Łukasz Prus

Ochrona praw podstawowych w internetowym procesie przetwarzania danych osobowych w Unii Europejskiej

Abstrakt

Współcześnie rola ochrona praw podstawowych nabiera nowego znaczenia wraz z rozwojem technologii w dziedzinie Internetu. W tej przestrzeni prawnej często dochodzi do konfliktu pomiędzy prawami podstawowymi administratora danych, osoby, której dotyczą oraz wszystkich użytkowników Internetu. A zatem konfliktu praw w relacjach horyzontalnych pomiędzy równorzędnymi podmiotami. Artykuł stara się dostarczyć odpowiedzi na pytanie, czy strony tego stosunku prawnego mogą skutecznie dochodzić ochrony na podstawie norm prawa administracyjnego. W publikacji zbadano trzy sytuacje dotyczące ochrony praw podstawowych, tj.: 1) publikacja danych osobowych na stronie internetowej, 2) dane osobowe jako wynik wyszukiwania, 3) adres IP jako dane osobowe.

Słowa kluczowe

prawa podstawowe, nowe technologie, ochrona danych osobowych w Internecie, wyszukiwarki internetowe, adres IP.

Wstęp

W 1890 r. S.D. Warren i L.D. Brandeis pisali, że „najnowsze wynalazki i metody biznesowe" takie jak fotografie i gazety naruszyły święte obszary życia prywatnego[1]. Autorzy podkreślili, że zmiany polityczne, społeczne i gospodarcze wymagają ponownego przemyślenie klasycznych praw, a nawet czasem prowadzą do uznania nowych[2]. Prawo powinno sprostać aktualnym wyzwaniom i zapotrzebowaniu społecznemu. Współcześnie ochrona praw podstawowych nabiera większego znaczenia wraz z rozwojem nowych

[1] S.D. Warren, L.D. Brandeis, *The Right of Privacy*, „Harvard Law Review" 1890, Vol. 4, Nr 5, s. 195; opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r. w sprawie C-131/12, *Google*, ECLI:EU:C:2013:424, pkt 1.

[2] Autorzy dokładnie pisali: „that the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. [...] This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations, which came with the advance of civilization, made it, clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature. Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right to be let alone", S.D. Warren, L.D. Brandeis, *op. cit.*, s. 193-195.

technologii[3]. Postęp w dziedzinie Internetu usunął ograniczenia w komunikowaniu się na odległość i zrewolucjonizował sposoby przetwarzania danych osobowych. Wszelkie dane mogą być natychmiast udostępnienie w formacie cyfrowym na całym świecie. Z jednej strony, sytuacja ta przynosi społeczne korzyści w wymianie informacji[4]. Z drugiej strony, tego rodzaju sytuacje mogą stać się płaszczyzną konfliktu pomiędzy prawami podstawowymi administratora danych, osoby której dotyczą, oraz wszystkich użytkowników Internetu[5]. Warto przy tym zauważyć, że administratorem danych może być zarówno organ administracji publicznej, jak i podmiot prawa prywatnego. Podjęte rozważania dotyczą tylko tego drugiego przypadku, tj. relacji horyzontalnych pomiędzy równorzędnymi podmiotami. Powstaje więc pytanie, czy strony tego stosunku prawnego mogą skutecznie dochodzić ochrony na podstawie norm prawa administracyjnego. Jednocześnie należy pamiętać, że pojęcie praw podstawowych jest znaczeniowo zbliżone do cywilistycznej konstrukcji dóbr osobistych (art. 23-24 i art. 448 k.c.)[6]. Ogólnie rzecz ujmując, można przyjąć, że każdemu dobru osobistemu odpowiada konkretne prawo podstawowe np. prawo ochrony prywatności, wizerunku, danych osobowych, własności intelektualnej, itd. W takich sytuacjach w grę wchodzą różne środki ochrony praw podstawowych (dóbr osobistych). Polski ustawodawca w art. 24 § 3 k.c. przesądził o niezależności cywilnoprawnych instrumentów ochrony od administracyjnoprawnych i karnoprawnych. Dopuszczalna jest nawet kumulacja środków ochrony, z tym zastrzeżeniem, że co do wysokości restytucji i kompensacji szkody jest ona limitowana przepisami o bezpodstawnym wzbogaceniu[7]. Niemniej jednak w unijnej przestrzeni prawnej jednostki coraz częściej korzystają z administracyjnoprawnych środków ochrony praw podstawowych. Można więc postawić tezę, że w dobie rozwoju nowych technologii, ochrona praw podstawowych pozostaje pod rządem prawa administracyjnego UE.

