętego[15]. Wyróżnione je na tle pozostałych danych osobowych przyjmując, że dotyczą one sfer należących do prywatności, a właściwie intymności osoby fizycznej[16], a ich ujawnienie może wiązać się z poczuciem zagrożenia oraz niebezpieczeństwem wywołania sytuacji dyskryminujących związanych między innymi z zatrudnieniem[17]. Przeciwieństwem danych wrażliwych są dane zwykłe. Nie zostały one, wymienione w ustawie

[12] P. Barta, P. Litwiński, *Ustawa…*, s. 87.

[13] Ibidem, s. 311.

[14] E. Kulesza, *Zdrowie: zasada i wyjątki*, Rzeczpospolita z 04.05.2000 r. http://archiwum.rp.pl/artykul/274696-Zdrowie:-zasada-i-wyjatki.html [dostęp 13.02.2017].

[15] Art. 27 ust. 1 u.o.d.o.

[16] P. Barta, P. Litwiński, *Ustawa…*, s. 87.

[17] P. Barta, P. Litwiński, *Ustawa…*, s. 324.

i należy do nich zaliczyć wszystkie dane, które nie zostały uznane za dane wrażliwe.

Na system ochrony danych osobowych wpływały liczne nowelizacje ustawy. Należy tu zwrócić uwagę na nowelizację u.o.d.o., którą wprowadziła od dnia 1 stycznia 2015 r. ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[18]. Dodanie w art. 43 ustawy o ochronie danych osobowych przepisu wprowadzającego nowe, kompleksowe zwolnienie z obowiązku zgłoszenia do rejestracji GIODO zbiorów, w których nie będą przetwarzane dane określone w art. 27 ust. 1 tej ustawy (tzw. dane szczególnie chronione), prowadzonych przez administratorów danych, którzy powołali i zgłosili GIODO Administratora Bezpieczeństwa Informacyjnego (ABI), jest skorelowane ze zmianą przepisów dotyczących administratora bezpieczeństwa informacji. Rejestracja zbiorów danych osobowych istniejąca bez ważnych zmian od 1997 r. miała służyć ucywilizowaniu tej sfery życia społecznego, jednak z biegiem czasu jej znaczenie malało i w końcu stała się jedynie pewnym obowiązkiem ewidencyjnym ciążącym na przedsiębiorcach[19]. Kompleksowe zwolnienie z obowiązku rejestracyjnego administratora danych, który powołał i zgłosił do rejestracji GIODO ABI, z jednoczesną zmianą przepisów odnoszących się do jego zadań i usytuowania organizacyjnego w jednostce administratora danych to istotna nowelizacja ustawy, jednak należy podkreślić, że zwolnienie z obowiązku rejestracyjnego nie dotyczyło zbiorów zawierających dane wymienione w art. 27 ust. 1 u.o.d.o., ponieważ w ramach rejestracji uregulowanej w polskiej ustawie wprowadzony został obowiązek kontroli wstępnej (*prior checking*) przetwarzania tych danych, tj. operacji, które mogą stwarzać zagrożenie praw i wolności podmiotu danych (art. 20 dyrektywy 95/46/WE). Ze względu na wymogi prawa unijnego w zakresie dopuszczalności kompleksowego zwolnienia administratorów danych z obowiązku rejestracji zbiorów wprowadzono nowe przepisy dotyczące statusu i zadań ABI, które zapewnić miały zachowanie standardów wyznaczonych dyrektywą 95/46/WE, tj.: niezależność w wykonywaniu zadań, obowiązek zapewnienia stosowania w jednostce organizacyjnej przepisów o ochronie danych osobowych, w szczególności przez przyznanie kompetencji do kontroli wewnętrznej w zakresie przestrzegania przepisów o ochronie danych osobowych, a także prowadzenie wewnętrznego rejestru zbiorów danych.

Zatem kolejnym novum była kompleksowa regulacja związana z administratorem bezpieczeństwa informacji (ABI), w szczególności w zakresie określenia jego zadań. Po znowelizowaniu ustawy instytucja ABI otrzymała ustawowo określone prawa i obowiązki, a także pozycję prawną w organiza-

[18] Dz. U. z 2014 r., poz. 1662 z późn. zm.

[19] P. Barta, P. Litwiński, *Ustawa*…, s. 8.

cji[20]. Następną zmianą były regulacje związane z transgranicznym przepływem danych stanowiące pewnego rodzaju hamulec dla rozwoju dziedziny związanej z przekazywaniem danych osobowych do państw trzecich – czyli poza granice Unii Europejskiej. Mimo, że dyrektywa 95/46/WE przewidywała instrumenty związane z tym procederem, to jednak polski ustawodawca w pracach nad pierwotnym tekstem u.o.d.o. ich nie uwzględnił. Dopiero wskazana powyżej zmiana wprowadziła do polskiego porządku prawnego podstawy prawne do przekazywania danych do państw trzecich oraz tzw. „standardowe klauzule umowne ochrony danych osobowych" zatwierdzane przez Komisję Europejską na podstawie wyżej wspomnianej dyrektywy[21].

