

Prawo do prywatności w dobie Internetu¹

Ewa Michałkiewicz²

Ewa Milczarek³

W niniejszym opracowaniu autorzy odnoszą się do problemu ochrony prywatności. Jest to szczególnie ważne w dobie powszechnej dostępności Internetu, gdzie granice prywatności stają się coraz mniej wyraźne. Wraz z rozwojem Internetu został ułatwiony nie tylko dostęp do danych osobowych, lecz także możliwość ich swobodnego kreowania. Z uwagi na fakt, że prywatność miliardów użytkowników Internetu jest zagrożona, i to zarówno ze strony przedsiębiorstw, jak i instytucji państwowych, autorzy opracowania sygnalizują konieczność wypracowania przez Polskę i UE mechanizmów służących do jej ochrony.

Uwagi wstępne

Prawa i wolności człowieka i obywatela są aktualnie bardzo popularnym tematem dyskusji i opracowań. Przede wszystkim dlatego, że stanowią one w większości prawa o charakterze podstawowym, które przysługują wszystkim jednostkom. Państwa, które w dzisiejszych czasach nie mogą lub nie chcą zapewnić obywatelom ochrony ich podstawowych praw, nie są uznawane za demokratyczne państwa prawa. Chronione są przede wszystkim życie i zdrowie ludzkie, a także godność ludzka oraz prawa wywodzące się z niej, np. prawo do poszanowania życia prywatnego i rodzinnego.

W wielu krajach europejskich i nie tylko przyjęto powszechnie obowiązującą zasadę, iż każdy człowiek ma prawo do prywatności w życiu osobistym, rodzinnym i prywatnym. Prawo to dosyć często jest konstytuowane w porządkach prawnych państw (np. Konstytucja RP), jak również zostało ukształtowane (tym razem jako wolność) w aktach prawnych o charakterze międzynarodowym oraz ponadnarodowym, m.in. w art. 7 Karty Praw Podstawowych Unii Europejskiej z 30.3.2010 r.⁴ Jednakże w dobie Internetu coraz trudniej jest zagwarantować państwom taką ochronę swoim obywatelom i rezydentom, zważywszy na szybkość i łatwość wprowadzania danych do sieci oraz ich rozprzestrzenianie się, a także z uwagi na wzrastającą popularność społecznościowych serwisów internetowych oraz brak zahamowań ludzi w dzieleniu się informacjami na własny temat. Te wszystkie czynniki, jak też wiele innych, przyczyniają się do tego, że informacje na temat życia prywatnego, rodzinnego, a często także zawodowego są zamieszczane i rozprzestrzeniane w sieci, np. w wyszukiwarkach internetowych typu Yahoo czy Google. Prawo do prywatności łączy się także z prawem do ochrony danych osobowych, które przysługuje każdemu obywatelowi i sprowadza się do tego, że dane osobowe każdego człowieka podlegają ścisłej ochronie i mogą być udostępniane tylko za zgodą tej osoby. Jednakże – podobnie jak w przypadku ochrony prywatności – coraz trudniejsze staje się zapewnienie obywatelom ochrony ich danych osobowych,

tym bardziej że dane takie dosyć często rozpowszechniane są przez nich samych.

W dzisiejszych czasach coraz chętniej odkrywa się swoją prywatność, udostępniając ją innym. Co więcej, niemalże powszechną praktyką stało się to, że przy korzystaniu z danego serwisu internetowego należy wprowadzić swoje dane osobowe i często nie są to strony sklepów internetowych, lecz również portale pozyskujące dodatkowe informacje o charakterze nawet intymnym (np. randkowe). Swoje dane udostępnia się co prawda po przeczytaniu regulaminu i wyrażeniu zgody na udostępnianie i przetwarzanie danych w określonych przez serwis przypadkach, jednakże nie stanowi to skutecznej ochrony przed rozpowszechnianiem naszych danych w sieci.

Nie powinny zatem dziwić przypadki, w których dochodzi do łamania prawa do prywatności i ochrony danych osobowych w Internecie. Przykładów takich przypadków jest wiele, poczynawszy od przywłaszczania wizerunku, zdjęć z prywatnych profili portali społecznościowych przez sklepy internetowe, zamieszczanie poniżających treści przez osoby poszukujące zemsty, a skończywszy na przypadkowym udostępnieniu numeru rejestracyjnego samochodu w pobliżu miejsca zamieszkania poprzez programy lokalizujące typu Google Maps. Te wszystkie przypadki pokazują nam tylko, iż współczesne granice prywatności stają się coraz mniej wyraźne.

Pojęcie prywatności

Pojęcie prywatności ukształtowało się już w czasach starożytnych, kiedy to jako pierwszy sferę życia domowego, rodzin-

¹ Wstęp i część 3 opracowała E. Michałkiewicz, część 4 i wnioski opracowana została przez E. Milczarek, część 2 przygotowały obie Autorki.

² Autorka jest asystentką w Katedrze Prawa Konstytucyjnego i Integracji Europejskiej, Uniwersytet Szczeciński Wydział Prawa i Administracji.

³ Autorka jest asystentką w Katedrze Prawa Konstytucyjnego i Integracji Europejskiej, Uniwersytet Szczeciński Wydział Prawa i Administracji.

⁴ Dz. Urz. UE C Nr 83, s. 389; dalej jako: KPP UE.

nego – *oikos* – od sfery życia publicznego politycznego – *polis* – oddzielił Arystoteles⁵. Co prawda rozumienie „prywatności” w znaczący sposób różniło się od znaczenia tego pojęcia w czasach współczesnych, jednakże nie sposób nie zaszykalizować, iż już wtedy pojęcie to zaczęło funkcjonować.

Kontynuatorami sposobu myślenia opartego na rozdziale sfer prywatnej i publicznej byli także w późniejszym czasie *B. Constant* oraz *J.S. Mill*. Swoje idee dotyczące sfery prywatności człowieka łączyli oni z innym prawem podstawowym, a mianowicie z prawem do wolności. „Punktem wyjścia systemu *J.S. Milla* – podobnie jak *B. Constanta* – był indywidualizm. Podobnie jak tam, celem rozważań było zapewnienie wolności rozumianej jako indywidualna odrębność jednostki. Sednem myśli *J.S. Milla* była pewność, że szacunek dla prywatności jest podstawą wolności, a o człowieczeństwie ludzi stanowi ich zdolność wyboru⁶. *J.S. Mill* przewidywał jednak, że w niektórych przypadkach, dotyczących np. bezpieczeństwa społecznego czy też sprawiedliwości, istnieje dopuszczalność ingerencji państwa w sferę życia prywatnego⁷, zatem nie przyznawał prawa do prywatności charakteru bezwzględniego.

Odpowiedzią na koncepcję liberalną prawa do prywatności była koncepcja komunitarystów. Ich zdaniem „liberalnie pojmowany system praw i wolności stanowi apologię ludzkiego indywidualizmu i egoizmu, który ignoruje jedną z najbardziej podstawowych potrzeb: bycia z innymi”. Podpisują się oni pod słowami *E. Fromma*, że „sama wolność negatywna czyni z jednostki ludzkiej istotę izolowaną i samotną. Prawo do prywatności (...) sankcjonuje tę izolację i samotność⁸”.

Pierwsza współczesna definicja ochrony prawa do prywatności pojawiła się w 1890 r. na łamach *Harvard Law Review* w eseju pt. *Right to Privacy*. W pracy tej prywatność określono jako „prawo do pozostawienia w spokoju”, a takie zdefiniowanie tego pojęcia stanowiło podwaliny dla rozwoju prawa do prywatności na całym świecie. Autorami nowoczesnej definicji „prywatności” byli *S.D. Warren* oraz *L.D. Brandeis*⁹. *R. Dopierała* wskazuje również na kilka innych koncepcji prywatności, które rozwinęły się już w czasach współczesnych. Jako pierwszy przykład podaje wnioski *A. Millera* oraz *E. Beardleya* z 1971 r., którzy to prawo do prywatności wiążą nierozdzielnie ze zdolnością człowieka do umiejętnego udostępniania informacji o sobie. To jednostka sama określa swoją sferę prywatności i może zdecydować o tym, jakie informacje o sobie udostępni innym. Zatem za wiedzę innych na temat danego człowieka odpowiedzialny jest on sam¹⁰. Kilkanaście lat później zdanie *A. Millera* i *E. Beardleya* potwierdza *W.A. Parent*, który uważa, że „prywatność jest warunkiem nieposiadania nieudokumentowanych informacji osobistych znanych innym¹¹”. Według niego rozpowszechnianie informacji, które zostały już upublicznione np. za sprawą prasy, mediów (*Ł. Kołodziejczyk* przypuszcza, że można tu mówić również o Internecie), nie stanowią naruszenia prawa do pry-

watności z jednego prostego powodu – przestały one być informacjami prywatnymi w momencie ich pierwszej publikacji¹². Koncepcje te spotykają się jednak z krytyką innych autorów, którzy wskazują na fakt, iż mogą one zostać łatwo obalone w przypadku np. inwigilacji, kiedy to informacje, którymi nie chcemy się dzielić, zostaną i tak uzyskane¹³.

Ostatnią wartą uwagi dwudziestowieczną definicję prywatności przedstawia nam *J. DeCew*, która proponuje spojrzeć na pojęcie prywatności w kilku wymiarach: informacyjnym, dostępności oraz ekspresji. Granice między poszczególnymi kategoriami nie są wyraźne, jednakże była to tak naprawdę pierwsza definicja, która zapoczątkowała erę koncepcji prywatności rozpatrywanych w aspekcie wielowymiarowym¹⁴. Autorka uważa, iż aby przyznać jakiejś informacji status prywatnej, należy umieścić ją w określonym kontekście regulowanym przez grupy społeczne, do których przynależy każdy człowiek, albo też odnieść ją do subiektywnych odczuć danej jednostki¹⁵.