W celu usystematyzowania dalszych rozważań należy podkreślić, że w procesie przetwarzania danych osobowych w Internecie wyróżnia się trzy sytuacje dotyczące ochrony praw podstawowych[8]:

1) publikacja danych osobowych na stronie internetowej,
2) dane osobowe jako wynik wyszukiwania,
3) adres IP jako dane osobowe.

[3] Opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r. …, pkt 2.

[4] *Ibidem*.

[5] Zob. opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 10 lipca 2014 r. w sprawie C-212/13, *Ryneš*, ECLI:EU:C:2014:2072, pkt 22.

[6] Zob. M. Pazdan, *Dobra osobiste i ich ochrona*, [w:] M. Safjan (red.), *System prawa prywatnego, tom 1. Prawo cywilne – część ogólna*, Warszawa 2012, s. 1231-1233; S. Dmowski, R. Trzaskowski, [w:] J. Gudowski (red.), *Kodeks cywilny. Komentarz. Część ogólna*, Warszawa 2014, s. 129-130.

[7] Przepis art. 24 § 3 K.c. stanowi, że kodeksowe roszczenia nie uchybiają uprawnieniom przewidzianym w innych przepisach. Co do kumulacji środków ochrony prawnej zob. wyrok Sądu Najwyższego z dnia 27 marca 2003 r., V CKN 4/01, niepubl.

[8] Zob. opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r. …, pkt 3.

1. Ochrona przed publikacją danych osobowych na stronach internetowych

W pierwszej sytuacji relewantna jest sprawa B. Lindqvist, która stworzyła stronę dla parafian. Na prywatnej stronie opublikowała informacje na temat członków tej wspólnoty, często wskazując ich z imienia i nazwiska. Autorka z dużą dozą humoru opowiadała m.in. o sposobie spędzania przez nich czasu wolnego. Opisywała także zdarzenia z ich życia rodzinnego, publikowała numery telefonu i inne dane. Jednocześnie nie uzyskała na to zgody tych osób i nie zgłosiła swoich działań do organu ochrony danych osobowych. Jednakże niezwłocznie po powzięciu informacji o braku zgody niektórych parafian, Pani B. Lindqvist skasowała swoją stronę[9]. W tych okolicznościach powstał spór o to, czy rozpowszechnienie na prywatnej stronie danych w postaci nazwiska lub numeru telefonu stanowi przetwarzanie danych osobowych zgodnie dyrektywą 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 (dalej jako dyrektywa)[10]. Odpowiadając na tak zadane pytanie, Trybunał przypomniał, że po myśli art. 3 ust. 1 zd. 1 dyrektywy[11] przez pojęcie danych osobowych należy rozumieć „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". Bezsprzecznie w tej definicji mieści się publikowanie nazwiska wraz z numerem telefonu. Stosownie zaś do art. 2 lit. b dyrektywy[12] przetwarzanie takich danych oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, takich jak np. transmisja, rozpowszechnianie lub udostępnianie w inny sposób. Trzeba przy tym wyjaśnić, że publikowanie danych na stronie internetowej wymaga użycia właściwych procesów informatycznych, aby uczynić stronę dostępną dla użytkowników. Tego rodzaju operacje częściowo realizowane są w sposób zautomatyzowany. A zatem publikacja na stronie internetowej danych pozwalających zidentyfikować osoby, których one dotyczą, stanowi przetwarzanie danych osobowych w sposób zautomatyzowany w rozumieniu dyrektywy[13]. Innymi słowy, wydawca strony internetowej zawierającej dane osobowe jest ich administratorem i ponosi z tego tytułu odpowiedzialność[14].