W dniu 25 stycznia 2012 r. Komisja *Europejska* opublikowała obszerny pakiet ustawodawczy mający na celu nowelizację przepisów UE dotyczących ochrony danych *osobowych*. Reforma miała na celu lepsze zapewnienie ochrony danych osobowych w UE, przy jednoczesnym zwiększeniu przysługującej użytkownikom kontroli ich własnych danych i zredukowaniu kosztów ponoszonych przez przedsiębiorców[22]. Nowelizacja była uzasadniana faktem, iż technologiczny postęp i globalizacja diametralnie zmieniły sposób gromadzenia danych, a także sposób uzyskiwania do nich dostępu oraz ich wykorzystywania[23]. Zmiany w systemie ochrony danych osobowych UE miały wzmocnić zaufanie konsumentów do usług online, stymulując jednocześnie wzrost zatrudnienia i innowacyjności w Europie. Pakiet ten obejmował politykę komunikacji w dziedzinie głównych celów politycznych reformy, wniosek w sprawie ogólnego rozporządzenia służącego modernizacji zasad zapisanych w dyrektywie o ochronie danych z 1995 r. oraz wniosek w sprawie szczegółowej dyrektywy w sprawie przetwarzania danych osobowych w obszarze współpracy policyjnej i sądowej w sprawach karnych. W grudniu 2015 r. Parlament – na szczeblu Komisji oraz Rada – na szczeblu ambasadorów osiągnęły porozumienie w sprawie nowych zasad ochrony danych. Nowe zasady zostały opublikowane w kwietniu 2016 r. i zaczną obowiązywać od maja 2018 r[24]. Zasady te określają następujące akty prawne: 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)[25]; Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony

[20] Ibidem, s. 8.

[21] Ibidem, s. 9.

[22] Agencja Praw Podstawowych UE, *Podręcznik …*, s. 21.

[23] http://www.europarl.europa.eu/atyourservice/pl/displayFtu.html?ftuId=FTU_5.12.8.html,[dostęp 11.03.2017r.].

[24] http://www.giodo.gov.pl/1520142/id_art/4587/j/pl/, [dostęp 11.03.2017 r.].

[25] Dz. Urz. UE, L 119, 04.05.2016 r., s. 1.

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 uchylająca decyzję ramową Rady 2008/977/WSiSW[26].

Najważniejsze propozycje zmian, jakie znalazły się w ogólnym rozporządzeniu o ochronie danych będą obejmowały następujące rozwiązania: 1) likwidację wymogów administracyjnych, takich jak obowiązek zgłaszania zbiorów danych do rejestracji organom nadzorującym ochronę danych – zamiast tego przewiduje się większą odpowiedzialność podmiotów przetwarzających dane osobowe (przedsiębiorcy i organizacje przetwarzające dane osobowe muszą powiadamiać krajowy organ nadzorczy o zasadniczych naruszeniach ochrony danych, najlepiej w ciągu 24 godzin)[27]; 2) administratorzy mają kontaktować się tylko z jednym krajowym organem nadzorującym ochronę danych, w tym państwie członkowskim UE, w którym mieści się główna siedziba przedsiębiorcy. Także osoby fizyczne będą mogły kontaktować się z organem odpowiedzialnym za ochronę danych w swoim państwie, nawet w przypadku, jeżeli ich dane są przetwarzane przez przedsiębiorstwo bądź instytucje mające siedzibę poza Unią Europejską. Zgoda na przetwarzanie danych ma być wyraźna, a nie domniemana[28]; 3) „prawo do bycia zapomnianym" ma pomóc podmiotom w zarządzaniu ryzykiem związanym z ochroną danych przetwarzanych *on line*: osoby fizyczne będą miały możliwość usunięcia swoich danych, w przypadku nieuzasadnionej podstawy do ich zachowania; 4) unijne przepisy muszą obowiązywać w przypadku, gdy dane osobowe są przetwarzane za granicą przez przedsiębiorców prowadzących działalność na rynku UE i oferujących swoje usługi obywatelom UE[29]; 5) krajowe, niezależne organy, które nadzorują ochronę danych będą wzmocnione, aby mogły skuteczniej egzekwować unijne przepisy na terytorium kraju. Zostaną w związku z tym upoważnione do nakładania kar na przedsiębiorców naruszających unijne przepisy o ochronie danych osobowych[30]. Zmiany obejmują także potrzeby zapobiegania przestępstwom, wykrywania ich, prowadzenia dochodzeń w ich sprawie i ich ścigania oraz powiązanych działań wymiaru sprawiedliwości w sprawach karnych. W dyrektywie tej zasady ogólne ochrony danych będą zastosowane w odniesieniu do współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych. Przepisy dyrek-

[26] Dz. Urz. UE, L 119, 04.05.2016 r., s. 89.

[27] *Raport o ochronie danych osobowych GIODO,* http://www.giodo.gov.pl/487/id_art/9146/j/pl/, [dostęp 11.03.2017 r.], s. 4.

[28] Ibidem, s. 4.

[29] Ibidem, s. 4.

[30] Ibidem, s. 5.

tywy będą miały zastosowanie do przekazywania danych zarówno w kraju, jak i do transferów transgranicznych[31].

W czasie trwania dwuletniego okresu przejściowego *vacatio legis* państwa członkowskie mają obowiązek dostosowania krajowych przepisów do nowych, zreformowanych i uaktualnionych zasad ochrony danych osobowych. W praktyce oznacza to zarówno konieczność zmiany przepisów polskiej ustawy o ochronie danych osobowych (nie będzie ona mogła powtarzać regulacji ujętych w unijnym rozporządzeniu) oraz zrewidowanie i ewentualne przekształcenie przepisów dotyczących danych osobowych, zawartych w innych aktach prawnych[32].

