STUDIA Koszalińsko-Kołobrzeskie

26 | 2019
DOI: 10.18276/skk.2019.26-16
s. 307–326

Krzysztof Łuszczek[1]

POLITYKA MEDIALNA UNII EUROPEJSKIEJ WOBEC PROBLEMU OCHRONY PRYWATNOŚCI W NOWYCH MEDIACH

Wstęp

Już starożytni rozdzielali sferę działalności publicznej od tego, co było zarezerwowane wyłącznie dla sfery wewnętrznej, domowej. Chociaż akcenty rozkładali inaczej niż my to dziś robimy. Arystoteles rozgraniczał sferę aktywności politycznej *polis* od rodzinnej zwanej *oikos*. Sfera publiczna była zarezerwowana przede wszystkim ludziom wolnym, natomiast *oikos* służyło przede wszystkim zabezpieczeniu potrzeb materialnych. Stąd dopuszczano do niej także niewolników. Relacje w *oikos* były więc odmienne niż w *polis*[2].

W toku rozwoju cywilizacji *oikos* nabierało znaczenia i stało się dla wolnego człowieka przestrzenią równie ważną jak *polis*. Znalazło to swoje zwięzłe streszczenie w stwierdzeniu amerykańskiej filozof A. Rand, która napisała, że „cywilizacja to postęp w stronę prywatności”[3]. Niewątpliwie prywatność w rozwiniętych demokracjach liberalnych stała się dziś wartością, której się nie kwestionuje i której się broni. Jednak podejście do niej szybko się zmienia, a dziś warunkowane jest przede wszystkim rozwojem nowych mediów. Podejście do prywatności jako wartości bezwzględnej zmieniły zamachy ter-

---

1 Ks. dr Krzysztof Łuszczek, doktor nauk humanistycznych, adiunkt w Instytucie Pedagogiki Uniwersytetu Szczecińskiego. Zajmuje się pedagogiką medialną i teorią mediów. Autor m.in. *Nowoczesna telewizja, czyli bliskie spotkania z kulturą masową* (Tychy: Maternus Media, 2004); *Kontrola społeczna nad dziećmi i młodzieżą w środowisku mediów elektronicznych. Studium porównawcze na przykładzie Stanów Zjednoczonych, Wielkiej Brytanii i Polski* (Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, 2013); *Wolność i kontrola w Internecie drugiej fali. Cyfrowe dylematy społeczeństwa obywatelskiego w Stanach Zjednoczonych i Unii Europejskiej* (Tychy: Maternus Media, 2015). Adres do korespondencji: 71-459 Szczecin, ul. Pawła VI 2; e-mail: krzysztof.luszczek@usz.edu.pl.

2 Jim Roy, „Polis and Oikos in Classical Athens”, *Greece and Rome* 46 (1999): 1–3.

3 Ayn Rand, *The Fountainhead* (Overland Park: International Collectors Library, 1968), 715.

rorystyczne w Nowym Jorku, Madrycie i Londynie. Demokracje liberalne poświęciły szereg praw demokratycznych (m.in. prawo do prywatności) na rzecz zapewnienia bezpieczeństwa. Jednak dziś w równej mierze co walka z terroryzmem, zagrażają prywatności wolnych obywateli działania wielkich, ponadnarodowych korporacji związanych z tzw. Internetem drugiej fali[4].

Prywatność niewątpliwie staje się wartością coraz bardziej docenianą przez ludzi. Obywatele, nawet przy poparciu dużych organizacji non-profit, nie są jednak w stanie jej efektywnie chronić. Stąd potrzeba zaangażowania państwa, które może stworzyć odpowiednie narzędzia do jej ochrony i przeciwstawić się wielkim korporacjom. Z drugiej strony, agencje rządowe wykazują na tym polu również dużą aktywność, zasłaniając się najczęściej potrzebą zapewnienia bezpieczeństwa.

Powstaje więc pytanie: Jak zachować delikatną równowagę między prawami obywateli do ochrony prywatności, zasadami wolnego rynku (co wiąże się ze zbieraniem informacji o konsumentach) oraz działaniami agencji rządowych mających z jednej strony chronić prawa obywateli, a z drugiej zapewnić im bezpieczeństwo?

1. Wpływ rozwoju nowych mediów na podejście do ochrony prywatności

Prywatność rodzi szereg różnych problemów począwszy od definicyjnych. Niektórzy uważają, że prywatność można zredukować do innych wartości[5]. Zazwyczaj prywatność określa się poprzez jej wymiary. Jednak granice między nimi nie są ostre. Często postuluje się o zaakceptowanie dwóch równoległych definicji prywatności: normatywnej i deklaratywnej[6].