[9] Wyrok TS z dnia 3 listopada 2003 r., w sprawie C-101/01, *Lindqvist*, ECLI:EU:C:2003:596, pkt 12-14. Podstawą tej sprawy był spór karny, jednak wnioski, jakie można wyprowadzić z wyroku Trybunału, mają charakter ogólny.

[10] Dz.Urz. L 2817, 23.11.1995, s. 31-50. W dniu 25 maja 2018 r. wejdzie w życie nowe 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) z dnia 27 kwietnia 2016 r. (Dz. Urz. L 119, s. 1), dalej jako RODO.

[11] Zob. art. 2 ust. 1 i art. 4 pkt 1 RODO.

[12] Zob. art. 4 pkt 2 RODO.

[13] Wyrok TS z dnia 3 listopada 2003 r., w sprawie C-101/01, pkt 24-27.

[14] Opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r. …, pkt 39.

Jednakże B. Linqvist podniosła, że w tym zakresie dochodzi do kolizji pomiędzy prawem do prywatności i wolności wypowiedzi (art. 11 ust. 1 KPP[15]). Wymogi prawne przewidujące warunek uprzedniego uzyskania zgody organu nadzoru i zakaz przetwarzania wrażliwych danych osobowych w jej ocenie są sprzeczne z ogólną zasadą swobody wypowiedzi. Dalej argumentowała, że wymiennie z nazwiska konkretnej osoby, tj. informacji „powszechnie znanej i banalnej" nie wyczerpuje znamion istotnego naruszenia prawa do prywatności[16]. Zdaniem Trybunału zarzut ten był chybiony, ponieważ prawo UE w zakresie ochrony danych osobowych nie zawiera ograniczeń sprzecznych z zasadą ogólną swobody wypowiedzi[17].

B. Lindqvist zauważyła jednak, że przetwarzała dane na własny użytek, gdyż nie stworzyła strony w ramach prowadzonej działalności gospodarczej. Jej strona internetowa miała charakter niezarobkowy i religijny. W jej ocenie autorka prywatnej strony stworzonej w ramach czynności o czysto osobistym lub domowym charakterze nie ma obowiązku uzyskania zgody organu na przetwarzanie danych osobowych[18]. Trybunał nie podzielił tych uwag. W myśl art. 3 ust. 2 *in fine* dyrektywa nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze[19]. Tymczasem dostęp do informacji upublicznionych na stronie internetowej może mieć nieograniczona liczba osób na całym świecie. Innymi słowy, utworzenie strony potencjalnie dostępnej dla wszystkich nie może być uznane za przetwarzanie danych „w trakcie czynności o czysto osobistym lub domowym charakterze"[20]. Decyduje więc nie tyle przeznaczenie strony, lecz jej dostępność.

O ile wykładnia Trybunału w jasny sposób przedstawia reguły udostępnienia danych osobowych w Internecie, to w doktrynie zauważono, że teza ta nie jest adekwatna do portali społecznościach takich jak np. *Facebook* lub *Instagram*[21]. W opinii z 2009 r. grupy roboczej do spraw ochrony jednostek w zakresie przetwarzania danych osobowych (*Working Party on the Protection of Individuals with regard to the Processing of Personal Data*) podkreślono, że użytkownicy portali społecznościach działają przede wszystkim w sferze prywatnej, rodzinnej lub domowej. Dostęp do prywatnych profili użytkowników z reguły jest limitowany przez jego posiadacza poprzez zarządzenie siecią kontaktów i „znajomych". Grupa robocza podkreśliła, że przetwarzanie danych osobowych przez użytkowników tych portali stanowi czynności o osobistym charakterze, chyba że

[15] Karta Praw Podstawowych Unii Europejskiej z 7 grudnia 2000 r. (Dz. UE C 2007.303.1 z dnia 14 grudnia 2007 r.)