Podsumowując należy zaznaczyć, że zarówno prawo krajowe, jak i regulacje na poziomie UE odnoszące się do ochrony danych osobowych wciąż stanowią obszar intensywnych regulacji. Pomimo dorobku orzeczniczego oraz doktryny ukształtowanej na przestrzeni dwóch dekad ustawodawca dostrzega nieustającą potrzebę zmian w ochronie danych osobowych, związaną z postępującym procesem informatyzacji, cyfryzacji i rozwoju TIK. Zmiany te wydają się niezbędne dla zapewnienia bezpieczeństwa danych osobowych przed ich nieuprawnionym przetwarzaniem i wykorzystywaniem.

Ochrona danych osobowych w nowych warunkach cyfrowych – wybrane zagadnienia

Skala pozyskiwania, gromadzenia oraz wymiany danych osobowych osiągnęła niezwykłą intensywność. Z jednej strony jest to możliwe właśnie dzięki nowym, ciągle rozwijającym się technologiom, z których korzystają podmioty władzy publicznej oraz prywatni przedsiębiorcy. Z drugiej strony, same osoby fizyczne biorą udział w procesie udostępniania wielu informacji ze swojego życia prywatnego, co powoduje, że stają się one publicznie dostępne i łatwe w procesie przetwarzania. Procesom tym sprzyja przede wszystkim szybki rozwój usług *on line*. Dane udostępniane w sieci teleinformatycznej mogą jednak stanowić źródło zagrożeń dla bezpieczeństwa informacyjnego. Korzystanie z nowoczesnych usług związanych z nowymi warunkami cyfrowymi nierozerwalnie wiąże się z udostępnianiem danych osobowych.

Każda czynność, związana z usługami świadczonymi elektronicznie, korzystanie z poczty elektronicznej, wyszukiwarek oraz portali społecznościowych wiąże się z udostępnianiem informacji. Należy przy tym zauważyć, że obecny poziom rozwoju technologicznego pozwala na identyfikację konkretnej osoby

[31] Ibidem, s. 5.

[32] http://www.giodo.gov.pl/1520142/id_art/4587/j/pl/, [dostęp 11.03.2017 r.].

z zastosowaniem odpowiednich środków technicznych mając w posiadaniu tylko szczątkowe informacje dotyczące takiej osoby.

Regulamin serwisu Facebook

W związku z niezmienną popularnością, jaką cieszy się Internet w gospodarstwach domowych, a co za tym idzie zwiększającą się liczbą użytkowników globalnej sieci, coraz bardziej powszechne staje się korzystanie z tzw. portali społecznościowych, a w szczególności dotyczy to serwisu Facebook. M. Pamuła definiuje to miejsce jako rodzaj społeczności internetowej, w której internauci mogą zaspokoić swoje naturalne potrzeby kontaktów z ludźmi, zdobywania doświadczeń, uzyskiwania informacji, jak i poszerzania zainteresowań[33]. Dotychczas serwisy społecznościowe służyły ich użytkownikom jako sposób spędzania wolnego czasu, gdzie podejmuje się wiele interaktywnych czynności takich jak autoprezentacja, poszukiwanie znajomych, tworzenie grup lub forum dyskusyjnego, wymiana informacji oraz zdjęć z innymi użytkownikami. Stanowią rodzaj usług www, w ramach których treści cyfrowe poddane udostępnieniu i ewentualnej wymianie tworzą sami internauci. Dlatego w tym przypadku tak ważna w tym obszarze jest kwestia ochrony prywatności oraz danych osobowych przetwarzanych przez portale społecznościowe. Zatem portal społecznościowy jest to rodzaj społeczności internetowych, które tworzone są lub współtworzone przez grupę internautów skupiającą osoby o podobnych zainteresowaniach lub znających się nawzajem[34]. M. Juza uznała natomiast, że serwisy społecznościowe dają możliwość zaprezentowania innym internautom własnej osoby oraz konsolidacji sieci kontaktów z innymi[35]. Coraz częściej jednak serwisy społecznościowe stają się miejscem świadczenia różnego typu usług, gdzie istnieje łatwa możliwość dostępu do konsumenta z przekazem promocyjnym własnej działalności. To także miejsce przekazu informacji zbliżone rodzajem udostępniania treści do prasy. W konsekwencji należy przyjąć, że serwisy społecznościowe to obszar szerokiej (bowiem globalnej) aktywności użytkowników wirtualnej rzeczywistości, które ze względu na cel działania

[33] M. Pamuła, *Serwis internetowy do komunikacji wewnątrz grup*, praca magisterska, Uniwersytet Warszawski, Wydział Matematyki, Informatyki i Mechaniki, Warszawa 2007, s. 9, http://students.mimuw.edu.pl/SR/prace- mgr/pamula/pamula2007-08-09.pdf, [dostęp 18.04.2017 r.].

[34] I. Gmińska, A. Kwiatkowski, *Ochrona danych osobowych na portalach społecznościowych na przykładzie Facebooka,* Zeszyty Naukowe Uczelnianej Rady Doktorantów Uniwersytetu Kazimierza Wielkiego, t. 2, nr 1, s. 34,. Bydgoszcz 2014.