W Polsce stosunkowo niedawno kwestia ta stała się tematyką rozważań *A. Kopffa*, który zdefiniował „prywatność” w pracy pt. *Koncepcja praw do intymności i do prywatności życia osobistego jako „prawo jednostki do życia własnym życiem układanym według własnej woli z ograniczeniem do minimum wszelkiej ingerencji zewnętrznej”¹⁶. Według *A. Mączyńskiego* prawo do prywatności wynika z prawa do godności i interpretacja prawa do prywatności musi być dokonywana przez pryzmat prawa do godności¹⁷.*

Należy zwrócić uwagę, iż prawo do prywatności nie występuje jedynie na tle rozważań filozoficznych, teoretycznych, ale pojawia się także w sferze regulacji i rozważań prawnych. Odniesienia do prawa do prywatności znajdziemy w wielu ważnych aktach prawa międzynarodowego, a także polskiego prawa krajowego.

Jako przykład regulacji międzynarodowych przytoczyć można Konwencję o Ochronie Praw Człowieka i Podstawowych Wolności z 4.11.1950 r.¹⁸, gdzie w art. 8 przyznaje się

⁵ *Ł. Kołodziejczyk*, *Prywatność w Internecie*, Warszawa 2014, s. 13.

⁶ *J. Braciak*, *Prawo do prywatności*, Warszawa 2004, s. 17–18.

⁷ *Ibidem*, s. 18.

⁸ *Ibidem*, s. 20.

⁹ *S.D. Warren, L.D. Brandeis*, *Right to privacy*, *Harvard Law Review* vol. IV, Nr 5, Cambridge 1980, s. 193.

¹⁰ *R. Dopierała*, *Prywatność w perspektywie zmiany społecznej*, Kraków 2013, s. 25.

¹¹ *Ibidem*, s. 25–26.

¹² *Ł. Kołodziejczyk*, *Prywatność...*, s. 17.

¹³ *Ibidem*, s. 17.

¹⁴ *Ibidem*, s. 18.

¹⁵ *R. Dopierała*, *Prywatność w perspektywie...*, s. 27.

¹⁶ *J.D. Sieńczyło-Chlabicz*, *Naruszenie prywatności osób publicznych przez prasę*, Kraków 2006, s. 97.

¹⁷ *A. Mączyński*, *Konstytucyjne podstawy prawa do godności i d prywatności*, wystąpienie z 26 Międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych, http://26konferencja.giodo.gov.pl/data/resources/MaczyńskiA_paper.pdf (dostęp z 1.1.2015 r.).

¹⁸ Konwencja zmieniona następnie Protokołami Nr 3, 5 i 8 oraz uzupełniona Protokołem Nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284).

każdemu prawo do poszanowania jego życia prywatnego, poszanowania korespondencji oraz do niedopuszczalności ingerencji władz publicznych w korzystanie z tego prawa (z wyjątkiem przypadków ujętych w ustawie i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób).

Współczesne państwa rozbudowują w znaczącym zakresie instrumenty prawne ochrony prywatności, ale jednocześnie znajdują powody, dla których mogą w to prawo ingerować. W Polsce ochrona prywatności i danych osobowych jest regulowana pierwszy raz wprost w Konstytucji RP. Ochrona prawa do prywatności jest uregulowana w art. 47, który stanowi, że „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”, oraz w art. 76, w myśl którego „władze publiczne chronią konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu oraz przed nieuczciwymi praktykami rynkowymi. Zakres tej ochrony określa ustawa”.

Ponadto Konstytucja RP wprowadziła nową kategorię konstytucyjną w postaci prawa podmiotowego do ochrony danych osobowych¹⁹. Uregulowana jest ona w art. 51 i w jej zakresie wchodzi m.in. warunek ustawowej podstawy obowiązku ujawnienia przez osobę dotyczących jej informacji (ust. 1), zakaz pozyskiwania, gromadzenia i udostępniania o obywatelach innych informacji niż niezbędne w demokratycznym państwie prawnym (ust. 2), prawo dostępu do dokumentów i zbiorów danych oraz żądania sprostowania bądź usunięcia danych nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (ust. 3 i 4). Przepis ten zawiera nadto generalną zapowiedź konstytucyjną, zgodnie z którą „zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa” (art. 51 ust. 5). Łączna analiza przywołanych przepisów w orzecznictwie TK doprowadziła do sformułowania koncepcji „autonomii informacyjnej” jednostki²⁰.

Prawo do prywatności do tej pory regulowało kwestię uprawnień państwa wobec obywatela. Obecnie coraz częściej zagrożenie wejścia w sferę prywatną obywatela zachodzi ze strony podmiotów prywatnych. Trybunał Konstytucyjny w wyroku z 19.2.2002 r. stwierdził, że art. 47 Konstytucji RP nakłada na ustawodawcę obowiązek zapewnienia jednostce odpowiedniej ochrony sfery życia prywatnego nie tylko przed ingerencją ze strony podmiotów prywatnych²¹. Rozwój Internetu sprawił, iż obecnie został ułatwiony nie tylko dostęp do danych osobowych, lecz także możliwość swobodnego kreowania takich danych. Informacje te są coraz częściej wykorzystywane przez internetowe przedsiębiorstwa, które udostępnione, a następnie zgromadzone dane wykorzystują w celach marketingowych.

Ochrona prywatności w Internecie ma coraz większe znaczenie dla społeczeństw w związku z rozwojem m.in. bankowości elektronicznej, portali społecznościowych i innych serwisów zbierających informacje na temat użytkowników Internetu. Informacje są zbierane również przez organy państwowe w celu ochrony bezpieczeństwa publicznego. Koncerny informatyczne, zwłaszcza internetowe, takie jak Google, Facebook, Twitter, Apple, gromadzą dane o swoich użytkownikach. Wspomniane przedsiębiorstwa zgromadzone dane wykorzystują m.in. do działalności handlowej. Praktyka pokazała, że ich zabezpieczenie jest iluzoryczne. Dane te nie były przez wspomniane przedsiębiorstwa szyfrowane i zostały wykorzystane przez amerykańską Agencję Bezpieczeństwa Krajowego²².

W UE zmiany w zakresie dostosowania prawa ochrony prywatności do poziomu rozwoju technologii informacyjnych zostały dokonane przez instrumenty prawa publicznego i nadanie obywatelom nowych publicznych praw podmiotowych. Stworzono wspólny rynek informacyjny, gdzie użytkownicy uzyskali prawo do „informacyjnego samookreślenia”, czyli do kontroli informacji na swój temat czy udzielania zgody na przetwarzanie danych osobowych²³. Obecnie możemy zaobserwować tendencje do ograniczenia zakresu prawa krajowego w sferze ochrony danych osobowych na rzecz prawa europejskiego. Zasadnicza w tej kwestii jest dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych²⁴ oraz art. 8 KPP UE.

W stosunku do pierwszego z aktów powstało wiele wątpliwości dotyczących stosowania go w stosunku do spraw związanych z Internetem. W 1995 r. nikt nie mógł bowiem przewidzieć, że w niedługim czasie dostęp do Internetu będzie miał każdy, a przesył informacji będzie niezwykle szybki i niczym nieograniczony, stąd uzasadnione obawy co do adekwatności przepisów zawartych we wspomnianym akcie do rzeczywistej sytuacji w środowisku cyfrowym. Mniej sceptyczny w tym temacie jest *L.A. Bygrave*, który chociaż zgadza się z zarzutem tworzenia prawa bez uwzględnienia w nim środowiska cyfrowego, to jednak twierdzi, iż regulacje dyrektywy 95/46/WE są na tyle „wystarczająco pojemne, aby

¹⁹ A. Mączyński, *Konstytucyjne...*, *passim*.

²⁰ Zob. m.in. wyrok TK z 17.6.2008 r., K 8/04, Dz.U. Nr 110, poz. 707.

²¹ Wyrok TK z 19.2.2002 r., U 3/01, OTK-A 2002, Nr 1, poz. 3.

²² Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych UE, Projekt sprawozdania w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, 2013/2188(INI), www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/1014/1014703/1014703pl.pdf (dostęp z 1.1.2015 r.).

²³ K. Dobrzeński, *LexInformatica*, Toruń 2008, s. 103–107

²⁴ Dz.Urz. UE L Nr 281, s. 31; dalej jako: dyrektywa 95/46/WE.

UE, stała się stroną pozwaną w kilku głośnych procesach dotyczących m.in. prawa do prywatności.

Wyszukiwarka Google i prawo do bycia zapomnianym

Wraz z upowszechnieniem Internetu nastąpiła również ewolucja prawa do prywatności, która polegała na konieczności rozszerzenia jego zakresu na nowe środowisko – sieć internetową. Stało się tak, dlatego iż właśnie na tym polu pojawiła się możliwość dokonywania nowych naruszeń dotyczących praw osobowych jednostki, w tym prawa do prywatności. Kiedyś „procedury postępowania z danymi osobowymi miały uchronić jednostkę przed ingerencją w jej sferę informacyjną z uwagi na automatyzację procesów wykorzystania danych. Obecnie ponownie zastanawiamy się nad uchronieniem jednostki przed ingerencją w jej autonomię informacyjną w związku z zastosowaniem nowych sposobów i środków przetwarzania danych osobowych – jak *cloudcomputing*, tyle tylko, że przy tej okazji warto również zastanowić się nad dotychczas funkcjonującym modelem autonomii informacyjnej”³².