[16] Wyrok TS z dnia 3 listopada 2003 r., w sprawie C-101/01, pkt 73-74.

[17] *Ibidem*, pkt 80-88.

[18] *Ibidem*, pkt 30.

[19] Zob. art. 2 ust. 2 lit. c RODO.

[20] R. Wong, J. Savirimuthu, *All or nothing: this is the question?: The application of art. 3 (2) Data Protection Directive 95/46/EC to the Internet*, „John Marshall Journal of Computer and Information Law" 2007, No. 8, s. 246.

[21] *Ibidem*; Z. Warso, *Cyfrowe terytoria – gdzie przebiega granica sfery prywatnej w sieci? Analiza z punku widzenia przepisów o ochronie danych osobowych*, [w:] D. Bychowska-Sieniarska, D. Głowacka (red.), *Wirtualne media – realne problemy*, Warszawa 2014, s. 143.

dostęp do tych danych mają osoby trzecie spoza grona samodzielnie wybranych kontaktów[22]. Natomiast rzecznik generalny N. Jääskinen uznał, że każdy akt komunikacji dokonywany za pośrednictwem mediów społecznościach dotyczących danych osobowych stanowi domniemaną ingerencję w prawa podstawowe, która wymaga uzasadnienia[23]. Wbrew oczekiwaniom nowe rozporządzenie raczej nie przyniesie nowych rozwiązań tego problemu prawnego. Zgodnie z art. 2 ust. 2 RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. W motywie 18 RODO doprecyzowano, że działalność o charakterze osobistym lub domowym nie może pozostawać w związku działalnością zawodową lub handlową i może polegać w szczególności na korespondencji, przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej aktywności. Jednakże rozporządzenie ma zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej. Innymi słowy, prawne ograniczenia związane ochroną danych osobowych mają zastosowanie do posiadaczy profili portali społecznościowych, jeżeli udostępniają je na rzecz nieograniczonego kręgu odbiorców i przetwarzają dane osobowe. A zatem linia orzecznicza zapoczątkowana w sprawie *Lindqvist* zachowuje swoją aktualność pod rządami nowego prawa[24].

2. Wtórna odpowiedzialność dostawców usług wyszukiwania informacji w Internecie

Powszechny dostęp do informacji w Internecie opiera się na pracy wyszukiwarek internetowych (*web search engine*)[25]. Dla wielu użytkowników stanowią one punkt wyjścia w procesie wyszukiwania informacji. Dlatego celowe jest omówienie wtórnej odpowiedzialności dostawców usług wyszukiwania. Problem ten dobrze obrazuje sprawa *Google Spain SL*, *Google Inc.* przeciwko *Agencia Española de Protección de Datos* (dalej jako AEPD) i M. Costeja González. Hiszpańska gazeta opublikowała w tradycyjnej formie dwa ogłoszenia o aukcji nieruchomości należącej do M. Costeja Gonzáleza w związku z niespłaconymi długami na rzecz zakładu ubezpieczeń społecznych. Następnie informacje te zostały upublicznione w internetowym wydaniu dziennika. Według M. Costeja Gonzáleza po wprowadzeniu jego imienia i nazwiska do wyszukiwarki w wynikach wyświetlono link do opisanych dwóch ogłoszeń na stronach internetowych gazety, które wiązały jego osobę z długiem. Aukcja odbyła się wiele lat temu, egzekucja została zakończona, a ogłoszenie nie było już aktualne. Skarga administracyjna M. Costeja Gonzáleza została częściowo oddalona w zakresie dotyczącym gazety. Hiszpańska

[22] Opinia 5/2009 w sprawie portali społecznościowych, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_pl.pdf [dostęp 26.11.2017].