[35] M. Juza, *Sieć społeczna - nowoczesne plemię. Serwis www.orkut.com jako przykład możliwości Internetu w upowszechnianiu sieciowej formy porządku społecznego*, [w:] *Wielka sieć. E-seje z socjologii Internetu*, J. Kurczewski (red.), Warszawa 2006, s. 237.

przyjmują postać środków społecznego przekazu, komunikacji prywatnej jak i świadczenia usług drogą elektroniczną o charakterze gospodarczym. To także miejsce pozyskiwania informacji prywatnej oraz obszar działań związanych z przestępczością w zakresie informacji.

Każdy kto, rejestruje się na portalach społecznościowych, decyduje się na udostępnianie swoich danych osobowych właścicielowi serwisu. Następuje to poprzez wyrażenie zgody na przetwarzanie danych osobowych. Zgodnie z wymogami dotyczącymi świadczenia usług drogą elektroniczną każdy z portali społecznościowych posiada regulamin korzystania z serwisu. Regulamin Facebooka[36] zawiera oświadczenie dotyczące praw i obowiązków stanowiący załącznik do umowy, którą musi zaakceptować każdy nowo zarejestrowany użytkownik portalu. Jest to dokument szczególnie istotny gdyż zawiera przepisy regulujące bezpośrednio prawa, jakie przysługują Facebookowi odnośnie zamieszczanych na serwisie treści i danych użytkowników. Podkreślić należy, że obowiązki te nie wynikają z jednolitych i skoordynowanych ustaleń na poziomie międzynarodowym.

W pierwszej kolejności należy przybliżyć „regulaminowe" definicje pojęć: treść, informacja oraz dane. Przez treści rozumie się wszystko to, co użytkownik serwisu zamieszcza na stronie Facebooka, a co nie zawiera się w terminie „informacja". Ta z kolei oznacza „dane, zdarzenia i inne informacje na temat użytkownika, w tym czynności wykonywane przez użytkowników i osoby niebędące użytkownikami, które korzystają z serwisu Facebook". Dane są natomiast pojęciem szerszym. Obejmują bowiem wszelkie dane włącznie z treściami i informacjami użytkownika, które on i inni użytkownicy mogą uzyskać z lub przesłać do serwisu Facebook[37]. W polityce serwisu Facebook zawarty został postulat odnoszący się do prywatności użytkowników, wskazujący na to, iż jej przestrzeganie jest dla serwisu bardzo ważną kwestią. Zostały w tym celu sformułowane zasady wykorzystania danych, z których użytkownik serwisu może czerpać wiedzę odnoszącą się do tego, jak korzystać z serwisu, a także w jaki sposób zbierane i wykorzystywane są dotyczące go dane[38].

Rejestracja w serwisie Facebook polega na podaniu informacji, do których należą: imię i nazwisko, adres poczty elektronicznej, data urodzenia, płeć, a także, w niektórych przypadkach numer telefonu. Podanie tych danych ma na celu łatwiejsze zidentyfikowanie osoby przez rodzinę bądź znajomych.

Podczas dalszego korzystania z serwisu użytkownik ma możliwość udostępniania w nim kolejnych informacji, związanych m. in. z wydarzeniami, w których brał udział on lub jego znajomi. Na szczególną uwagę zasługuje fakt, iż informacje o użytkowniku Facebook może czerpać nie tylko bezpośrednio

[36] http://www.facebook.com/legal/terms, [dostęp 18.04.2017 r.].
[37] http://www.facebook.com/legal/terms, [dostęp 18.04.2017 r.].
[38] I. Gmińska, A. Kwiatkowski, *Ochrona danych osobowych* …, s. 37.

od osoby zainteresowanej, ale także od innych użytkowników, którzy zamieścili je w serwisie, nawet bez wiedzy czy zgody tej osoby. Kolejnymi typami źródeł, z których Facebook może czerpać informacje są: 1) informacje o sieci i połączeniu, takie jak adres IP, a także numer telefonu komórkowego, dane dotyczące systemu operacyjnego, lokalizacji, odwiedzanych stron. Facebook czerpie je każdorazowo po zalogowaniu się do serwisu, niezależnie czy jest to dokonywane za pośrednictwem komputera stacjonarnego, laptopa czy też telefonu komórkowego; może otrzymać te informacje za pomocą systemu GPS; 2) dane pozyskiwane poprzez gry, witryny, aplikacje, które działają w oparciu o platformę Facebooka, a także za pomocą plików cookie; 3) informacje uzyskiwane poprzez odbieranie wiadomości czy wyszukiwanie osób, stron, a także dokonywanie zakupów w serwisie[39].

Informacja raz rozpowszechniona za pośrednictwem serwisu Facebook może zostać skopiowana i przekazana przez każdego, kto tylko miał do niej dostęp. Istnieją jednak informacje, które zawsze są dostępne publicznie. Należą do nich: imię, nazwisko, zdjęcia profilowe oraz zdjęcia w tle, płeć, nazwa użytkownika oraz jego identyfikator. Jeżeli użytkownik nie zgadza się na ujawnienie swojego autentycznego imienia i nazwiska usługodawca może usunąć konto. Regulamin portalu społecznościowego Facebook pozwala użytkownikowi serwisu na wykorzystywanie pozyskanych wcześniej od innych użytkowników informacji do różnych celów. Do takich celów należą m.in. informowanie użytkownika o zbliżających się wydarzeniach w pobliżu miejsca jego pobytu czy usprawniania już istniejących lub nowo tworzonych usług. Z drugiej jednak strony, pozyskane informacje mogą zostać wykorzystane do celów wynikających ze współpracy z partnerami, reklamodawcami i innymi przedsiębiorstwami działającymi na rynku. *Regulamin ten pozwala również na udostępnienie informacji dostawcom usług*[40].