Na tle prawa polskiego przyjmuje się, iż autonomia informacyjna, zagwarantowana przepisami samej Konstytucji RP, jest niczym innym jak możliwością samodzielnego decydowania jednostki o tym, jakie informacje na swój temat udostępni, a także kontrolą nad tymi informacjami oraz innymi, które nie zostały przez nią ujawnione, ale i tak znalazły się w sferze informacji publicznych³³. W podejściu tym widać znaczne podobieństwa ze sposobem myślenia W.A. Parenta, który uważał, iż sferę swojej prywatności może chronić sam człowiek, który jest odpowiedzialny za to, co przedostaje się do sfery publicznej i ma zdecydowanie największy wpływ na dokonywanie selekcji publicznych informacji o sobie. Jednakże także w tym przypadku można tej koncepcji zarzucić krótkowzroczność. Nie przewiduje ona bowiem sytuacji, w których to jednostka nie będzie mogła w żadnej mierze czuć nad tym, co tak naprawdę na jej temat zostało upublicznione. „Sieć zwiiera nie tylko materiały (zdjęcia, nagrania, relacje), które zostały w niej umieszczone intencjonalnie. Niejednokrotnie pojawiają się w niej przekazy przygotowane bez wiedzy zainteresowanego, które naruszają wizerunek i dobra osobiste osoby, przedstawiając ją w negatywnym, kompromitującym czy kontrowersyjnym kontekście. Pewne dane mogą być także generowane i użytkowane bez wiedzy użytkownika za sprawą technologii inwigilujących”³⁴. R. Dopierała wskazuje również na to, iż obecnie w Internecie nikt nie jest anonimowy, ponieważ każdy posiada adres IP, na podstawie którego następuje jego identyfikacja. Dzięki adresowi IP administratorzy stron internetowych, a także inne podmioty mogą sprawdzać aktywność konkretnych użytkowników Internetu. Taki sam pogląd wyrażają J. Barta

i R. Markiewicz. Ich zdaniem: „Nie przysparza dziś poważnych trudności ustalenie, kto i kiedy oraz jakie »wywoływał« informacje; również kto z kim korespondował elektronicznie, w jakich uczestniczył forach dyskusyjnych, jakie prezentował tam poglądy itd. (...) Przy pomocy specjalnych programów (tzw. *packetsniffers*) wyszukiwane mogą być przepływające w sieci dane określonego rodzaju, na przykład wybierane według słów kluczowych lub według danych”³⁵.

Doskonałym przykładem utraty kontroli nad krążącymi w Internecie informacjami na swój temat może być głośna w zeszłym roku sprawa M.C. Gonzalez, który złożył skargę do hiszpańskiej agencji danych AEPD przeciwko oddziałowi Google – Google Spain SL. Sprawa dotyczyła faktu, iż po wpisaniu do wyszukiwarki Google danych M.C. Gonzalez pojawiał się wynik wyszukiwania, który odsyłał do jednej ze stron gazet, na której to widniały zamieszczone kilkanaście lat wcześniej informacje dotyczące zlicytowania majątku skarżącego w związku z jego niewypłacalnością. Sprawa miała miejsce dosyć dawno, licytacja ostatecznie nie nastąpiła, jednakże ślad po niej pozostał do dnia dzisiejszego i według M.C. Gonzalez w sposób negatywny wpływał na jego dobre imię, a także na prowadzone przez niego obecnie interesy. W związku z tym, powołując się na szeroko rozumiane prawo do prywatności, a także na prawo do ochrony danych osobowych, skarżący zażądał usunięcia wspomnianych informacji z wyszukiwarki w sposób trwały, by nie pojawiały się już więcej obok jego imienia i nazwiska. Co prawda AEPD przychylił się do wniosku M.C. Gonzalez, jednakże za sprawą sądu hiszpańskiego, rozpatrującego tę sprawę po odwołaniu przez Google Spain SL, finalnie spór trafił przed oblicze TSUE³⁶.

Trybunał w odpowiedzi na wniesione przez sąd hiszpański pytanie prejudycjalne dokonał wykładni niektórych przepisów wspomnianej już dyrektywy 95/46/WE, a także oparł swoje orzeczenie na analizie art. 7 i 8 KPP UE. Wyrok TSUE wywołał prawdziwą burzę, ponieważ nie tylko różnił się znacząco od opinii rzecznika generalnego, ale wyznaczał nowy kierunek interpretowania przepisów prawnych dotyczących Internetu i wyszukiwarek. Trybunał orzekł: „osoba ta może, ze względu na przysługujące jej i przewidziane w art. 7 i 8 KPP UE, zażądać tego, aby dana informacja nie była już podawana do wiadomości szerokiego kręgu odbiorców poprzez zawarcie jej na takiej liście wyników wyszukiwania,

³² M. Sakowska-Baryła, *Cloudcomputing a autonomia informacyjna jednostki*, [w:] G. Szpor (red.), *Internet. Cloudcomputing. Przetwarzanie w chmurach*, Warszawa 2013, s. 146.

³³ *Ibidem*, s. 147.

³⁴ R. Dopierała, *Technologiczne i medialne przeobrażenie prywatności*, [w:] A. Kuczyńska, K. Stachura (red.), *Pomiędzy realnością i wirtualnością. Internet i nowe technologie w życiu codziennym*, Gdańsk–Warszawa 2012, s. 11.

³⁵ J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 28.

³⁶ Opinia rzecznika generalnego N. Jaaskinena przedstawiona 25.6.2013 r., C-131/12, Dz.Urz. UE Nr 424, s. 3.

UE, stała się stroną pozwaną w kilku głośnych procesach dotyczących m.in. prawa do prywatności.

Wyszukiwarka Google i prawo do bycia zapomnianym

Wraz z upowszechnieniem Internetu nastąpiła również ewolucja prawa do prywatności, która polegała na konieczności rozszerzenia jego zakresu na nowe środowisko – sieć internetową. Stało się tak, dlatego iż właśnie na tym polu pojawiła się możliwość dokonywania nowych naruszeń dotyczących praw osobowych jednostki, w tym prawa do prywatności. Kiedyś „procedury postępowania z danymi osobowymi miały uchronić jednostkę przed ingerencją w jej sferę informacyjną z uwagi na automatyzację procesów wykorzystania danych. Obecnie ponownie zastanawiamy się nad uchronieniem jednostki przed ingerencją w jej autonomię informacyjną w związku z zastosowaniem nowych sposobów i środków przetwarzania danych osobowych – jak *cloudcomputing*, tyle tylko, że przy tej okazji warto również zastanowić się nad dotychczas funkcjonującym modelem autonomii informacyjnej”³².

Na tle prawa polskiego przyjmuje się, iż autonomia informacyjna, zagwarantowana przepisami samej Konstytucji RP, jest niczym innym jak możliwością samodzielnego decydowania jednostki o tym, jakie informacje na swój temat udostępnia, a także kontrolą nad tymi informacjami oraz innymi, które nie zostały przez nią ujawnione, ale i tak znalazły się w sferze informacji publicznych³³. W podejściu tym widać znaczne podobieństwa ze sposobem myślenia W.A. Parenta, który uważał, iż sferę swojej prywatności może chronić sam człowiek, który jest odpowiedzialny za to, co przedostaje się do sfery publicznej i ma zdecydowanie największy wpływ na dokonywanie selekcji publicznych informacji o sobie. Jednakże także w tym przypadku można tej koncepcji zarzucić krótkowzroczność. Nie przewiduje ona bowiem sytuacji, w których to jednostka nie będzie mogła w żadnej mierze czuć nad tym, co tak naprawdę na jej temat zostało upublicznione. „Sieć zwiiera nie tylko materiały (zdjęcia, nagrania, relacje), które zostały w niej umieszczone intencjonalnie. Niejednokrotnie pojawiają się w niej przekazy przygotowane bez wiedzy zainteresowanego, które naruszają wizerunek i dobra osobiste osoby, przedstawiając ją w negatywnym, kompromitującym czy kontrowersyjnym kontekście. Pewne dane mogą być także generowane i użytkowane bez wiedzy użytkownika za sprawą technologii inwigilujących”³⁴. R. Dopierała wskazuje również na to, iż obecnie w Internecie nikt nie jest anonimowy, ponieważ każdy posiada adres IP, na podstawie którego następuje jego identyfikacja. Dzięki adresowi IP administratorzy stron internetowych, a także inne podmioty mogą sprawdzać aktywność konkretnych użytkowników Internetu. Taki sam pogląd wyrażają J. Barta

i R. Markiewicz. Ich zdaniem: „Nie przysparza dziś poważnych trudności ustalenie, kto i kiedy oraz jakie »wywoływał« informacje; również kto z kim korespondował elektronicznie, w jakich uczestniczył forach dyskusyjnych, jakie prezentował tam poglądy itd. (...) Przy pomocy specjalnych programów (tzw. *packetsniffers*) wyszukiwane mogą być przepływające w sieci dane określonego rodzaju, na przykład wybierane według słów kluczowych lub według danych”³⁵.

Doskonałym przykładem utraty kontroli nad krążącymi w Internecie informacjami na swój temat może być głośna w zeszłym roku sprawa M.C. Gonzalez, który złożył skargę do hiszpańskiej agencji danych AEPD przeciwko oddziałowi Google – Google Spain SL. Sprawa dotyczyła faktu, iż po wpisaniu do wyszukiwarki Google danych M.C. Gonzalez pojawiał się wynik wyszukiwania, który odsyłał do jednej ze stron gazet, na której to widniały zamieszczone kilkanaście lat wcześniej informacje dotyczące zlicytowania majątku skarżącego w związku z jego niewypłacalnością. Sprawa miała miejsce dosyć dawno, licytacja ostatecznie nie nastąpiła, jednakże ślad po niej pozostał do dnia dzisiejszego i według M.C. Gonzalez w sposób negatywny wpływał na jego dobre imię, a także na prowadzone przez niego obecnie interesy. W związku z tym, powołując się na szeroko rozumiane prawo do prywatności, a także na prawo do ochrony danych osobowych, skarżący zażądał usunięcia wspomnianych informacji z wyszukiwarki w sposób trwały, by nie pojawiały się już więcej obok jego imienia i nazwiska. Co prawda AEPD przychylił się do wniosku M.C. Gonzalez, jednakże za sprawą sądu hiszpańskiego, rozpatrującego tę sprawę po odwołaniu przez Google Spain SL, finalnie spór trafił przed oblicze TSUE³⁶.