[23] Opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r.…, pkt 118.

[24] Zob. E. Bielak-Jomaa, D. Lubosz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 118 i n.

[25] Opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r.…, pkt 45.

agencja do spraw ochrony danych osobowych uznała, że publikacja opisanych ogłoszeń była prawnie uzasadniona, a jej celem było jak najszersze rozpowszechnienie informacji o licytacji, tak aby zapewnić skuteczność egzekucji. Jednakże AEPD uznała za zasadną skargę w zakresie dostawcy usług wyszukiwania, zobowiązując Google do przyjęcia środków niezbędnych do usunięcia danych osobowych skarżącego z wyników wyszukiwania i uniemożliwienia dostępu do tych danych w przyszłości. Google, kwestionując ten pogląd, twierdziło, że jako wyszukiwarka nie tworzy nowych danych i nie zmienia istniejących. Jedynie wskazuje, gdzie można znaleźć szukane hasła. Ponadto w ocenie Google, dostawca usług wyszukiwania nie jest administratorem danych, gdyż nie sprawuje kontroli nad danymi zamieszonymi na stronach osób trzecich. Operator wyszukiwarki jest jedynie pośrednikiem pomiędzy użytkownikami Internetu a właścicielami stron. Należy jednak odnotować, że rezultat wyszukiwania nie jest wynikiem przeszukania całej sieci, lecz opiera się na procesie zbierania treści przetworzonych przez wyszukiwarkę. Ponadto wyświetla ona dodatkowe treści wraz z linkiem, aby ułatwić użytkownikom korzystanie z wyników wyszukiwania[26]. Innymi słowy, wyszukiwarka w zautomatyzowany sposób gromadzi dane osobowe zamieszczone na innych stronach, zapisuje je, porządkuje, selekcjonuje, indeksuje i udostępnia według własnego uznania. A zatem operacje wykonywane przez wyszukiwarki internetowe spełniają przesłanki definicji legalnej „przetwarzania danych osobowych", o której mowa art. 2 lit. b dyrektywy. Bez znaczenia jest przy tym fakt, że dostawca tych usług jest jedynie pośrednikiem. W orzecznictwie utrwalony jest pogląd, że wtórne udostępnianie danych osobowych opublikowanych wcześniej w innych mediach wypełnia znamiona ich przetwarzania[27]. Trybunał uznał również, że operator wyszukiwarki internetowej jest administratorem danych, gdyż określa cele i sposoby tych operacji. Tym bardziej, że bez działalności wyszukiwarek użytkownik nie odnalazłby źródłowych stron internetowych publikujących dane osobowe.

Tak więc z jednej strony, wyszukiwarki jako instrument rozpowszechniania danych osobowych w wymiarze globalnym mogą znacząco oddziaływać na prawa podstawowe do poszanowania prywatności oraz ochrony tych danych[28]. Z drugiej strony, we współczesnym społeczeństwie informacyjnym prawo użytkownika Internetu do uzyskania informacji (art. 11 ust. 1 zd. 2 KPP) zasługuje na szczególną ochronę. W końcu zaś działalność operatorów wyszukiwarek stanowi przejaw wolności prowadzenia działalności gospodarczej w rozumieniu art. 16 KPP[29]. W kontekście tego konfliktu powstaje pytanie, czy administracja pośrednia i bezpośrednia UE może skutecznie egzekwować wobec podmiotów prywatnych prawo do bycia zapomnianym (*right to be forgotten*)[30]. Odpowiadając na tak zadane pytanie, rzecznik generalny N. Jääskinen wyjaśnił, że operatorzy wyszukiwarek nie mogą być obarczani obowiązkiem usuwania z ich zasobów

[26] *Ibidem*, pkt 34-35.

[27] Wyrok TS z dnia 13 maja 2014 r. w sprawie C-131/12, *Google Spain SL i Google Inc. v. (AEPD) i M. Costeja Gonzálezowi*, ECLI:EU:C:2014:317, pkt 30.