Rejestracja w serwisie jest równoznaczna z akceptacją jego regulaminu. Oznacza to automatyczne zezwolenie na wykorzystywanie informacji o użytkownikach przez Facebook do własnych celów. W regulaminie istnieją dosyć nieostre sformułowania odnoszące się do sytuacji, w których serwis może informacje o użytkownikach udostępniać podmiotom trzecim. Wskazują, iż sytuacja taka następuje w trzech wypadkach: 1) gdy otrzymali zezwolenie użytkownika, 2) gdy poinformowali o tym użytkownika (na przykład w regulaminie), 3) gdy usunięto z udostępnianych informacji imię i nazwisko użytkownika oraz dane umożliwiające jego identyfikację.

Uprawnieniem wzbudzającym najwięcej kontrowersji jest udzielenie przez użytkownika właścicielowi serwisu licencji pozwalającej na wykorzystanie dowolnych treści objętych prawem własności intelektualnej użytkownika, które zostały opublikowane przez niego w serwisie Facebook. Licencja ta jest

[39] http://www.facebook.com/legal/terms, [dostęp 18.04.2017 r.].

[40] http://www.facebook.com/legal/terms, [dostęp 18.04.2017 r.].

niewyłączna, zbywalna, bezpłatna i obejmuje prawo do udzielenia sublicencji oraz ma charakter globalny[41].

W pewnym stopniu na zasady regulacji usług świadczonych on line wpływają przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[42], która stanowi *lex specialis* do u.o.d.o. w warunkach świadczenia usług on line oraz poddaje ochronie wszelkie dane osobowe, nawet te, które nie są zebrane w zbiorach, tak jak to reguluje u.o.d.o.

Zgodnie z art. 18 ust. 1 u.ś.u.d.e „Usługodawca może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego"[43]. Proces przetwarzania danych może nastąpić wówczas, gdy osoba będzie o tym poinformowana i gdy zostanie określony dokładny cel przetwarzania danych. Usługodawca może przetwarzać dane usługobiorcy takie jak: nazwisko i imiona, numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, jeżeli jest inny niż adres zameldowania, dane służące do weryfikacji podpisu elektronicznego usługobiorcy oraz adresy elektroniczne usługobiorcy.

Należy zaznaczyć, że usługodawca w celu realizacji umowy może przetwarzać również inne dane osobowe niż wymienione powyżej ze względu na właściwość świadczonej usługi lub sposobu jej rozliczania. Powinien jednak zaznaczyć, że dane te będą niezbędne do świadczenia usługi drogą elektroniczną. Jeżeli usługobiorca wyrazi zgodę usługodawca może przetwarzać dane osobowe dla celów m.in. reklamowych czy badania rynku[44]. Usługodawca nie może przetwarzać danych osobowych usługobiorcy po zakończeniu korzystania z usługi świadczonej drogą elektroniczną. Jednak ustawodawca dopuszcza takie przetwarzanie po zakończeniu korzystania z usługi świadczonej drogą elektroniczną co do danych, które są: 1) niezbędne do rozliczenia usługi oraz dochodzenia roszczeń z tytułu płatności za korzystanie z usługi; 2) niezbędne do celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, za zgodą usługobiorcy; 3) niezbędne do wyjaśnienia okoliczności niedozwolonego korzystania z usługi, 4) dopuszczone do przetwarzania na podstawie odrębnych ustaw lub umowy.

Należy podkreślić, że u.ś.u.d.e. stanowi implementację dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektó-

[41] I. Gmińska, A. Kwiatkowski, *Ochrona danych osobowych* …, s. 38.

[42] Tj. Dz.U. z 2017 r. poz.1219, dalej u.ś.u.d.e.

[43] Art. 19 ust. 2 pkt 2 u.ś.u.d.e.

[44] http://www.kancelarialebek.pl/index.php/2016/04/01/ochrona-danych-osobowych-w-swietle-ustawy-o-swiadczeniu-uslug-droga-elektroniczna/, [dostęp 28.04.2017 r.].

rych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[45] i odnosi się do usług świadczonych na wspólnym rynku UE. W tym sensie zasady korzystania z danych osobowych, o których mowa w u.ś.u.d.e., w ramach serwisu Facebook nie mają znaczenia.

Należy także zaznaczyć, że serwis społecznościowy jest prowadzony przez Facebook Inc. z siedzibą w USA. Polska spółka Facebook Poland sp. z o.o. jest natomiast spółką zależną od Facebook Global Holdings II LLC, która również ma siedzibę w USA. Facebook Poland to przedsiębiorstwo świadczące usługi z zakresu doradztwa marketingowego na rzecz podmiotów z terytorium Polski. Poza tym, polski oddział zajmuje się badaniem rynku opinii publicznej, współpracą z agencją reklamową oraz działalnością związaną z reprezentowaniem mass mediów. Polskich użytkowników, którzy zakładają konto na tym portalu, wiąże umowa z Facebook Ireland Ltd. Przy czym użytkownik z obszaru Unii Europejskiej musi liczyć się z koniecznością zaakceptowania jurysdykcji USA.

Korzystanie z portali społecznościowych niesie ze sobą wiele korzyści oraz możliwości, ale jednocześnie nie jest to miejsce wolne od zagrożeń, które znajdują swoje źródło w niewłaściwym postępowaniu z danymi osobowymi. Należy przy tym zauważyć, że kwestia ta nie została dostatecznie rozstrzygnięta na poziomie międzynarodowym a charakter globalny sieci wciąż stanowi istotny problem w ochronie danych osobowych jej użytkowników.