Trybunał w odpowiedzi na wniesione przez sąd hiszpański pytanie prejudycjalne dokonał wykładni niektórych przepisów wspomnianej już dyrektywy 95/46/WE, a także oparł swoje orzeczenie na analizie art. 7 i 8 KPP UE. Wyrok TSUE wywołał prawdziwą burzę, ponieważ nie tylko różnił się znacząco od opinii rzecznika generalnego, ale wyznaczał nowy kierunek interpretowania przepisów prawnych dotyczących Internetu i wyszukiwarek. Trybunał orzekł: „osoba ta może, ze względu na przysługujące jej i przewidziane w art. 7 i 8 KPP UE, zażądać tego, aby dana informacja nie była już podawana do wiadomości szerokiego kręgu odbiorców poprzez zawarcie jej na takiej liście wyników wyszukiwania,

³² M. Sakowska-Baryła, *Cloudcomputing a autonomia informacyjna jednostki*, [w:] G. Szpor (red.), *Internet. Cloudcomputing. Przetwarzanie w chmurach*, Warszawa 2013, s. 146.

³³ *Ibidem*, s. 147.

³⁴ R. Dopierała, *Technologiczne i medialne przeobrażenie prywatności*, [w:] A. Kuczyńska, K. Stachura (red.), *Pomiędzy realnością i wirtualnością. Internet i nowe technologie w życiu codziennym*, Gdańsk–Warszawa 2012, s. 11.

³⁵ J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 28.

³⁶ Opinia rzecznika generalnego N. Jaaskinena przedstawiona 25.6.2013 r., C-131/12, Dz.Urz. UE Nr 424, s. 3.

prawa te są co do zasady nadrzędne nie tylko wobec interesu gospodarczego operatora wyszukiwarki internetowej, lecz również wobec interesu, jaki może mieć ten krąg odbiorców w znalezieniu tej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby. Taka sytuacja nie ma jednak miejsca, jeśli, ze szczególnych powodów, takich jak rola odgrywana przez tę osobę w życiu publicznym, należałoby uznać, że ingerencja w jej prawa podstawowe jest uzasadniona nadrzędnym interesem tego kręgu odbiorców polegającym na posiadaniu, dzięki temu zawarciu na liście, dostępu do danej informacji³⁷.

Po wydaniu 13.5.2014 r. powyższego orzeczenia rozgorzała dyskusja. Zwolennicy takiego podejścia do tematu głosili nową erę doby Internetu, w której to będzie można bronić swojego wizerunku poprzez ponowne uzyskanie wpływu na to, co na nasz temat zostało umieszczone. Optymiści wspominali nawet o ukonstytuowaniu nowej formy ochrony prawa do prywatności, a mianowicie prawa do bycia zapomnianym³⁸.

Pojęcie to pojawiło się już kilka lat wcześniej i oznaczało znacznie więcej niż dotychczasowe prawo do bycia pozostawionym w spokoju. Nie chodziło tu bowiem tylko o wskazanie, by inni (czy to osoby prywatne, czy organy państwowe) nie ingerowali w sferę naszego życia prywatnego, lecz także o to, abyśmy posiadali narzędzie prawne, umożliwiające nam realny wpływ na informacje na nasz temat, które już zostały upublicznione. Prawo takie miało dawać nam możliwość pełnej kontroli nad tym, jak będziemy postrzegani przez innych, bowiem powinno przysługiwać nam prawo żądania usunięcia niektórych informacji o nas, pojawiających się w Internecie np. za sprawą wyszukiwarek. To właśnie „wyszukiwarki zostały uznane za jedno z podstawowych wyzwań technicznych w Dokumencie Grupy Roboczej art. 29⁷, WP 170 »Program prac na lata 2010–2011« przyjętym 15.2.2010 r. Wyzwanie to wymagało szczególnej uwagi z punktu widzenia ochrony danych osobowych. (...) Cel i charakter działania wyszukiwarek nie jest jednorodny. Wyszukiwarki spełniają dwie podstawowe role: pośrednika oraz dostawcy usług dodatkowych, na bazie informacji pozyskanych przez użytkowników i własnych dostarczanych treści. Zasadnicze działanie kojarzone z wyszukiwarkami polega na świadczeniu usług wyszukiwawczych. Usprawnienie tych działań stanowi uzasadnienie dla przetwarzania danych użytkowników. Więcej zgromadzonych danych oraz jak najdłuższy okres ich gromadzenia to bardziej precyzyjne wyniki³⁹. Wyszukiwarki bowiem gromadzą nie tylko informacje na temat naszej aktywności w Internecie, typu wyniki wyszukiwania czy historia dokonywanych zakupów, dzięki czemu może powstać spersonalizowana lista propozycji w oparciu o najczęściej odwiedzane przez nas witryny, lecz również inne informacje dotyczące użytkownika, które zostały umieszczone przez niego samego, np. w celu rejestracji na określonym portalu internetowym⁴⁰.

W takich przypadkach nie jesteśmy w stanie określić, co tak naprawdę dzieje się z tymi wszystkimi danymi, które nawet tylko jednorazowo zostały udostępnione w Internecie. Nic zatem dziwnego, że po wydaniu wspomnianego wyroku przez TS rozbrzmiały głosy, iż prawo do zapomnienia stało się w końcu faktem, ponieważ w obliczu nieustającego i wymykającego się spod kontroli przemiatu informacji i danych osobowych takie prawo pomogłoby uregulować kilka podstawowych kwestii. Czy aby jednak na pewno?

Niektórzy z komentatorów byli nieco bardziej sceptyczni. Wskazywali na wiele spraw, których tak naprawdę wyrok wcale nie regulował, oraz na istotne problemy, które nie zostały wcale rozwiązane. Co prawda orzeczenie TSUE wiąże na przyszłość sądy krajowe państw członkowskich przy rozstrzyganiu podobnych spraw, jednakże już w tym momencie kończy się rzeczywisty wpływ prawa unijnego na ochronę naszej prywatności i danych osobowych.

Trybunał w wyroku w sprawie Google Spain SL przyznał jednostkom prawo do żądania wymazania informacji na ich temat w przypadku, kiedy tylko jednostka takie dane uzna za niekorzystne dla siebie. Co więcej, żądanie takie nie musi być nawet uzasadnione możliwością poniesienia przez jednostkę jakiegokolwiek szkody ze względu na to, iż prawo wniesienia żądania wynika bezpośrednio z prawa do prywatności i prawa do ochrony danych osobowych. Sceptycy ogłosili jednak, że na tym kończy się wpływ TSUE na ochronę naszych praw podstawowych. Mamy bowiem takie prawo, ale nie ma żadnych regulacji dotyczących już samej procedury wnoszenia naszych żądań oraz nie funkcjonują żadne mechanizmy, które mogłyby nasze żądania sankcjonować. Trybunał nie posiada przecież bezpośredniej możliwości kontrolowania i nakładania sankcji na spółki krajowe w przypadku, kiedy nie chciałyby się one zastosować do wniosku jednostki, a sprawa rozgrywa się na poziomie krajowym. Do jakichkolwiek działań są upoważnione jedynie sądy krajowe, które różnią się przecież między sobą sposobem przeprowadzania postępowań sądowych. Sam wyrok nie reguluje także kwestii procedury wnoszenia wniosków o usunięcie danych. W związku z tym przysługuje nam prawo do żądania usunięcia określonych informacji na nasz temat z wyszukiwarek, jednakże nie zostało określone, w jaki sposób należy wnieść takie żądanie, aby było ono skuteczne. Pozostaje nam

³⁷ Wyrok TSUE z 13.5.2014 r., C-131/12, www.eur-lex.europa.eu.

³⁸ Zob. Prawo do bycia zapomnianym, <http://www.infor.pl/prawo/prawo-konsumenta/konsument-w-sieci/694634,2,Prawo-do-bycia-zapomnianym-w-Internecie.html> (dostęp z 2.1.2015 r.); *L. Faciejew*, Kioskarz przed Trybunałem. Google i prawo do zapomnienia, <http://kulturaliberalna.pl/2014/09/30/google-prawo-do-zapomnienia-w-internecie/> (dostęp z 2.1.2015 r.).

³⁹ *B. Fisher*, Prawo użytkowników wyszukiwarek internetowych do poszanowania ich autonomii informacyjnej, [w:] *G. Szpor* (red.), *Internet, Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011, s. 65–67.

⁴⁰ *Ibidem*, s. 66.

stosowanie formularza, który na swoim serwisie zamieściło samo Google, jednakże w dalszym ciągu brakuje regulacji dotyczących dalszego postępowania. W jakim terminie Google powinno rozpatrzyć sprawę? Na jakiej podstawie Google może odmówić wymazania wpisu? Jak się zachować, kiedy nastąpi taka odmowa? W rezultacie oddziały Google zostały zasypane żądaniem internautów, które są rozpatrywane dosyć opieszale, co zresztą nie powinno dziwić, zważywszy na brak przygotowania na taki stan rzeczy działów prawnych oddziałów wyszukiwarki.

P. Górecki wskazuje na dane zawarte w tzw. raporcie przejrzystości, który został opublikowany przez firmę Google w związku napływającymi z całego świata wnioskami o wymazanie danych. Wynika z niego, że w okresie od 13.5.2014 r. do 9.10.2014 r. napłynęło łącznie 144 907 wniosków, z samej Polski 3665⁴¹.

Zarzut dotyczący braku regulacji prawnych oraz procedur, które w procesie rozpatrywania wniosków o usunięcie danych powinny być przestrzegane i stosowane przez Google, został częściowo odparty dzięki uchwalonym 26.10.2014 r. przez Grupę Roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych „Wytycznym w sprawie wdrożenia wyroku Trybunału Sprawiedliwości Unii Europejskiej Google Spain and INC v. Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12”. W dokumencie tym Grupa Robocza zawarła 13 pytań (kryteriów), według których Google powinno rozpatrywać wnioski z żądaniem usunięcia danych oraz szczegółowe opisy i wyjaśnienia tychże pytań⁴². Wciąż jednak brakuje opisu dokładnej procedury dotyczącej rozpatrywania wniosków oraz ewentualnej procedury odwoławczej. Obecnie kraje członkowskie UE w przypadku odmowy Google usunięcia danych wnioskodawcy stosują krajowe procedury sądowe, które w poszczególnych państwach mogą się od siebie różnić.