Pionierami nowożytnych ujęć prywatności są S. Warren i L. Brandeis. W swoim artykule *The Right to Privacy* opublikowanym w 1890 r. na łamach *Harvard Law Review* wyodrębnili ogólne „prawo do bycia pozostawionym w spokoju" (*the right to be let alone*). Ubolewali, że najnowsze wynalazki i metody prowadzenia działalności gospodarczej, takie jak błyskawiczne fotografie i branża gazet codziennych, wtargnęły na uświęcony teren życia prywatnego i domowego. Zaproponowali jego wyodrębnienie spośród innych praw, aby lepiej chronić prawa jednostki[7].

---

4 Określenia *the second wave of Internet* użyli Lyn Gorman i David McLean dla nazwania drugiej fazy w rozwoju globalnego Internetu. Cechuje ją intensywny rozwój mediów społecznościowych oraz realizm w podejmowaniu inwestycji związanych z e-gospodarką po tzw. *krachu dotcomów* z przełomu tysiącleci. Lyn Gorman, David McLean, *Media i społeczeństwo. Wprowadzenie historyczne* (Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, 2010), 272.

5 Deborah G. Johnson, „Computer Ethics", w: *Academy and the Internet*, red. Helen Nissenbaum, Monroe E. Price (New York, Washington, D.C./Baltimore, Bern, Frankfurt am Main, Berlin, Brussels, Vienna, Oxford: Peter Lang Inc., International Academic Publishers, 2004), 143–144.

6 Łukasz Kołodziejczyk, *Prywatność w Internecie* (Warszawa: Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, 2014), 19.

7 Samuel Warren, Louis D. Brandeis, „The Right to Privacy", *Harvard Law Review* 5 (1890), dostęp 16.04.2015, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Prywatność zaczęto określać w szerokim spektrum praw człowieka. A. Westin uważa, że jest to roszczenie jednostek, grup lub instytucji do tego, aby mogły decydować, w jaki sposób informacje o nich zostaną ujawnione na zewnątrz. Precyzując to określenie, amerykański badacz podaje kilka wymiarów prywatności (m.in. odosobnienie, intymność, anonimowość, rezerwę)[8]. Określanie wymiarów prywatności stało się dość powszechne przy próbach jej zdefiniowania.

I. Altman twierdzi, że kontrola jednostki nad ujawnianymi informacjami ma charakter selektywny. Fakt prywatności jest uniwersalny, natomiast mechanizmy zarządzania nią są indywidualne. Altman zwraca uwagę m.in. na kontekst kulturowy i społeczny. Wśród mechanizmów społecznych wymienia procesy społeczne oraz relacje społeczne. To prowadzi do tego, że w pewnych sytuacjach ludzie ujawniają maksimum informacji o sobie, w innych ograniczają je do minimum. Jest to zależne od człowieka, który dąży do homeostazy w swojej aktualnej sytuacji życiowej[9].

Inaczej traktuje prywatność W. Parent. Jego definicja ma charakter nienormatywny. Nie odnosi się więc ani do norm moralnych, ani prawnych. Podkreśla nieuchwytność fenomenu prywatności[10]. Uważa, że prywatność to stan, w którym jednostka zachowuje jako poufne pewne niepublikowane informacje. Zwiększenie lub zmniejszenie prywatności to bardziej zmiana stanu, a nie różny poziom kontroli[11].

H. Nissenbaum mówi o tzw. kontekstowym podejściu do prywatności. Z ujawnieniem własnej prywatności związanych jest kilka elementów. Są to aktorzy, którzy biorą udział w określonej grze, przestrzeń, w której jest osadzona, oraz informacje, które mają być ujawnione. Według Nissenbaum nie jest możliwa pełna kontrola informacji, a jedynie jej dostosowanie do kontekstu społecznego. Proponuje, aby kontrolę prywatności rozumieć jako możliwość zróżnicowanego dzielenia się informacją o sobie. Prywatność zostaje naruszona, kiedy nie przestrzega się normy stosowności oraz normy dystrybucji. Pierwsza określa jakie informacje mogą być w danej chwili przekazane, a druga komu i w jakim czasie. Nissenbaum uważa, że takie sytuacyjne podejście bardziej odzwierciedla problem ochrony prywatności[12]. Zwraca jednak uwagę, że wciąż istnieją problemy definicyjne. Ale największy wpływ na zmianę podejścia do prywatności mają dziś wielkie korporacje internetowe. Niektórzy wręcz bagatelizują prywatność uważając, że faktycznym proble-

8 Alan Westin, „Social and Political Dimensions of Privacy", *Journal of Social Issues* 2 (2003): 431–433, dostęp 24.02.2017, http://www.privacysummersymposium.com/reading/westin.pdf.