[28] *Ibidem*, pkt 36 i 38.

[29] Opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r.…, pkt 119-125

[30] *Ibidem*, pkt 133.

legalnie uzyskanych informacji. Odmienny pogląd w jego ocenie skutkowałby cenzurą[31]. Inaczej orzekł Trybunał, przyjmując pewną gradację konkurencyjnych praw podstawowych. Po pierwsze, mając na względzie potencjalne konsekwencje uzyskania listy wyników wyszukiwania zawierających dane osobowe, ingerencja w prawo do prywatności i ochrony danych osobowych nie może być uzasadniona jedynie interesem gospodarczym operatora wyszukiwarki[32]. Po drugie, prawo do prywatności i ochrony danych osobowych należy uznać za nadrzędne wobec prawa do uzyskania informacji, chyba że ze względu na rolę osoby w życiu publicznym należy uznać, iż ingerencja w prawa podstawowe jest uzasadniona nadrzędnym interesem i prawem użytkowniku Internetu do informacji[33]. Odmowa ochrony z tego tytułu może więc nastąpić np. wobec aktywnych w życiu publicznym polityków, urzędników organów administracji publicznej, o ile przetwarzane dane mają związek z ich pracą lub osób skazanych prawomocnymi wyrokami, chyba że nastąpiło zatarcie skazania.

3. Prawo do bycia zapomnianym

Rozwój Internetu doprowadził więc do uznania przez Trybunał nowego prawa podstawowego, czyli prawa do bycia zapomnianym, które znajduje swoje umocowanie w art. 7-8 KPP. Osoba, której dane dotyczą, ma prawo, aby jej dane osobowe, w szczególności imię i nazwisko, zostały usunięte z wyników wyszukiwania, jeżeli dane te nie są już konieczne. Może się nawet zdarzyć tak, że początkowo uzasadnione przetwarzanie danych osobowych z czasem staje się zbędne. Nie jest zatem konieczne udostępnianie tych danych w świetle celów, dla których pierwotnie były przetwarzane. Tak też było w przypadku M. Costeja Gonzáleza. Wynik wyszukiwania prowadzonego za pomocą imienia i nazwiska odsyłał do dwóch ogłoszeń o aukcji jego nieruchomości. Wprawdzie początkowo interes publiczny wymagał upublicznienia tego rodzaju informacji w celu zapewnienia skuteczności egzekucji, niemniej jednak po 16 latach wiązanie imienia i nazwiska M. Costeja Gonzáleza z długami, które zostały spłacone, nie było uzasadnione tym celem. Innymi słowy, oceniając zasadność prawa do bycia zapomnianym, należy brać pod uwagę nie tylko cechy podmiotowe (rolę w życiu publicznym), lecz również przedmiotowe, czyli aktualność celu przetwarzania tych danych[34].

W końcu należy zbadać, czy rejestracja adresów IP może naruszać prawa podstawowe. Wpierw jednak należy omówić istotę adresów IP i ocenić, czy stanowią one nową kategorię danych osobowych. Rzecznik generalny M. Compos Sanchez-Bordony wyjaśnił, że adres IP to ciąg liczb binarnych, przydzielany urządzeniu (komputerowi, tabletowi, smartfonowi itd.), które go identyfikuje i umożliwia dostęp do sieci. Adres IP jest przesyłany do serwera, na którym zarejestrowana jest strona internetowa[35]. Tego rodzaju infor-

[31] *Ibidem*, pkt 135 i 136.

[32] Wyrok TS z dnia 13 maja 2014 r. w sprawie C-131/12, pkt 81 i 97.

[33] *Ibidem*, pkt 97.

[34] *Ibidem*, pkt 99.