Orzecznictwo Europejskiego Trybunału Sprawiedliwości

Na konieczność podjęcia działań koordynacyjnych w przestrzeni ochrony danych osobowych wskazuje ostatnie orzecznictwo Europejskiego Trybunału Sprawiedliwości (ETS). Jednym z ważniejszych spraw z zakresu ochrony danych osobowych jaką na przestrzeni ostatnich lat rozpatrywał Trybunał Sprawiedliwości Unii Europejskiej jest sprawa Google Spain[46]. W wyroku Trybunał odniósł się do dwóch zasadniczych kwestii. Po pierwsze, do kwestii tzw. „prawa bycia zapomnianym", po drugie, do zagadnienia związanego z zakresem terytorialnym stosowania przepisów Dyrektywy 95/46/WE[47]. W 2010 r. obywatel Hiszpanii Mario Costeja González wniósł do hiszpańskiej agencji ochrony danych skargę

[45] DZ.U. UE L 178, 17.07.2000, s.1-16.

[46] Wyrok Europejskiego Trybunału Sprawiedliwości w sprawie C-131/12 Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González z dnia 13 maja 2012 r., http://curia.europa.eu/juris/liste.jsf?language=pl&num=C-131/12, [dostęp 28.04.2017 r.].

[47] M. Czerniawski, *Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa TSUE*, s. 93 [w:] *Polska i Europejska ochrona danych osobowych*, E. Bielak-Jomaa, D. Lubasz (red.), Warszawa 2016, s. 33.

skierowaną przeciwko wydawcy publikowanego w Hiszpanii, wysokonakładowego dziennika oraz przeciwko spółkom Google Spain i Google Inc. González wskazał, że internauta wprowadzając jego dane w postaci imienia i nazwiska do wyszukiwarki „Google Search" na liście wyników wyszukiwania *widzi* link do stron dziennika „La Vanguardia" z zaznaczonymi datami. Był to link do stron, gdzie widniało ogłoszenie związane z licytacją nieruchomości zajętej przez zakład ubezpieczeń społecznych w związku z niezapłaconymi przez Gonzáleza należnościami na rzecz ubezpieczyciela[48].

Skarga obywatela hiszpańskiego dotyczyła nakazania spółce La Vanguardia usunięcia bądź zmiany tych stron w ten sposób, by nie były na nich widoczne jego dane osobowe. Skarżący uzasadniał żądanie faktem, że sprawa zaległości i zajęcia jego nieruchomości została wyjaśniona i zakończona.

Hiszpański organ oddalił skargę w zakresie dotyczącym dziennika w uzasadnieniu podając, że wydawca opublikował informacje działając zgodnie z prawem. Skargę jednak uwzględniono w zakresie *odpowiedzialności* Google Spain i Google Inc. Agencja Española de Protección de Datos, zwróciła się do spółek o przyjęcie niezbędnych środków służących usunięciu danych skarżącego oraz uniemożliwienie dostępu do tych danych. Spółki Google wniosły do Audiencia Nacional sprawującego władzę sądowniczą nad całym terytorium Hiszpanii sądu I instancji lub apelacyjnego z siedzibą w Madrycie dwie skargi o stwierdzenie nieważności wydanej przez AEPD decyzji[49]. Z kolei sąd ten skierował do ETS szereg pytań prejudycjalnych, czyli pytań, które pozwalają sądom państw członkowskich, w ramach rozpatrywanego przez nie sporu, zwrócić się do Trybunału z pytaniem o wykładnię prawa Unii *Europejskiej. Podkreślić należy, iż wydane w tym trybie orzeczenie wiąże inne sądy krajowe,* które spotkają się z identycznym problemem[50]. Sentencja wyroku ETS w sprawie Google Spain wskazuje, że operator wyszukiwarki internetowej odpowiada za przetwarzanie danych osobowych, pojawiających się na stronach internetowych publikowanych przez osoby trzecie, co oznacza, że w sytuacji, gdy na liście wyników związanych z wyszukiwaniem polegającym na wpisaniu do wyszukiwarki imienia i nazwiska konkretnej osoby wyświetlany jest link do strony internetowej zawierającej informacje o tej osobie, przysługuje jej prawo zwrócenia się do operatora o usunięcie tego adresu z listy wyników wyszukiwania, gdy operator nie nada dalszego biegu takiemu wnioskowi, osoba, której dane są nadal przetwarzane, może zwrócić się do odpowiednich organów z wnioskiem o usunięcia tego adresu internetowego. Trybunał uznał m.in., iż działalność prowadzona przez

[48] Trybunał Sprawiedliwości Unii Europejskiej KOMUNIKAT PRASOWY nr 70/14, s. 1, Luksemburg, 13 maja 2014 r., https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070pl.pdf, [dostęp 28.04.2017 r.].

[49] Ibidem, s. 2.

[50] Ibidem, s. 4.

wyszukiwarki internetowe w sytuacji, gdy takie informacje zawierają dane osobowe powinna być uznana za „przetwarzanie danych osobowych" w rozumieniu art. 2 lit. b) dyrektywy *95/46/WE. W wyroku ETS przesądzono, iż w tym konkretnym przypadku operatora wyszukiwarki internetowej należy traktować jako „administratora" odpowiedzialnego za przetwarzanie danych osobowych*[51]. Rewolucyjny wyrok odnoszący się do sprawy Google Spain zmienił status jednostki w warunkach zagrożeń związanych z jego danymi osobowymi.