9 Irvin Altman, „Privacy Regulation: Culturally Universal or Culturally Specific?", *Journal of Social Issues* 3 (1977): 76–79, dostęp 26.02.2017, http://courses.cs.vt.edu/cs6204/Privacy-Security/Papers/Privacy/Privacy-Regulation.pdf.

10 William Parent, „Privacy: A Brief Survey of the Conceptual Landscape", *Santa Clara High Technology Law Journal* 1 (1995): 21.

11 Parent, „Privacy: A Brief Survey of the Conceptual Landscape", 25–26.

12 Helen Nissenbaum, „A Contextual Approach to Privacy Online", *Daedalus, the Journal of the American Academy of Arts & Science* 4 (2011): 43, dostęp 4.03.2017, https://www.amacad.org/multimedia/pdfs/publications/daedalus/11_fall_nissenbaum.pdf.

mem jest to, w jaki sposób wykorzystujemy dane[13]. Stąd potrzeba uporządkowania tej sfery społecznego życia, tym bardziej, że znajduje się ona dziś pod silną presją nowych technologii i komputerów[14].

Pewną metodę na porządkowanie tej rzeczywistości zaproponowała już w 1991 r. S. Petronio. *Communication privacy management* – CPM (zwana pierwotnie *communication boundary management*) służy określeniu w jaki sposób i w jakich okolicznościach człowiek ujawnia prywatne informacje o sobie. Petronio mówi o trzech regułach sterujących ujawnianiem informacji. Reguła przepuszczalności (*permeability*) opisuje szerokość, głębokość oraz liczbę przesyłanych informacji. Reguła połączeń (*linkages*) określa, jakie osoby mogą poznać informacje prywatne. Posiadanie informacji prywatnych implikuje odpowiedzialność za zarządzanie nimi. W końcu reguła współposiadania (*shared ownership*) określa, do czego mają prawo osoby będące w grupie posiadającej informację[15].

Nie wszyscy jednak uważają za potrzebne zajmowanie się w szczegółach prywatnością. J. Thomson uważa, że nie chodzi o to, że prywatność nie jest ważna, ale nie ma potrzeby wyszczególniania prawa do ochrony prywatności. Jest ono gwarantowane już przez inne przepisy i nie potrzeba mnożyć bytów[16]. Takie stanowiska są jednak odosobnione, zwłaszcza w kontekście tego, jak sferę prywatności przewartościował rozwój nowych mediów. J. van Dijk definiował je jako zintegrowane, interaktywne i oparte na kodzie binarnym media, które rozwinęły się na przełomie XX i XXI wieku[17]. Zmieniły one całkowicie podejście do prywatności, zwłaszcza jeżeli chodzi o sferę mediów społecznościowych.

Założyciel Facebooka M. Zuckerberg uznał w 2010 r., że prywatność przestała już dziś być normą społeczną. Co więcej uznał, że ludziom dzisiaj tak naprawdę nie zależy na prywatności. „Dla ludzi wygodne stało się nie tylko dzielenie się większą liczbą różnego rodzaju informacji, ale także robienie tego bardziej otwarcie i z większą liczbą innych osób" – powiedział w trakcie gali nagród Crunchie Awards przyznawanych przez serwis TechCrunch[18].

Jednak użytkownicy mediów społecznościowych w coraz większej liczbie są przeciwni tezie wygłoszonej przez Zuckerberga. Ma na to wpływ przede wszystkim edukacja,

---

13 Solon Barocas, Helen Nissenbaum, „Big Data's End Run around Anonymity and Consent", w: *Privacy, Big Data and the Public Good. Frameworks for Engagement*, red. Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum (New York: Cambridge University Press, 2014), 46.

14 Barocas, Nissenbaum, „Big Data's End Run around Anonymity and Consent", 63.

15 Sandra Petronio, „Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples", *Communiaction Theory* 4 (1991): 311–335.

16 Judith J. Thomson, „The Right to Privacy", *Philosophy and Public Affairs* 4 (1975): 312.

17 Jan van Dijk, *Społeczne aspekty nowych mediów* (Warszawa: Wydawnictwo Naukowe PWN, 2010): 20.

18 „Zuckerberg: prywatność już nie jest normą społeczną", dostęp 12.01.2010, http://www.wirtualnemedia.pl/artykul/zuckerberg-prywatnosc-juz-nie-jest-norma-spoleczna.

sposób formułowania polityki prywatności przez serwisy, a także osobiste doświadczenia internautów[19].