[35] Opinia rzecznika generalnego M. Camposa Sancheza-Bordony przedstawiona w dniu 12 maja 2016 r., w sprawie C582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:339, pkt 1; wyrok TS

macje mogą określać zainteresowania użytkowania Internetu. A zatem ingerować w prawa podstawowe określne w art. 7-8 KPP. Jednakże dostawcy dostępu do sieci internetowej (firmy telekomunikacyjne) przyznają użytkownikom Internetu statyczny lub dynamiczny adres IP. Statyczny adres IP to niezmienny ciąg liczb binarnych przypisany do komputera łączącego się z siecią. Dynamiczny adres IP zmienia się przy każdy nowym połączeniu[36]. Decydującą przesłanką w rozstrzygnięciu, czy adres IP stanowi dane osobowe w rozumieniu art. 2a dyrektywy, jest możliwość zidentyfikowania za jego pomocą konkretnej osoby. Z tej perspektywy statyczny adres IP stanowi prawnie chronione dane osobowe, które pozwalają na precyzyjną identyfikację użytkowników Internetu[37]. Jednakże dynamiczny adres IP sam w sobie nie wystarczy, aby zidentyfikować urządzenie, które łączy się z siecią[38].

Przedstawiony problem prawny był przedmiotem rozpoznania w sprawie P. Breyera, który systematycznie przeglądał strony niemieckich służb federalnych. Właściciele stron byli dostawcami usług internetowych, czyli podmiotami prawa prywatnego. Większość tych portali rejestrowała każde logowanie w celu ochrony przed atakami. Administratorzy stron przechowywali m.in. dzień i godzinę logowania oraz adres IP. P. Breyer w skardze skierowanej do sądu administracyjnego domagał się zakazania przechowywania dynamicznego adresu IP[39]. Następnie sprawa była przedmiotem rozpoznania w trybie pytania prejudycjalnego. Z jednej strony Trybunał podkreślił, że dynamiczny adres IP nie dostarcza danych odnoszących się do zidentyfikowanej osoby, jako że taki adres nie wskazuje wprost tożsamości właściciela komputera lub innej osoby, która mogłaby z niego korzystać. Z drugiej jednak strony może zdarzyć się tak, że firma teleinformatyczna dysponuje dodatkowymi informacjami, które w połączeniu z dynamicznym adresem IP, zarejestrowanym przez właściciela strony, umożliwi pośrednią identyfikację użytkownika[40]. Zgodnie z art. 2 lit. a) dyrektywy osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny. Ponadto w motywie 26 dyrektywy wyjaśniono, że w celu ustalenia, czy można określić konkretnego użytkownika, należy wziąć pod uwagę wszystkie sposoby, jakimi można posłużyć się w celu zidentyfikowania takiej osoby. Skoro więc tego rodzaju informacje mogą, racjonalnie rzecz biorąc, pośrednio identyfikować użytkownika, nie jest konieczne, aby wszystkie dane były rejestrowane tylko przez jeden podmiot. W analizowanej sprawie ustalono, że właściciel strony internetowej mógł domagać się, aby organ wymiaru sprawiedliwości zobowiązał firmę telekomunikacyjną do przedstawienia dodatkowych informacji umożliwiających wszczęcie postępowania

z dnia 19 października 2016 r. w sprawie C582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI: EU:C:2016:779, pkt 15.

[36] Opinia rzecznika generalnego M. Camposa Sancheza-Bordony przedstawiona w dniu 12 maja 2016 r. …, pkt 2.

[37] Zob. *ibidem,* pkt 6; wyrok TS z dnia 24 listopada 2011 r. w sprawie C70/10, *Scarlet Extended,* ECLI: EU:C:2011:771, pkt 51.

[38] Opinia rzecznika generalnego M. Camposa Sancheza-Bordony przedstawiona w dniu 12 maja 2016 r. …, pkt 7.

[39] Wyrok TS z dnia 19 października 2016 r. w sprawie C582/14, pkt 17-30.