Innym wyrokiem, który wpłynął na zmianę zakresu odpowiedzialności usługodawców on line jest wyrok w sprawie Weltimmo[52], którego podstawową kwestią było ustalenie prawa właściwego wewnątrz Unii Europejskiej, a odnoszącego się do zakresu terytorialnego działania organów nadzorczych na Słowacji oraz na Węgrzech.

Firma Weltimmo, będąca spółką zarejestrowaną na Słowacji, prowadziła stronę internetową poświęconą płatnym ogłoszeniom o nieruchomościach położonych na Węgrzech. W ramach swojej działalności, przetwarzała dane osobowe ogłoszeniodawców. Wielu ogłoszeniodawców zwracało się do Weltimmo, za pośrednictwem poczty elektronicznej, o usunięcie po miesiącu ich ogłoszeń oraz dotyczących ich danych osobowych. Słowacki przedsiębiorca tego jednak nie zrobił, a w związku z brakiem wpływów za wystawione faktury Weltimmo przekazał dane osobowe ogłoszeniodawców agencjom zajmującym się ściąganiem wierzytelności. Rozpoznający spór w sprawie kasacyjnej Sąd Najwyższy Węgier skierował do ETS pytanie, czy w takim stanie rzeczy dyrektywa zezwala, aby węgierski organ nadzorczy zastosował krajową – węgierską – ustawę, która została przyjętą na podstawie dyrektywy *95/46/WE* [53]. ETS stwierdził, że uregulowania państwa członkowskiego, które dotyczą ochrony danych powinny być stosowane także do spółki zagranicznej, która prowadzi w tym państwie swoją działalność. W dyrektywie prawodawca europejski przyjął, że każde państwo członkowskie ma obowiązek wyznaczyć co najmniej jeden organ władzy publicznej, który będzie odpowiedzialny za kontrolę stosowania przepisów krajowych przyjętych przez państwa członkowskie na mocy tej dyrektywy. Trybunał uznał, że „Organy te posiadają kompetencje związane z wykonywaniem na terytorium własnego kraju uprawnień polegających na dochodzeniu

[51] Dyrektywa Parlamentu Europejskiego i Rady 95/46 z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. UE L 281, s. 31.

[52] Wyrok *ETS* w sprawie C-230/14 Weltimmo s.r.o. / Nemzeti Adatvédelmi és Információszabadság Hatóság z dnia 1 października 2015 r., http://curia.europa.eu/juris/liste.jsf?num=C-230/14&language=PL, [dostęp 28.04.2017 r.].

[53] Trybunał Sprawiedliwości Unii Europejskiej KOMUNIKAT PRASOWY nr 111/15, s. 1, Luksemburg, 1 października 2015 r., https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150111pl.pdf, [dostęp 28.04.2017 r.].

oraz interweniowaniu, niezależnie od tego, jakie prawo krajowe będzie miało zastosowanie do konkretnego przypadku przetwarzania danych. Do każdego organu z żądaniem wykonania jego uprawnień może się zwrócić organ innego państwa członkowskiego[54]". Wyrok jest istotny zwłaszcza dla przedsiębiorców, którzy świadczą usługi wyłącznie za pośrednictwem sieci teleinformatycznej. ETS podkreślił, że zastosowanie przepisów prawa państwa członkowskiego innego niż państwo rejestracji może wynikać, po pierwsze, z tego, że działalność administratora danych polega na prowadzeniu stron internetowych z ogłoszeniami o nieruchomościach, dotyczących nieruchomości położonych na terytorium tego państwa członkowskiego i zredagowanych w jego języku, a w związku z tym ta działalność jest w głównej mierze nakierowana na to państwo członkowskie.

Podsumowując należy stwierdzić, że wykładnia ETS, obejmująca przepisy Dyrektywy 95/46/WE, oparta była na zasadzie, zgodnie z którą, każde z państw członkowskich stosuje w przypadku przetwarzania danych osobowych, przepisy prawa krajowego przyjmowane na mocy tego unijnego aktu prawnego.

W warunkach zmian związanych z przyjęciem Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. podkreśla się, że ochrona osób fizycznych w zakresie przetwarzania danych osobowych jest jednym z praw podstawowych. Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych powinny – niezależnie od ich obywatelstwa czy miejsca zamieszkania – przestrzegać ich podstawowych praw i wolności, zwłaszcza prawa do ochrony danych osobowych. Niniejsza dyrektywa ma przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Zgodnie z pkt 15) preambuły dyrektywy jej celem jest zapewnienie jednakowego stopnia ochrony osób fizycznych poprzez prawnie wykonalne prawa obowiązujące w całej Unii, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zbliżenie przepisów państw członkowskich nie powinno skutkować osłabieniem gwarantowanej przez nie ochrony danych osobowych, a wręcz przeciwnie – powinno służyć zapewnieniu wysokiego stopnia ochrony w całej Unii. W celu zachowania bezpieczeństwa danych osobowych administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz powinni wdrożyć środki – takie jak szyfrowanie – minimalizujące takie ryzyko. Środki takie powinny zapewnić odpowiedni stopień bezpieczeństwa i poufności, oraz uwzględniać stan wiedzy technicznej, koszty ich wdrożenia w stosunku do ryzyka naruszenia i charakter danych osobowych podlegających ochronie. Państwa członkowskie powinny przyjąć, że należy informować państwa