W badaniach przeprowadzonych w 2013 r. 59% konsumentów za największe zagrożenie dla prywatności w Internecie uznało Facebooka. Na dalszych miejscach uplasowały się Twitter (40%) i Google (32%). Efektem tego było przenoszenie profili na serwisy zapewniające lepszą ochronę prywatności (np. Snapchat)[20]. Tym bardziej budzą sprzeciw takie postulaty Zuckerberga jak bezwarunkowe udostępnienie Facebooka dzieciom poniżej trzynastego roku życia[21].

Ale nie tylko działania Facebooka budzą kontrowersje użytkowników. Gigant na rynku nowych technologii – Google – przysparza równie wielu problemów. W 2009 r. prawie 250 tys. Niemców zaprotestowało przeciwko usłudze Street View. Zażądało usunięcia lub zamazania obrazów własnych domów w usłudze. Korporacja przyznała, że nie będzie mogła spełnić wszystkich żądań użytkowników[22]. Jeszcze większy niepokój internautów wywołała informacja, że Google regularnie czyta pocztę na serwisie pocztowym Gmail. Co prawda szybko pospieszono z wyjaśnieniem, że robią to automaty, a jedynym celem jest profilowanie reklam, a nie pozyskanie informacji osobistych, jednak niesmak pozostał. Microsoft nie omieszkał wytknąć tego Google przy okazji promocji własnego serwisu pocztowego Outlooka[23]. Ale również firmie założonej przez B. Gatesa wytknięto działania szkodzące prywatności internautów. Chodziło o przejęty w 2011 r. przez Microsoft komunikator Skype. Korporacji zarzucono, że umożliwia podsłuchiwanie rozmów na komunikatorze. Microsoft nie odniósł się bezpośrednio do tych zarzutów[24].

Media społecznościowe żywią się informacjami, jakie zostawiają w nich użytkownicy. Zdecydowana większość z nich ma charakter osobisty. Nie wszyscy użytkownicy posiadają jednak wiedzę na temat sposobu ich gromadzenia i przetwarzania. Nie wszystkie dane wirtualne będą stanowić dane osobowe w rozumieniu prawa. Trzeba je ocenić przez pryzmat czasu, działań i kosztów prowadzących do zidentyfikowania osoby na podstawie posiadanych danych. W stosunku do adresów IP i plików cookies istnieje wiele możliwości fałszowania danych. Może się zdarzyć, że adres IP, e-mail lub pliki cookies

19 Kołodziejczyk, *Prywatność w Internecie*, 28.

20 Badania McCann Truth Central „Prawda o prywatności" zostały przeprowadzone w listopadzie 2013 r. na próbie 1100 osób powyżej 18 roku życia. „Facebook największym zagrożeniem dla prywatności w Internecie", dostęp 14.01.2014, http://www.wirtualnemedia.pl/artykul/facebook-najwiekszym-zagrozeniem-dla-prywatnosci-w-internecie.

21 „Zuckerberg: Facebook powinien być dostępny dla dzieci poniżej 13. roku życia", dostęp 25.05.2011, http://www.wirtualnemedia.pl/artykul/zuckerberg-facebook-powinien-byc-dostepny-dla-dzieci-ponizej-13-roku-zycia.

22 „Google: prawie ćwierć miliona Niemców nie chce Street View", dostęp 22.10.2010, http://www.wirtualnemedia.pl/artykul/google-prawie-cwierc-miliona-niemcow-nie-chce-street-view.

23 Katarzyna Jasiołek, „Google czyta naszą pocztę – przypomina Microsoft", *Komputer Świat* 8.02.2013, dostęp 19.04.2015, http://www.komputerswiat.pl/nowosci/programy/2013/06/google-czyta-nasza-poczte-przypomina-microsoft-wideo.aspx.

24 „Czy można podsłuchiwać rozmowy ze Skype? «Bez komentarza!»", dostęp 24.07.2012, http://tech.wp.pl/kat,1009785,title,Czy-mozna-podsluchiwac-rozmowy-na-Skype-Bez komentarza,wid,14785021,wiadomosc.html?ticaid=114e48.

nie identyfikują użytkownika. Wtedy są to tylko dane techniczne, a nie osobowe. Dane osobowe w sieci będą takimi, o ile na ich podstawie będzie można zidentyfikować użytkownika[25]. Takimi danymi mogą być także np. pewne dane biometryczne gromadzone przez niektóre serwisy. Biometria jest to metoda „automatycznej identyfikacji osobistej opartej na pewnych cechach fizycznych lub behawioralnych człowieka"[26].

Prywatność wirtualną możemy określić jako osadzenie „wymiarów prywatności znanych z epoki przedinternetowej w nowym, wirtualnym kontekście"[27]. Natomiast cyfrowe dane osobowe to „dane osobowe w środowisku cyfrowym, dostępne bądź przetwarzane nie tylko online, ale również offline, oraz dane przetwarzane na wszelkich urządzeniach cyfrowych, we wszelkiego rodzaju systemach informatycznych"[28].