Kolejnym minusem, jakiego dopatrywali się sceptycy, jest usunięcie z wyszukiwarki niekorzystnej dla nas informacji, ale tylko z wyników wyszukiwania w danym państwie, czyli w państwie złożenia żądania. Przykładowo, jeżeli zostanie złożony wniosek o usunięcie informacji z polskiej wyszukiwarki, rzeczywiście zniknie ona bezpowrotnie, ale tylko w Polsce, a będzie można ją odnaleźć np. na angielskiej stronie tej samej wyszukiwarki⁴³. W związku z taką liczbą nieścisłości nie można jednoznacznie stwierdzić, aby od 13.5.2014 r. można było cieszyć się pełnią prawa do bycia zapomnianym.

Kolejny aspekt, który pojawia się *à propos* rozważań nad prawem do zapomnienia, to aspekt moralny tego problemu. Oczywiście należy się zgodzić, że takie uprawnienie może być błogosławieństwem dla osób, które zostały bezprawnie oczernione, czy też dla prześladowanych w Internecie przez rówieśników nastolatków. Jednakże powstaje pytanie, czy takie prawo do wymazania wszelkich, nawet tych niechlubnych,

informacji na czyjś temat powinno zostać bez ograniczeń przyznane każdemu? Trybunał w swoim wyroku dokonał rozróżnienia osób prywatnych od tych jednostek, które znajdują się w sferze publicznej, i w związku z tym informacje ich dotyczące stanowią wartość wyższą dla interesu ogółu niż dla jednostkowego prawa podmiotowego tych osób fizycznych. W tym przypadku zostały rozwiane wątpliwości sceptyków, którzy w prawie do zapomnienia upatrywali się ukrytego narzędzia do walki politycznej⁴⁴. Jeżeli bowiem TSUE nie uregulowałaby tej kwestii, z prawa do zapomnienia z pewnością chętnie korzystaliby politycy, którzy chcieliby ukryć swoje niechlubne występkę, tudzież chcieliby manipulować wyborcami poprzez adekwatną zmianę swoich poglądów politycznych i przekonań. W tym przypadku jednak nie są oni bezwzględnie uprawnieni do wysuwania swoich żądań w celu zapomnienia ich przewinień ze względu na fakt, że należą do sfery publicznej. Jednakże nie można oczywiście w pełni odmówić im takiego prawa i rzeczywiście mogą się zdarzyć przypadki, kiedy to prawo do usunięcia informacji będzie wykorzystywane w walkach politycznych. Problem moralny o wiele bardziej istotny powstaje jednak w związku z informacjami dotyczącymi pewnej grupy jednostek, której nie można zakwalifikować do grupy osób publicznych. Chodzi tu np. o przestępców: seryjnych morderców, gwałcieli czy pedofilów. Są to niewątpliwie osoby prywatne, którym przysługuje pełnia prawa do prywatności oraz ochrony ich danych. Powstaje jednak wątpliwość, czy rzeczywiście ich prawa podmiotowe są ważniejsze niż interes ogółu? Czy przez niczym nieograniczone prawo jednostki do wymazywania informacji o fakcie, iż była wielokrotnie skazywana za gwałty, nie może dojść do kolejnych przestępstw na tle seksualnym? Czy rodzice nie powinni wiedzieć, iż w ich okolicy po opuszczeniu zakładu karnego zamieszkuje osoba skazana za pedofilię? Wyroki wydawane w ostatnim czasie, chociażby w Polsce, wskazują na możliwość utrwalenia się pewnej linii orzeczniczej. Szczególnie głośny za sprawą mediów stał się wyrok w sprawie z powództwa *Leszka L.*, który to w procesie cywilnym wniósł do SO w Warszawie pozew przeciwko Google Inc., kiedy spółka, według niego bezprawnie, odmówiła usunięcia jego danych z wyszukiwarki. Chodziło kon-

⁴¹ Zob. P. Górecki, 3665 Polaków postanowiło skorzystać z prawa do bycia zapomnianym, http://wyborcza.biz/biznes/1,100896,16780398,3665_Polakow_postanowilo_skorzystac_z_prawa_do_bycia.html (dostęp z 2.1.2015 r.).

⁴² Zob. Guidelines on the implementation of the Court of Justice of the European Union judgment on „Google Spain and INC v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (dostęp z 2.1.2015 r.).

⁴³ Zob. M. Wawrzyn, Tysiące ludzi chcą skorzystać z prawa do bycia zapomnianym. A Internet i tak będzie pamiętał, <http://gadzetomania.pl/1295,tysiace-ludzi-chca-skorzystac-z-prawa-do-bycia-zapomnianym-a-internet-i-tak-bedzie-pamiatal> (dostęp z 2.1.2015 r.); Ł. Pawłowski, Internet i prawo do zapomnienia, <http://kulturaliberalna.pl/2014/09/30/internet-prawo-zapomnienia/> (dostęp z 2.1.2015 r.).

⁴⁴ Internetu nie da się kontrolować, <http://kulturaliberalna.pl/2014/09/30/internet-kontrola-prawo-do-zapomnienia/> (dostęp z 2.1.2015 r.).

kretnie o list gończy, który został rozesłany za *Leszkiem L.*, a informacja o nim, mimo że list został prawdopodobnie cofnięty, nadal wyświetlała się w wynikach wyszukiwarki. Sąd Okręgowy w Warszawie pozew oddalił z uwagi na niewystarczający materiał dowodowy, jednakże jednocześnie wspomniał, iż list gończy stanowi taką wyjątkową sytuację, w której to prawo do prywatności zostaje niejako wyłączone, w związku z czym nie można mówić o jego naruszeniu. List gończy służy bowiem temu, aby jak największa liczba osób mogła zapoznać się z informacjami o osobie poszukiwanej⁴⁵. Przy okazji tego wyroku należałoby również wspomnieć o innej zasadzie w prawie polskim, która również mogłaby wpływać na korzyść zwolenników pozostawiania informacji o skazaniach w sieci, a mianowicie argument, iż ogłoszenie wyroku jest zawsze jawne.

Bez względu na osobiste przekonania oraz wyniki rozważań moralnych należy jednak wskazać, iż oprócz głosów bezkrytycznego przyjęcia prawa do zapomnienia pojawiają się również głosy, które wskazują – w sposób trafny lub mniej trafny – na zagrożenia, które mogą wyniknąć ze źle rozumianego, a przede wszystkim źle uregulowanego, prawa do bycia zapomnianym⁴⁶. Na chwilę obecną decyzje o wykreśleniu danego wpisu są decyzjami uznaniowymi prawników Google i to od nich w dużej mierze zależy, czy coś pozostanie na stronie, czy też z niej zniknie⁴⁷. Jak wynika z przytaczanego już raportu przejrzystości, w krótkim czasie po wydaniu wyroku pozytywnie rozpatrywane były niemalże wszystkie wnioski zgłaszane do Google, z czasem jednak tendencja ta zmalała – „w skali całego kontynentu 58,2% wniosków zostało odrzuconych, a 41,8% zostało rozpatrzonych pozytywnie. Przykładowo wniosek pewnej Włoszki o usunięcie linków do informacji o zabójstwie jej męża sprzed lat, gdzie pojawiło się jej nazwisko. Z kolei odmownie załatwiono wniosek szwajcarskiego finansisty, który prosił o usunięcie dziesięciu linków do informacji o jego aresztowaniu”⁴⁸. Z publikowanych przez Google raportów przejrzystości wynika, iż liczba wniosków o usunięcie danych, które są rozpatrywane pozytywnie, utrzymuje się ciągle mniej więcej na tym samym poziomie. Raport przejrzystości opublikowany w pierwszą rocznicę wydania wyroku TSUE wskazywał, iż liczba wniosków zwiększyła się do 254 271, a jedynie 41,3% z nich jest załatwiana zgodnie z żądaniem wnioskodawcy⁴⁹. W ostatnim z dostępnych raportów przejrzystości Google podaje informację, iż liczba zgłaszanych wniosków o usunięcie danych wynosi 309 093, a 41,5% rozpatrywanych jest pozytywnie⁵⁰.

Podsumowując, nie można jeszcze mówić o w pełni ukształtowanym prawie do bycia zapomnianym, jednakże trzeba jednoznacznie wskazać na fakt, iż TSUE nadał nam takie prawo i nakreślił ramy tego uprawnienia. To tylko od dalszych regulacji i wspólnie przyjętych sposobów interpretacji prawa zależy, czy rzeczywiście za jakiś czas będziemy mogli się cieszyć pełnią prawa do zapomnienia. Prawo to posiada wielu zwolenników, jednakże nie można podchodzić do niego w sposób zupełnie bezkrytyczny. Aby regulacje dotyczące

tego uprawnienia były sensowne, należy też przyjrzeć się dokładnie wielu zastrzeżeniom, które wysuwane są z kolei przez sceptyków. Tylko tworząc odpowiednie regulacje prawne, które z jednej strony będą szanowały nasze prawo do prywatności i ochrony danych osobowych, jak również z drugiej strony będą uwzględniały interes ogółu, możemy się cieszyć pełnią ochrony praw podmiotowych przy jednoczesnym poczuciu bezpieczeństwa.

Wyszukiwarka Google StreetView i ochrona prywatności

Wyszukiwarki internetowe, takie jak Google, ułatwiają korzystanie z Internetu, przez co stanowią istotny element europejskiego społeczeństwa informacyjnego. Ich funkcjonowanie stwarza jednak sporo problemów, do których można przede wszystkim zaliczyć kwestie związane z rodzajem i liczbą przechowywanych danych oraz pozyskiwaniem zgody na ich wykorzystanie, politykę w zakresie ich zatrzymywania, kończąc na śledzeniu aktywności użytkowników. Jak słusznie zauważono na seminarium pt. Ochrona danych w Internecie organizowanym przez Komisję Wolności, Sprawiedliwości i Spraw Wewnętrznych⁵¹, należy oddzielić funkcjonowanie samej wyszukiwarki od udostępnianych przez nią innych usług internetowych, takich jak poczta elektroniczna, mapy czy serwisy społecznościowe.