[40] *Ibidem*, pkt 37-39.

karnego. W konkluzji Trybunał uznał, że dynamiczny adres IP zarejestrowany przez właściciela strony internetowej stanowi dane osobowe, o ile dysponuje on środkami prawnymi umożliwiającymi pośrednie zidentyfikowanie osoby w połączeniu z dodatkowymi informacjami, jakimi dysponuje dostawca dostępu do Internetu[41]. Co więcej, Trybunał zastrzegł, że art. 7 lit. f dyrektywy sprzeciwia się regulacjom krajowym dopuszczającym przetwarzanie danych osobowych bez uprzedniego właściwego wyważania dostępności mediów online z prawami podstawowymi ochrony życia prywatnego i danych osobowych użytkowników Internetu[42].

Zakończenie

Z ogółu podjętych rozważań wynika, że tradycyjne prawa podstawowe korygują i dostosowują sytuację prawną jednostek, a często nawet prowadzą do sformułowania nowych praw podstawowych. Tym samym wprowadzają one wyższe standardy ochrony w szybko zmieniającej się przestrzeni prawnej UE[43]. Ponadto normy prawa administracyjnego wprowadzają efektywne i innowacyjne instrumenty ochrony praw podstawowych również w relacjach horyzontalnych pomiędzy równorzędnymi podmiotami.

Protection of fundamental rights in the online process of personal data processing in the European Union

Abstract

In nowadays protection of fundamental rights takes on new importance together with the development of technologies in the field of Internet. In this legal space, there is often a conflict between the fundamental rights of the data controller, person whose these data concern and all of the users of Internet. Thus the conflict of rights in horizontal relations between equivalent entities. The article tries to answer the question whether parties of this legal relationship are allowed to effectively seek protection based on the rules of administrative law. The article analyzes three situations concerning the protection of fundamental rights: 1) publication of personal data on the website, 2) personal data as a result of the search, 3) IP address as a personal data.

Key words

fundamental rights, new technologies, data protection in Internet, web search engine, IP address.

Dr Łukasz Prus – adiunkt w Zakładzie Porównawczej Administracji Publicznej Instytutu Nauk Administracyjnych na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

[41] Wyrok TS z dnia 19 października 2016 r. w sprawie C582/14, pkt 41-49.

[42] *Ibidem*, pkt 62-64.

[43] O pojęciu-narzędziu przestrzeni prawnej zob. F. Longchamps, *Z problemów poznania prawa*, Wrocław 1968, s. 41; Ł. Prus, *Przestrzeń prawna jako narzędzie badawcze europejskiej kultury prawnej*, [w:] J. Zimmermann (red.), *Przestrzeń w prawie administracyjnym*, Warszawa 2013, s. 25 i n.

Literatura

Bielak-Jomaa E., Lubosz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018

Dmowski S., Trzaskowski R., [w:] J. Gudowski (red.), *Kodeks cywilny. Komentarz. Część ogólna*, Warszawa 2014

Longchamps F., *Z problemów poznania prawa*, Wrocław 1968

Pazdan M., *Dobra osobiste i ich ochrona*, [w:] M. Safjan (red.), *System prawa prywatnego, tom 1. Prawo cywilne – część ogólna*, Warszawa 2012

Prus Ł., *Przestrzeń prawna jako narzędzie badawcze europejskiej kultury prawnej*, [w:] J. Zimmermann (red.), *Przestrzeń w prawie administracyjnym*, Warszawa 2013

Warren S.D., Brandeis L.D., *The Right of Privacy*, „Harvard Law Review" 1890, Vol. 4, No. 5

Warso Z., *Cyfrowe terytoria – gdzie przebiega granica sfery prywatnej w sieci? Analiza z punku widzenia przepisów o ochronie danych osobowych*, [w:] D. Bychowska-Sieniarska, D. Głowacka (red.), *Wirtualne media – realne problemy*, Warszawa 2014

Wong R., Savirimuthu J., *All or nothing: this is the question?: The application of art. 3 (2) Data Protection Directive 95/46/EC to the Internet*, „John Marshall Journal of Computer and Information Law" 2007, No. 8