Technologia komputerowa umożliwia na niespotykaną dotąd skalę gromadzenie informacji o ludziach. Może dziać się to szybko i z wykorzystaniem wielu źródeł np. od użytkowników kart kredytowych, platform cyfrowych czy telefonii komórkowej. Umożliwia manipulowanie danymi na szeroką skalę. To może budzić niepokój, bo społeczeństwo informacyjne (*information society*) zamienia się w społeczeństwo nadzorowane (*surveillance society*). Podkreśla się często, że Internet może być łatwo wykorzystany do stworzenia cyfrowego *panoptikonu* i osiągnięcia jego efektu. Jedną z istotnych cech takiego systemu jest to, że ludzie nie wiedzą, przez kogo są obserwowani[29].

Od początku XXI wieku, przede wszystkim w Stanach Zjednoczonych i Europie, podejmowano próby ochrony prywatności w przestrzeni cyfrowej. Rozwiązania amerykańskie można określić jako fragmentaryczne i podejmowane *ad hoc*. Natomiast w Europie miały one charakter bardziej kompleksowy. Amerykanie często przyjmowali odrębne rozwiązania dla różnych rodzajów mediów. Pojawił się również problem międzynarodowego transferu informacji. Dane chronione w jednym kraju, przesłane do drugiego, często już nie mogą liczyć na taką ochronę[30].

2. Działania na poziomie państw członkowskich Unii Europejskiej

Działania podejmowane przez Unię Europejską występują na dwóch poziomach – ogólnounijnym oraz na poziomie państw członkowskich Unii. Mimo, że oba te systemy powinny być zharmonizowane często dochodzi między nimi do tarć, a nawet działań sprzecznych ze sobą (np. kiedy jakieś państwo uzna dyrektywę unijną za sprzeczną z własną konstytucją i odmawia jej wprowadzenia). Prowadzi to do sporów między instytucjami unijnymi a poszczególnymi państwami. Poza tym działania na obu poziomach można

25 Monika Brzozowska, *Ochrona danych osobowych w sieci* (Wrocław: Wydawnictwo Presscom, 2012): 39.

26 Brzozowska, *Ochrona danych osobowych w sieci*, 56.

27 Kołodziejczyk, *Prywatność w Internecie*, 30.

28 Brzozowska, *Ochrona danych osobowych w sieci*, 19.

29 Johnson, „Computer Ethics", 155–156.

30 Johnson, „Computer Ethics", 156–157.

rozpatrywać zarówno na płaszczyźnie formalnej (np. stanowione prawo), jak i nieformalnej (np. działania różnych fundacji czy tworzenie kodeksów dobrych praktyk). Działania podejmowane przez poszczególne państwa unijne mają szereg cech charakterystycznych bądź oryginalnych rozwiązań, które nie obejmują całej Unii.

Wśród krajów unijnych Niemcy cechuje szczególna konsekwencja przyjmowanych rozwiązań. W 2010 r. hamburski pełnomocnik ds. ochrony danych J. Caspar wdrożył procedurę ukarania Facebooka grzywną za gromadzenie prywatnych informacji o ludziach bez zgody i wiedzy zainteresowanych. Chodziło także o pozyskiwanie informacji o ludziach, którzy nie posiadają profilów na portalu. J. Caspar uznał gromadzenie danych o osobach trzecich jako sprzeczne z przepisami o ochronie danych[31].

Niemcy posiadają jedne z najbardziej restrykcyjnych przepisów dotyczących ochrony danych w Europie. Wynika to w dużej mierze z doświadczeń historycznych. Czasy nazizmu, a przede wszystkim komunizmu i długoletnia działalność Stasi (Ministerium für Staatssicherheit) doprowadziła do przyjęcia tak ostrych przepisów. Ich fundamentem jest zapis mówiący o tym, że dane nie mogą być gromadzone bez wyraźnej zgody użytkownika. J. Caspar poruszył także problem zbierania przez Facebook danych biometrycznych. Uznał, że użytkownicy nie mają dokładnych informacji na ten temat, a niektóre mogą wprowadzić ich w błąd. A co najważniejsze, nie wiedzą, jak usunąć dane biometryczne. Facebook odrzucił zarzuty niemieckiego inspektora danych osobowych, ale zaznaczył, że weźmie je pod uwagę przy wprowadzaniu zmian w polityce prywatności[32].