Od lat prym wśród wyszukiwarek w Polsce i na świecie wiodzie wyszukiwarka Google⁵². W ramach serwisu udostępniono usługę Google StreetView, dostępną w Mapach Google i Google Earth, która prezentuje zdjęcia panoramiczne w zakresie 360 stopni wykonane z poziomu ulicy oraz wnętrza wybranych obiektów. Usługa została uruchomiona po raz pierwszy w Stanach Zjednoczonych w 2007 r., a dziś jest dostępna dla ponad 3000 miast w 50 krajach na siedmiu kontynentach. Zdjęcia są wykonywane przez pojazdy wyposażone w zaawansowane technologicznie aparaty fotograficzne. Oprócz materiałów zbieranych przez sam koncern uruchomiono możliwość dostarczania zdjęć przez użytkow-

⁴⁵ Sąd oddalił cywilny pozew przeciwko Google o „prawo do zapomnienia”, <http://www.lex.pl/czytaj/-/artykul/sad-oddalil-cywilny-pozew-przeciw-google-o-prawo-do-zapomnienia> (dostęp z 30.8.2015 r.).

⁴⁶ Internetu nie da się kontrolować, <http://kulturaliberalna.pl/2014/09/30/internet-kontrola-prawo-do-zapomnienia/> (dostęp z 2.1.2015 r.).

⁴⁷ *Ibidem*.

⁴⁸ P. Górecki, 3665 Polaków postanowiło..., *passim*.

⁴⁹ M. Maj, Prawo do bycia zapomnianym ma rok. Google usuwa 41% zgłoszonych URL-i, <http://di.com.pl/prawo-do-bycia-zapomnianym-marok-google-usuwa-41-zgloszonych-url-i-52130> (dostęp z 13.5.2015 r.).

⁵⁰ Raport przejrzystości, <http://www.google.com/transparencypreport/removals/europeprivacy/?hl=pl> (dostęp z 30.8.2015 r.).

⁵¹ Materiały z seminarium Ochrona danych w Internecie; Google-DoubleClick i inne analizy przypadku, Komisja Wolności, Sprawiedliwości i Spraw Wewnętrznych, 21.1.2008 r., Bruksela, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/oj/701/701671/701671pl.pdf (dostęp z 1.1.2015 r.).

⁵² Ranking popularności wyszukiwarek internetowych, <http://www.ebizmba.com/articles/search-engines> (dostęp z 1.1.2015 r.).

ników serwisu. Zaznaczyć warto, że zdjęcia nie są obrazem w czasie rzeczywistym⁵³.

Od samego początku istnienia usługi budziła ona kontrowersje związane z ochroną danych osobowych i ochroną prawa do prywatności. W związku z tym, że została ona aktywowana początkowo w Stanach Zjednoczonych, to właśnie tam doszło do pierwszych sporów sądowych. Sądy rozpatrywały m.in. pozew małżeństwa *Boringów*, które domagało się odszkodowania związanego z wykorzystaniem bez zgody wizerunku ich domu w usłudze. Koncern bronił się, podając m.in., że w dobie obecnych technologii nie istnieje coś takiego jak „całkowita prywatność”. Sąd odrzucił pozew, podając w uzasadnieniu, że małżeństwo nie było w stanie udowodnić, iż sytuacja doprowadziła do ich upokorzenia⁵⁴.

Do ciekawego przypadku doszło w mieście NorthOaks. To małe położone w stanie Minnesota 4500 miasto jest w całości własnością samych mieszkańców. Koncern bez uzyskania wcześniejszej zgody dokonał zdjęć na terenie miasta i udostępnił je w swojej usłudze. Mieszkańcy zażądali usunięcia zdjęć z serwisu, co też uczyniono⁵⁵.

By uniknąć dalszych spraw sądowych i protestów Google zdecydowało, że zdjęcia zrobione w ramach usługi będą po zebraniu przetwarzane komputerowo, by automatycznie zamazywać twarze i tablice rejestracyjne⁵⁶. Obecnie użytkownicy mogą poprosić o uczynienie nierozpoznawalnym dodatkowych elementów dowolnego zdjęcia, na którym widać użytkownika, jego rodzinę, samochód czy dom. Użytkownicy mogą również poprosić o usunięcie zdjęć przedstawiających niedozwolone treści, takie jak nagość lub przemoc poprzez przycisk „Zgłoś problem”⁵⁷.

Duże zaniepokojenie społeczne wzbudziła informacja o zbieraniu przez samochód Google StreetView w trakcie wykonywania fotografii do usługi dodatkowych danych z niezabezpieczonych sieci Wi-Fi użytkowników, znajdujących się na trasie przejazdu samochodu. Pozyskano w ten sposób informacje obejmujące dane techniczne, informacje o treściach przesyłanych przez sieci, hasła, dokumenty oraz filmy wideo. Zarzuty zostały potwierdzone przez sąd. Na tle tej sprawy uwidocznił się problem nieadekwatności większości aktów prawnych w Stanach Zjednoczonych odnoszących się do technologii informacyjnych do obecnej rzeczywistości. Ochrona prywatności jednostki nie jest realizowana w oczekiwany przez społeczeństwo zakresie. Niekontrolowanemu przepływowi danych sprzyja fakt, że sprzęt komputerowy jest w domyślnych ustawieniach nieszyfrowany, czego świadomości nie mają użytkownicy⁵⁸.

Europa jest dla dostawcy usług internetowych ważnym rynkiem, więc usługa StreetView trafiła do niej dość szybko. Pierwszym europejskim krajem, w którym ją uruchomiono była Francja⁵⁹. Usługa szybko rozprzestrzeniała się na kolejne europejskie kraje. We wszystkich dochodziło do sporów w kwestii ochrony prawa do prywatności.

Do walki o prawo do prywatności swoich obywateli zaangażowały się również organy państwowe. Od 2010 r. Google miał duże trudności z Czeskim Biurem Ochrony Danych Osobowych, które wielokrotnie odrzucało podania o kontynuowanie prac nad uruchomieniem usługi u naszych południowych sąsiadów. Dopiero w 2012 r., po spełnieniu wielu wymagań, wydano na nie zgodę⁶⁰. Prace nad usługą na jakiś czas były wstrzymane również w Grecji, gdzie domagano się od Google podania informacji m.in. w sprawie sposobu przechowywania danych⁶¹. Z kolei włoska organizacja WatchDog wniosła o ukaranie koncernu w związku z nieprawidłowym oznakowaniem samochodów dokonujących zdjęć. Zarzuty potwierdzone zostały przez tamtejsze instytucje odpowiedzialne za ochronę danych osobowych, które nałożyły na Google karę 1,4 mln dolarów⁶². Wstrzymanie działalności serwisu zarządził na pewien czas również sąd w Szwajcarii. Pozew złożył federalny komisarz ds. ochrony danych, odpowiadającym tym samym setkom skarg Szwajcarów⁶³. Sąd nakazał, aby inne cechy identyfikacyjne, takie jak kolor skóry lub ubiór, osób sfotografowanych w pobliżu tzw. newralgicznych placówek, takich jak schroniska dla kobiet, domy starców, więzienia, szkoły, sądy i szpitale, stały się nierozpoznawalne oraz by Google doprowadził do 100% skuteczności w zamazywaniu twarzy⁶⁴.

Bazując na informacjach ze Stanów Zjednoczonych europejskie instytucje również dokonały kontroli pobierania danych z niezabezpieczonych sieci WiFi. Krajowy Urząd ds. Informatyki we Francji wykrył, iż Google czerpało z tej działalności

⁵³ Oficjalna strona Google, <http://www.google.pl/intl/pl/maps/about/partners/streetview/business/faq/#what> (dostęp z 1.1.2015 r.).

⁵⁴ Wyrok amerykańskiego Sądu Apelacyjnego z 28.1.2010 r. w sprawie Aaron C. Boring, Christine Boring przeciwko Google Inc. Nr 09-2350/www.wsg.com/attorneys/BIOS/PDFs/boring_v_google.pdf (dostęp z 1.5.2015 r.).

⁵⁵ L. Pabst, North Oaks tell Google Maps: Keep out we mean it, StarTribune, <http://www.startribune.com/lifestyle/19416279.html> (dostęp z 1.1.2015 r.).

⁵⁶ R. Lesiecki, GODO skontrolował usługę Google StreetView, <http://www.lex.pl/czytaj/-/artykul/giodo-skontrolowal-usluge-google-street-view?refererPlid=68376126> (dostęp z 1.1.2015 r.).

⁵⁷ Oficjalna strona Google, <http://www.google.pl/intl/pl/maps/about/partners/streetview/business/faq/#what> (dostęp z 1.1.2015 r.).

⁵⁸ Federal Statutes – Wiretap Act – Ninth Circuit Holds That Intercepting Unencrypted Wi-Fi Broadcasts Violates the Wiretap Act, Harvard Law Review Vol. 127, No. 6, April, http://cdn.harvardlawreview.org/wp-content/uploads/2014/04/vol127_joffe_v_google.pdf (dostęp z 1.1.2015 r.).

⁵⁹ A. Chitu, Google Street View in France, <http://googlesystem.blogspot.com/2008/07/google-street-view-in-france.html> (dostęp z 1.1.2015 r.).

⁶⁰ StreetView wraca do Czech, <http://www.gisplay.pl/google-maps-sp-2004448274/nawosci-googlemaps/2566-street-view-wraca-do-czech.html> (dostęp z 1.1.2015 r.).

⁶¹ D. Błaszczykiewicz, Grecja zatrzymuje StreetView, <http://www.idg.pl/news/345067/grecja.zatrzymuje.google.street.view.html> (dostęp z 1.1.2015 r.).

⁶² A. Szymański, Google zapłaci Włochom 1,4 mln dolarów grzywny za słabe oznakowanie swoich samochodów, <http://pclub.pl/news57190.html> (dostęp z 1.1.2015 r.).