[54] Wyrok ETS w sprawie C-230/14Weltimmo s.r.o. / Nemzeti Adatvédelmi és Információszabadság Hatóság z dnia 1 października 2015 r., http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=PL, [dostęp 28.04.2017 r.].

trzecie lub organizacje międzynarodowe o wszelkich specjalnych wymogach dotyczących przekazania danych. *Dalsze przekazanie danych osobowych powinno być poprzedzone uzyskaniem uprzedniej zgody właściwego organu*. Właściwy organ, który dokonał pierwotnego przekazania, powinien także mieć możliwość uzależnienia dalszego przekazania od spełnienia szczególnych warunków. Zgodnie z art. 40 dyrektywy dotyczącym międzynarodowej współpracy na rzecz ochrony danych osobowych państwa członkowskie muszą m.in. wypracować mechanizmy współpracy międzynarodowej ułatwiające skuteczne egzekwowanie przepisów o ochronie danych osobowych, zapewnić wzajemną pomoc międzynarodową w egzekwowaniu przepisów o ochronie danych osobowych, w tym poprzez powiadomienia, przekazywanie skarg, pomoc w prowadzeniu postępowań wyjaśniających oraz wymianę informacji, z zastrzeżeniem odpowiednich zabezpieczeń ochrony danych osobowych i innych podstawowych praw i wolności oraz upowszechniać wymianę i dokumentowanie przepisów i praktyk w dziedzinie ochrony danych osobowych, w tym dotyczących kolizji jurysdykcyjnych z państwami trzecimi.

Nowe zasady stanowią początek regulacji niezbędnych dla prawidłowego przetwarzania danych osobowych w warunkach cyfrowych.

Bibliografia:

P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2016

J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015

E. Kulesza, *Zdrowie: zasada i wyjątki*, Rzeczpospolita z 04.05.2000 r.

M. Pamuła, *Serwis internetowy do komunikacji wewnątrz grup*, praca magisterska, Uniwersytet Warszawski, Wydział Matematyki, Informatyki i Mechaniki, Warszawa 2007

I. Gmińska, A. Kwiatkowski, *Ochrona danych osobowych na portalach społecznościowych na przykładzie Facebooka,* Zeszyty Naukowe Uczelnianej Rady Doktorantów Uniwersytetu Kazimierza Wielkiego, t. 2, nr 1 Bydgoszcz 2014

M. Juza, *Sieć społeczna - nowoczesne plemię. Serwis www.orkut.com jako przykład możliwości Internetu w upowszechnianiu sieciowej formy porządku społecznego*, [w:] *Wielka sieć. Eseje z socjologii Internetu*, J. Kurczewski (red.), Warszawa 2006

M. Czerniawski, *Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa TSUE*, s. 93 [w:] *Polska i europejska ochrona danych osobowych*, E. Bielak-Jomaa, D. Lubasz (red.), Warszawa 2016

Streszczenie

Ochrona danych osobowych w nowych warunkach cyfrowych wymaga redefinicji i zmian przepisów prawa. Rozwój nowych technologii powoduje, iż obecne przepisy prawa nie są adekwatne do nowych wyzwań w ochronie danych osobowych. Dlatego też prawo to jest ciągle zmieniane i udoskonalane. Istotną rolę odgrywają tu organy powołane do przestrzegania przepisów odnoszących się do ochrony prywatności. Ważna z punktu widzenia osób fizycznych – bo to właśnie ich dotyczy ochrona danych

– wydaje się również świadomość związana z istniejącymi zagrożeniami płynącymi z korzystania z serwisów internetowych, w tym w szczególności z serwisów społecznościowych. Użytkownicy korzystając z nich nie zawsze mają pełną świadomość, czy dane umieszczane w sieci – a wymagane np. w procesie rejestracji – nie zostaną wykorzystane przez osoby do tego nieuprawnione. Zagadnienie to dotyka takich kwestii jak: odpowiedzialność za treści umieszczane w sieci, odpowiedzialność za usługi świadczone drogą elektroniczną, prawo do bycia zapomnianym, jurysdykcja w obszarze globalnego świadczenia usług. Ochrona prawna, którą gwarantują nowe przepisy unijne stanowi początek niezbędnej w tym zakresie reformy.

Słowa klucze: dane osobowe, odpowiedzialność za świadczenie usług elektronicznych, bezpieczeństwo prawne osób fizycznych, prawo do bycia zapomnianym, prawo do prywatności.

Legal protection of personal data in new digital conditions

Summary

The protection of personal data in the new digital conditions requires redefinition and changes of the law. The development of new technologies means that the current legal provisions are not matched to new challenges in the protection of personal data. Therefore, this law is still changed and improved. The most important role is played by bodies appointed to comply with provisions relating to the protection of privacy. Important from the point of view of individuals - because it is their data protection – it also seem the awareness related to the existing threats resulting from the use of websites, in particular from social websites. Users using them are not always fully aware that the data placed on the network will not be used by unauthorized persons. This problem touches on issues such as: responsibility for content on the web, responsibility for services provided electronically, the right to be forgotten, jurisdiction in the area of global service provision. The legal protection, which is guaranteed by the new EU regulations, is only the starting point of the necessary changes in this area.

Keywords: personal data, responsibility for the provision of electronic services, legal security of individuals, the right to be forgotten, the right to privacy.