Spór dotyczący zbierania danych przez Facebook przeciągnął się. Tak naprawdę niemiecki urząd nie mógł wyrządzić serwisowi wielkiej szkody (poza nałożeniem niewielkiej kary finansowej), ale liczyły się też straty wizerunkowe. W toku sporu Facebook zgodził się na usunięcie niektórych danych biometrycznych Europejczyków. Przy okazji jednak okazało się, że samo rozpoznawanie twarzy nie przeszkadzało niemieckim urzędnikom prowadzącym postępowanie przeciw serwisowi. Chodziło przede wszystkim o to, że serwis może zbierać dane o ludziach, którzy nie wyrazili na to zgody. J. Caspar podsumowując w 2013 r. niemiecki spór z Facebookiem, zaznaczył, że kluczową kwestią jest świadoma zgoda użytkownika na przetwarzanie danych osobowych. Inspektor podkreślił ten aspekt sporu, ponieważ śledząc go można było odnieść wrażenie, że niemieccy urzędnicy walczą z nowymi technologami czy ze zbieraniem danych jako takich[33].

Spór z Facebookiem w Niemczech miał jeszcze jedną odsłonę. Zaangażowała się w niego federalna minister ds. ochrony konsumentów I. Aigner. Odwiedziła Stany Zjednoczone, aby sondować możliwość nacisku na korporacje internetowe za pośrednictwem

31 Johannes Caspar, „Sammlung der Daten von Nicht-Nutzern durch Facebook unzulässig", dostęp 28.02.2017, https://www.datenschutz-hamburg.de/uploads/media/pressemeldung-2010-04-08__Facebook_Maengel_.pdf.

32 Cyrus Farivar, „Facebook violates German law, Hamburg data protection official says", dostęp 20.04.2015, http://www.dw.de/facebook-violates-german-law-hamburg-data-protection-official-says/a-15290120.

33 Florian Schmidt, „Datenschützer Caspar kritisiert Gesichtserkennung bei Facebook", *Computer Bild* 9.02.2013, dostęp 28.02.2017, http://www.computerbild.de/artikel/cb-News-Internet-Gesichtserkennung-Facebook-Datenschutz-Johannes-Caspar-Gesichtserkennung-6259152.html.

amerykańskich agencji rządowych, przede wszystkim Federalnej Komisji Handlu (Federal Trade Commission). Europejskie agencje rządowe mają ograniczone możliwości nacisku na firmy internetowe, gdyż większość największych korporacji ma swoje siedziby w Stanach Zjednoczonych i są przedsiębiorstwami amerykańskimi. I. Aigner stwierdziła, że standardy ochrony prywatności w Stanach Zjednoczonych są niższe niż w Unii Europejskiej, dlatego nie można dopuszczać do transferu danych do krajów stosujących niższe standardy. Sprzeciw niemieckiej minister wobec Facebooka szedł nawet tak daleko, że była przeciwna umieszczaniu zakładek profili społecznościowych na stronach internetowych niemieckich urzędów rządowych[34].

Jedną z najbardziej znanych akcji społecznych w obronie danych osobowych w mediach społecznościowych zainicjował austriacki student prawa M. Schrems. Spopularyzował on sam problem i doprowadził do tego, że przedstawiciele Facebooka spotkali się z nim, obiecując poprawę polityki prywatności. Cała sprawa rozpoczęła się od wniosku złożonego przez M. Schremsa do Facebooka, aby ujawnił wszystkie informacje, które serwis zebrał na jego temat od momentu założenia profilu. Austriak wykorzystując drogę prawną, doprowadził do przesłania mu tych informacji. Otrzymał dysk komputerowy zawierający 1222 strony informacji. Co było szczególnie zaskakujące, większość z nich Austriak usunął wcześniej ze swego profilu. To sprowokowało M. Schremsa do zainicjowania akcji na rzecz ochrony danych osobowych[35].

Facebook wyszedł naprzeciw niektórym jego żądaniom. M. Schrems uznał te ustępstwa za pozorne i rozpoczął akcję *Europe v Facebook*. Za pośrednictwem strony internetowej zaczął gromadzić środki i zwolenników mających umożliwić ewentualny proces z Facebookiem. Akcję M. Schremsa za pośrednictwem strony internetowej wsparło kilkadziesiąt tysięcy osób[36]. Facebook powołał się na dwa raporty irlandzkich organów zajmujących się ochroną danych osobowych (siedziba Facebooka znajduje się w Dublinie), które potwierdzały, że serwis działa zgodnie z irlandzkim i europejskim prawem[37]. W 2014 r. organizatorzy kampanii złożyli pozew zbiorowy przeciw Facebookowi w sądzie w Wiedniu[38]. Osiągnęli przez to podstawowy cel, jakim było zwrócenie uwagi i podniesienie świadomości społecznej w kwestii ochrony danych osobowych.