⁶³ I. Krawczyk, Szwajcaria. Google złoży apelację w sprawie Street View, <http://www4.rp.pl/artykul/656304-Szwajcaria--Google-zlozy-apelacje-w-sprawie-Street-View-.html> (dostęp z 1.5.2015)

⁶⁴ Ika, Apelacja Google w sprawie Google StreetView, <http://www.rp.pl/artykul/656304-Apelacja-Google-w-sprawie-Street-View-w-Szwajcarii.html> (dostęp z 1.1.2015 r.).

zyski. Jednak kary nakładane na warty ponad 50 mld dolarów koncern były stosunkowo niskie (za opisane wykroczenie nałożono karę 150 tys. euro)⁶⁵. Państwa nie wypracowały skutecznej formy wpływania na serwis, stosowane do tej pory sankcje nie przyczyniły się znacząco do zmiany jego zachowań.

Osoby prywatne nie pozostały bierne wobec praktyk Google. Uwieczniony na zdjęciu w trakcie załatwiania swoich potrzeb fizjologicznych na własnej nieruchomości, upublicznionym w usłudze StreetView, Francuz wystąpił na drogę sądową, domagając się odszkodowania oraz usunięcia zdjęcia z serwisu. Mimo że na zdjęciu zamazano jego twarz, w małej miejscowości, w której mieszkał, bez problemu został rozpoznany, tym bardziej że stał przy samochodzie opatrzonym jego nazwiskiem (nazwisko było jednocześnie firmą, pod którą prowadził działalność gospodarczą). Sąd nakazał usunięcie zdjęcia, jednak odszkodowania nie zasądził, odsyłając obywatela do wymiaru sprawiedliwości Stanów Zjednoczonych, gdyż uznał, że w tym zakresie nie jest właściwy⁶⁶.

Wartość zbieranych przez usługę danych docenili urzędnicy podatkowi na Litwie. Wykorzystując oferowane przez Google narzędzia, zidentyfikowali około 100 właścicieli domów oraz 30 przedsiębiorców budowlanych naruszających przepisy podatkowe związane z prawem budowlanym⁶⁷. Dane zbierane przez Google były również analizowane i wykorzystywane na potrzeby działalności Amerykańskiej Narodowej Agencji Bezpieczeństwa⁶⁸. Jest to alarmujące, gdyż informacje (w tym prywatną korespondencję) zebrane w jednym miejscu z różnych przedsiębiorstw internetowych przez instytucje państwowe całkowicie pozbawiają obywatela prywatności, w związku z czym staje się on bezbronny w konfrontacji z państwem.

Wiele zagadnień związanych z funkcjonowaniem Internetu i nowych technologii było już przedmiotem rozważań na gruncie prawa niemieckiego. Warto zwrócić na nie szczególną uwagę ze względu na podobieństwo systemów prawa, w tym zasad i procedur prawa administracyjnego. Jak słusznie zauważa *I. Lipowicz*, niemieckie rozważania pokazują istnienie konfliktu między ochroną danych osobowych a wolnością informacyjną oraz ochroną autonomii informacyjnej⁶⁹.

Niemiecki Trybunał był autorem ciekawego orzeczenia w sprawie ochrony prawa do prywatności w związku z działalnością serwisu. Przedsiębiorstwu Google przygotowującemu usługę StreetView⁷⁰ nakazano przygotowywać panoramiczne widoki jedynie do wysokości 2 metrów. Nie pozwolono również pokazywać twarzy ani tablic rejestracyjnych pojazdów. Małe domy umieszczano w usłudze jedynie w przypadku, gdy są ze względu na swoje położenie przedmiotem częstej obserwacji, a duże domy wielorodzinne jedynie wtedy, gdy nie posiadały one cech odróżniających od innych domostw. W Niemczech Google wprowadziło możliwość żądania usunięcia całego budynku z usługi. Trybunał orzekł, że „prywatność przestrzeni chroni to, co umyka oku ogółu” i chronić należy również opisy drogi i tożsamość mieszkańców. Uznało, że liczba przetwarzanych przez koncern danych zdecydowanie przeważa nad interesem administratora danych.

Zamazania obrazu swoich domostw zażądało około 3% właścicieli. „Ofiarą” tych regulacji okazało się samo Google, które ze względu na sprzeciw jednego z użytkowników budynku, w którym wynajmuje swoje biuro, musiał go uczynić nierozpoznawalnym⁷¹. W związku z tym widok siedziby Google w Monachium jest niedostępny w usłudze⁷².

Warty zauważenia jest fakt, że niemieckie prawodawstwo wyłącza stosowanie wobec usługi ochrony wolności prasy [art. 5 ust 1 zd. 2 niemieckiej ustawy zasadniczej (*Grundgesetz*)], gdyż działalność koncernu nie ma charakteru dziennikarsko-redakcyjnego⁷³.

Przyznać należy, że w Polsce służby zajmujące się ochroną danych osobowych stanęły na wysokości zadania i jeszcze przed wejściem na rynek usługi Generalny Rzecznik Ochrony Danych Osobowych odbył serie spotkań z przedstawicielami koncernu w celu określenia warunków działalności w kraju. Zobowiązał go m.in. do uprzedniego informowania mieszkańców miast o planowanym rozpoczęciu zdjęć (co dopiero później stało się standardem w UE) i do odpowiedniego oznakowania pojazdów Google. W Polsce wprowadzono zasadę, że budynki mogą być fotografowane z wysokości nie wyższej niż 3 metry od poziomu ulicy i nakazano usunięcie twarzy osób oraz numerów rejestracyjnych pojazdów.

Generalny Inspektorat Danych Osobowych wielokrotnie kontrolował efekty pracy Google w Polsce. Sprawdzał m.in., czy zbierane były informacje o danych dotyczących sieci bezprzewodowych Wi-Fi⁷⁴. W 2011 r. przeprowadził kompleksową kontrolę, która miała na celu ustalenie zgodności przetwarzania danych przy użyciu urządzeń i systemów

⁶⁵ ES, Rekordowa kara dla Google, Forbes, <http://www.forbes.pl/styl-zycia/artykul/Technologie/rekordowa-kara-dla-google,12756,1> (dostęp z 1.1.2015 r.).

⁶⁶ *B. Gubernat*, Google Street View podgląda Polskę. Czy byli już u Ciebie? Fundacja Panoptykon, <http://panoptykon.org/wiadomosc/google-street-view-podglada-polske-czy-byli-juz-u-ciebie> (dostęp z 1.1.2015 r.).

⁶⁷ *L. Dapkus*, Lithuania tax officials tap Street View to catch cheats, Boston Globe, <http://www.bostonglobe.com/business/2013/04/10/lithuania-tax-man-uses-google-maps-find-dodgers/VmEVRtYjsU1DdcB5xWiQDK/story.html> (dostęp z 1.1.2015 r.).

⁶⁸ Mig, AP. Washington Post: NSA włamała się do centrów przetwarzania danych Google i Yahoo, http://m.wiadomosci.gazeta.pl/wiadomosci/1,117915,14873247,_Washington_Post__NSA_wlamala_sie_do_centrow_przetwarzania.html (dostęp z 1.1.2015 r.).

⁶⁹ *I. Lipowicz*, O mądre i wrażliwe państwo, <http://www.brpo.gov.pl/sites/default/files/Biuletyn%20RPO-Materia%C5%82y%20nr%2080.pdf> (dostęp z 1.1.2015 r.).

⁷⁰ Google StreetView to usługa, która pokazuje panoramiczne widoki z poziomu ulicy i pozwala użytkownikom na wyświetlanie wybranych części świata, w tym Polski.

⁷¹ *I. Spiecker gen. Dohmann*, „Prywatny pomiar świata” jako problem ochrony danych. O obchodzeniu się z informacją przestrzenną na przykładzie Google StreetView, [w:] *G. Szpor, W.R. Wiewiórowski* (red.), Internet. Prawno-informacyjne problemy sieci, portali i e-usług, Warszawa 2012, s. 73.

⁷² *J. Korbik*, Niemieckie rozdwojenie jaźni, czyli kto się boi Google StreetView, <http://www.cafebabel.pl/spoeczenstwo/artykul/niemieckie-rozdwojenie-jazni-albo-kto-sie-boi-google-street-view.html> (dostęp z 1.1.2015 r.).

⁷³ *I. Spiecker gen. Dohmann*, Prywatny pomiar świata jako..., s. 76.

⁷⁴ *G. Szpor*, Problemy administracyjnoprawne związane z ekspansją Internetu, [w:] *G. Szpor, W.R. Wiewiórowski* (red.), Internet. Prawno-informacyjne problemy sieci, portali i e-usług, Warszawa 2012, s. 77-78.

informatycznych z przepisami o ochronie danych osobowych⁷⁵. Sprawdzono również warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Do uchybień w zakresie działania usługi zaliczono m.in. niewyznaczenie przez Google administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad związanych z właściwym zabezpieczaniem danych osobowych. Ponadto wbrew przepisom ustawy o ochronie danych osobowych kierowcom samochodów należących do Google'a, na których zamontowane zostały urządzenia służące do rejestracji obrazu widoku ulicy, nie zostały nadane upoważnienia do przetwarzania danych osobowych. Kierowcy mają dostęp do obrazu kontrolnego, dzięki któremu dokonują oceny jakości i poprawności wykonywanych zdjęć oraz są odpowiedzialni za bezpieczeństwo dysków twardych, na których są zapisywane wykonane zdjęcia. W związku z tym kierowcy uczestniczą w procesie przetwarzania danych osobowych i administrator powinien nadać im upoważnienia do ich przetwarzania oraz wpisać ich do odpowiedniej ewidencji. Google nie zawarł również w opracowanej przez siebie polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, oraz sposobu przepływu danych pomiędzy poszczególnymi systemami. Według GODO nieprawidłowości te dotyczą jedynie formalnej strony działalności i nie mają wpływu na ewentualny wyciek danych lub możliwości przekazywania ich podmiotom nieupoważnionym. Koncern skorygował swoją działalność zgodnie z zaleceniami GODO⁷⁶.

Stanowisko unijnej Grupy Roboczej ds. ochrony danych ustanowionej na mocy art. 29⁷⁷ zaleca, by w przypadku StreetView okres przechowywania źródłowych zdjęć ulic, które po anonimizacji są zamieszczane w Internecie, wynosił maksymalnie sześć miesięcy. W Polsce niszczenie zdjęć źródłowych następuje zaraz po anonimizacji⁷⁸.

Działalność serwisu w zakresie prawa do prywatności nadal w naszej opinii nie chroni wystarczająco użytkowników. Mimo możliwości usunięcia niechcianych obrazów z serwisu Google w swojej polityce prywatności zastrzega prawo do nieuwzględniania żądań wielokrotnie przesyłanych, wymagających nieproporcjonalnych nakładów prac technicznych (np. opracowania nowego systemu lub całkowitej zmiany dotychczasowej praktyki), stwarzających ryzyko naruszenia prywatności innych osób, skrajnie trudnych do zrealizowania (m.in. dotyczących informacji znajdujących się w systemach kopii zapasowych). Kontrowersyjne jest również zastrzeżenie, że niepoprawne dane o użytkownikach, co do których został zgłoszony wniosek o zmianę, mogą zostać zachowane przez serwis w „uzasadnionych celach biznesowych lub prawnych”. Niestety, próżno szukać definicji owych „uzasadnionych celów”, jest to pojęcie na tyle szerokie, że pozwala zachowywać każde dane. Co więcej, usunięte dane i obrazy nie zawsze są natychmiast usuwane z aktywnych serwerów oraz mogą

nadal być przechowywane w systemach kopii zapasowych⁷⁹. Serwis Google Maps zbiera również informacje o użytkownikach, w tym o ich lokalizacji. Od niedawna, gdy wpisemy imię i nazwisko danej osoby, w serwisie wyświetli się lokalizacja, w której najczęściej przebywają.

W naszym kraju podobny zakres usług, które świadczy Google StreetView, oferowany jest przez inne serwisy, takie jak Zumi czy Norc. Założyć należy, że dynamiczny rozwój Internetu będzie doprowadzać do mnożenia się takich i podobnych serwisów. W związku z tym GODO wraz z Rzecznikiem Praw Obywatelskich opracowują zasady umieszczania zdjęć miejsc publicznych w Internecie⁸⁰.

Podsumowanie

W opinii polskiego Rzecznika Praw Obywatelskich polski system prawny zapewnia wysoki standard ochrony autonomii informacyjnej jednostki wyrażonej na poziomie Konstytucji i skonkretyzowany w wielu ustawach⁸¹. Pokrzywdzony upublicznieniem zdjęć w serwisie może przede wszystkim powoływać się na przepisy prawa cywilnego. Jak stanowi art. 23 KC, dobra osobiste człowieka, takie jak wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Warto zwrócić uwagę na art. 81 ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych⁸², który stanowi, że rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej, a zezwolenia nie wymaga rozpowszechnianie wizerunku osoby stanowiącej jedynie szczegółowości, takiej jak zgromadzenie, krajobraz, publiczna impreza. Pamiętać należy, że o dokonaniu naruszenia dobra osobistego decyduje obiektywna ocena, a nie subiektywne odczucie osoby zainteresowanej⁸³.

Działalność StreetView może stanowić zagrożenie dla ochrony dóbr osobistych czy praw autorskich (utworów architektonicznych, architektoniczno-urbanistycznych,

⁷⁵ Chodzi głównie o ustawę z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.) oraz rozporządzenie MSWiA z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

⁷⁶ Google StreetView z uchybieniami, http://giodo.gov.pl/1520001/id_art/4176/j/pl (dostęp z 1.1.2015 r.).

⁷⁷ Niezależny europejski organ doradczy, powołany na mocy art. 29 dyrektywy 95/46/WE.

⁷⁸ Zob. o usłudze StreetView, http://www.giodo.gov.pl/1520001/id_art/3387/j/pl (dostęp z 1.1.2015 r.).

⁷⁹ Polityka prywatności usługi Google Maps, <https://maps.google.com/intl/pl/policies/privacy/> (dostęp z 1.1.2015 r.).

⁸⁰ S. Czubkowska, GODO sprawdza legalność Google StreetView, http://prawo.gazetaprawna.pl/artykuly/464750,giodo_sprawdza_legalnosc_google_street_view.html (dostęp z 1.1.2015 r.).

⁸¹ S. Trociuk (red.), Biuletyn Rzecznika Praw Obywatelskich 2014, Nr 1, s. 74.

⁸² T.j. Dz.U. Nr 90, poz. 631 ze zm.

⁸³ Wyrok SA w Łodzi z 28.8.1996 r., I ACr 341/96, OSA 1997, Nr 7–8, poz. 43, s. 42.

urbanistycznych, innej twórczości typu *street art*, rzeźb). Według *M. Siwickiego* stosowana przez koncern anonimizacja nie wyłącza odpowiedzialności tego podmiotu ze względu na naruszenie prywatności i prawa do wizerunku. Zwraca on również uwagę na fakt, że osoba na zdjęciach powinna mieć także prawo decydowania o formie i zakresie obróbki graficznej, więc samo zgłoszenie żądania uczynienia nierozpoznawalnym wizerunku zainteresowanego jest niewystarczające do uniknięcia odpowiedzialności koncernu z tytułu odpowiedzialności za naruszenie dóbr osobistych⁸⁴. W Polsce nie doszło jeszcze do żadnych postępowań sądowych związanych z działalnością usługi. Warto jednak zwrócić uwagę na mogące się pojawić w przyszłości problemy dotyczące właściwości miejscowej sądu. Jak zwrócono uwagę we wspomnianym już francuskim orzeczeniu, Google posiada na terenie UE oddziały, w tym również w Polsce. Posiadają one różne specjalizacje. Z punktu widzenia właściwości miejscowej należy brać pod uwagę np. siedzibę administratora serwisu i lokalizację urzędów służących do pozyskiwania danych⁸⁵.

W wymiarze unijnym warto zwrócić uwagę m.in. na art. 8 KPP UE gwarantujący prawo osób fizycznych do ochrony danych osobowych i dyrektywę o ochronie danych osobowych i swobodnym przepływie tych danych⁸⁶. Dla Europejczyków sfera prywatności i ochrony danych jest niezwykle istotna, co znajduje potwierdzenie w liczbie pytań kierowanych corocznie do Parlamentu Europejskiego. Większość odnosiła się do ochrony danych w kontekście funkcjonowania nowych technologii i w związku z tym przestrzegania zasad ochrony danych przez państwa trzecie.

Doświadczenia europejskich krajów posłużyły instytucjom unijnym w wypracowywaniu standardów ochrony prawa do prywatności. Unia będzie się skupiać w swojej działalności na: wzmocnieniu praw osób fizycznych (np. przez zwiększenie przejrzystości i wzmocnienie kontroli nad danymi osobowymi), poprawie sytuacji w zakresie aspektów ochrony danych związanych z rynkiem wewnętrznym (przez zmniejszenie obciążeń administracyjnych oraz zagwarantowanie równych szans), rewizji przepisów o ochronie danych w obszarze współpracy policyjnej i współpracy wymiarów

sprawiedliwości w sprawach karnych, aby dane osobowe były objęte wysokim poziomem ochrony w tych dziedzinach, również wówczas gdy są one przesyłane poza granice UE, a także bardziej skuteczne egzekwowanie tych przepisów (w tym poprzez wzmocnienie i dalszą harmonizację roli i uprawnień organów ochrony danych)⁸⁷.

Jak słusznie zwrócono uwagę na konferencji inauguracyjnej działalność projektu PHAENDRA⁸⁸ dotyczącej współpracy i koordynacji między organami ochrony danych osobowych w UE, nawet największe wysiłki organów nie są w stanie nadążyć za dynamiką Internetu. Prywatność miliardów użytkowników Internetu⁸⁹ jest zagrożona, i to zarówno ze strony przedsiębiorstw, jak i instytucji państwowych. Internet w rękach jednych jest narzędziem do osiągania zysków za wszelką cenę, w rękach drugich – narzędziem sprawowania kontroli nad obywatelami. Często nieświadomi zagrożeń użytkownicy umieszczają w Internecie tzw. dane wrażliwe. Pierwszy raz wiedza o tak wielu jest dostępna tak powszechnie, co wymaga wypracowania nowych metod działania. Zarówno Polska, jak i UE muszą znaleźć sposoby skutecznego oddziaływania na rosnące w siłę koncerny internetowe, a także muszą chronić prywatność swoich obywateli również przed ingerencją innych państw.

⁸⁴ *M. Siwicki*, Google StreetView a ochrona prywatności, wizerunku i praw autorskich, MoP 2014, Nr 18 <http://czasopisma.beck.pl/monitor-prawniczy/artukul/emgoogle-street-viewem-a-ochrona-prywatnosc-i-wizerunku-i-praw-autorskich/> (dostęp z 1.5.2015 r.)

⁸⁵ *P.A. Kozyra*, Twórcy aplikacji i dane osobowe. Rozmowa z Generalnym Inspektorem Danych Osobowych dr. Wojciechem Rafałem Wiewiórkowskim, Nowoczesne Zarządzanie 2014, Nr 1, s. 53.

⁸⁶ Dyrektywa 95/46/WE.

⁸⁷ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej, KOM(2010) 609 wersja ostateczna, Bruksela, 4.11.2010 r., http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pl.pdf (dostęp z 1.5.2015 r.)

⁸⁸ Rozpoczęcie projektu badawczego UE w zakresie wspierania współpracy między organami ochrony danych, Oświadczenie prasowe z 20.2.2013 r.

⁸⁹ *A. Kozłowski*, ONZ: 3 mld użytkowników Internetu w 2015 roku, <http://pclub.pl/news57631.html> (dostęp z 1.1.2015 r.).

Right for privacy in the era of the Internet

In the present study, the authors relate to the problem of security of privacy. It is very important in the era of generally available Internet where the borders of privacy are becoming less and less clear. With the development of the Internet, personal data access is easier along with possibilities of its free creation. Considering the fact that privacy of billions of Internet users is in danger, both from enterprises and state institutions, authors of the study emphasize the necessity of developing, by Poland and EU, mechanism that will protect that privacy.