Do podjęcia zindywidualizowanych działań europejskich państw wobec mediów społecznościowych doprowadził także rozwój zagrożenia ze strony światowego terroryzmu. Po zamachach na redakcję „Charlie Hebdo" francuski prezydent F. Hollande zabrał głos

---

34 Karsten Polke-Majewski, „Ilse Aigner «Bei Facebook sehe ich viele Fragezeichen»", *Zeit* 20.09.2011, dostęp 1.03.2017, http://www.zeit.de/digital/datenschutz/2011-09/aigner-facebook-datenschutz.

35 Kevin J. O'Brien, „Austrian Law Student Faces Down Facebook", *The New York Times* 5.02.2012, dostęp 20.07.2016, http://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html?

36 Barbara Gubernat, „Europa przeciwko Facebookowi – przygotowania do decydującego starcia", dostęp 1.03.2017, http://panoptykon.org/wiadomosc/europa-przeciwko-facebookowi-przygotowania-do-decydujacego-starcia.

37 „Grupa studentów walczy z Facebookiem", dostęp 5.12.2012, http://www.wirtualnemedia.pl/artykul/grupa-studentow-walczy-z-facebookiem.

38 „Sammelklage gegen Facebook eingebracht", dostęp 21.04.2015, http://www.ots.at/presseaussendung/OTS_20140801_OTS0060/sammelklage-gegen-facebook-eingebracht.

w sprawie mediów społecznościowych. Stwierdził, że oczekuje od platform społecznościowych i operatorów internetowych stałego monitorowania serwisów. Profile osób nawołujących w Internecie do działań ekstremistycznych i terrorystycznych powinny być zamykane. Francuski minister spraw wewnętrznych B. Cazeneuve miał podjąć na ten temat rozmowy w Stanach Zjednoczonych z przedstawicielami Twittera, Facebooka, Google'a i Microsoftu[39].

Z kolei w Wielkiej Brytanii obserwujemy szereg działań o charakterze edukacyjnym. Brytyjskie szkoły dysponują szeroką gamą pomocy służących z jednej strony rozwijaniu umiejętności zarządzania prywatnością na terenie szkoły, jak również realizacji programów edukacyjnych dotyczących m.in. ochrony prywatności w Internecie. Starają się one tłumaczyć i wprowadzać w codzienność zasady zapisane w *Data Protection Act* z 1998 r.[40]

Działania podejmowane w niektórych krajach Unii Europejskiej na polu ochrony prywatności w sieci są bardziej radykalne niż np. w Stanach Zjednoczonych i bardzo często cechują się pewnym indywidualnym stylem i kierunkami podejmowanych decyzji. Stąd w wielu wypadkach apele o to, aby dane osobowe Europejczyków nie były transferowane do USA, gdzie jest niższy poziom ochrony. Dla samej Europy wciąż problemem jest harmonizacja prawa służącego ochronie prywatności. Dla pojedynczych obywateli niezmiernie istotna jest wiedza oraz edukacja w zakresie omawianych problemów. Szkoła poprzez odpowiednie programy powinna przygotowywać dzieci i młodzież do właściwego zarządzania swoją prywatnością. Chodzi przede wszystkim o to, aby nie dopuszczać do wyłudzania informacji osobistych przez wielkie korporacje internetowe. Dzieci i młodzież najszybciej stają się ofiarami sieciowych wyłudzeń danych osobowych.

3. Działania na poziomie ogólnounijnym

Unia Europejska podejmuje szereg działań za pośrednictwem różnych instytucji na rzecz ochrony danych osobowych. W 1950 r. przyjęto *Europejską Konwencję Praw Człowieka*. W celu przestrzegania jej zapisów powołano w 1959 r. Europejski Trybunał Praw Człowieka w Strasburgu. Wielokrotnie w swoim orzecznictwie odnosił się on do ochrony danych osobowych. Przy okazji dał wykładnię art. 8 *Europejskiej Konwencji Praw Człowieka*, dotyczącego ochrony życia prywatnego i rodzinnego. Mówi m.in., że „każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji"[41]. Trybunał w Strasburgu wyjaśnił, że nie chodzi jedynie o sta-

39 „Francja wzywa Twittera, Facebooka i Google do blokowania kont terrorystów", dostęp 29.01.2015, http://www.wirtualnemedia.pl/artykul/francja-wzywa-twittera-facebooka-i-google-do-blokowania-kont-terrorystow.

40 Podstawowy akt prawny w Wielkiej Brytanii określający zasady przetwarzania informacji umożliwiających identyfikację ludzi.

41 Rada Europy, „Europejska Konwencja Praw Człowieka", dostęp 3.03.2017, http://www.echr.coe.int/Documents/Convention_POL.pdf, art. 8 p. 1.

nie na straży zapisów konwencji. Chodzi również o aktywne zaangażowanie na rzecz skutecznego poszanowania życia prywatnego i rodzinnego[42].

Zmiany wywołane rozwojem nowych technologii w środowisku informacyjnym człowieka spowodowały przyjęcie kolejnych dokumentów unijnych, regulujących ochronę danych osobowych. W 1981 r. została podpisana w Strasburgu konwencja 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Nie odnosi się ona bezpośrednio do środowiska cyfrowego, raczej chodzi o gromadzenie danych przez różnego rodzaju agencje rządowe oraz ich transgraniczną wymianę. W 2011 r. podjęto jednak działania modernizacyjne mające na celu przede wszystkim uwzględnienie w konwencji cyfrowego środowiska informacyjnego. Konwencja jest otwarta także na państwa spoza Unii Europejskiej. Pierwszym krajem spoza Unii, który przystąpił do konwencji w sierpniu 2013 r. był Urugwaj[43].

Głównym aktem prawnym UE dotyczącym ochrony danych jest dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dyrektywa o ochronie danych). Miała ona przede wszystkim harmonizować działania podejmowane już wcześniej przez poszczególne państwa unijne. Dyrektywa zajmuje się m.in. transmisją danych osobowych drogą cyfrową, określając jej twórców i administratorów, ich obowiązki i odpowiedzialność. W artykułach 14 i 15 zajmuje się zgodą zainteresowanej osoby na przetwarzanie jej danych osobowych i przyznaje jej prawo do sprzeciwu[44]. Uzupełnieniem dyrektywy jest rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych. Reguluje ono przede wszystkim sposoby przetwarzania danych osobowych w instytucjach unijnych[45].

Dwa lata później weszła w życie dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[46]. Przepisy dyrektywy miały uzupełniać to, co już wcześniej było zapisane w dyrektywie o ochronie danych. Gwarantuje bezpieczeństwo i poufność w komunikacji drogą elektroniczną. Art. 5 stwierdza, że „korzystanie z sieci łączności elektronicznej

---

42 Np. w orzeczeniu ETPC, K.U. przeciwko Finlandii, nr 2872/02 z 2 grudnia 2008 r., dostęp 9.03.2017, http://www.prawaczlowieka.pl/precedens/aktualnosci/wyrok-w-sprawie-k-u-przeciwko-finlandii-ochrona-dobrego-imienia-przed-znieslawieniem-za-pomoca-in.html.

43 Agencja Praw Podstawowych Unii Europejskiej, Rada Europy – Europejski Trybunał Praw Człowieka, *Podręcznik europejskiego prawa o ochronie danych* (Luksemburg: Urząd Publikacji Unii Europejskiej, 2014), 17.

44 Dyrektywa o ochronie danych, Dz.U. L 281 z 23.11.1995, art. 14 i 15.

45 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

46 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002.

w celu przechowywania informacji lub uzyskania dostępu do informacji przechowanej na terminalu abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem, że abonent lub użytkownik otrzyma jasną i wyczerpującą informację zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania, oraz zostanie zaoferowane mu prawo do odmówienia zgody na takie przetwarzanie przez kontrolera danych". Dyrektywa zajmuje się również danymi mogącymi posłużyć lokalizacji. Ich przetwarzanie może odbywać się albo anonimowo albo po wyraźnej zgodzie abonenta. Zapisy dyrektywy o prywatności i łączności elektronicznej odnoszą się w dużej części do łączności telefonicznej. Przepisy powstawały, gdy telefonia komórkowa przeżywała dynamiczny rozwój, a stacjonarna ulegała szybkiej cyfryzacji.

Szczególnie wiele dyskusji dotyczących ochrony danych osobowych wywołało przyjęcie dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE[47]. Została ona przyjęta na fali oburzenia po zamachach w Madrycie i Londynie. Niepokój budził przede wszystkim zakres danych, jakie miały gromadzić państwa członkowskie UE i o sposobie korzystania z elektronicznych środków łączności przez obywateli. Art. 5 dyrektywy wymienia cały katalog takich danych. Na przykład w przypadku elektronicznej poczty internetowej i telefonii internetowej dyrektywa nakazywała rejestrować:

- datę i godzinę zalogowania i wylogowania sesji internetowej na podstawie danej strefy czasowej, włącznie z adresem protokołu komunikacyjnego dynamicznego lub statycznego (IP) przydzielonym przez dostawcę usług internetowych dla danej komunikacji oraz identyfikatorem użytkownika abonenta lub zarejestrowanego użytkownika,
- datę i godzinę zalogowania i wylogowania z elektronicznej poczty internetowej i telefonii internetowej na podstawie danej strefy czasowej.

Zgodnie z przepisami dyrektywy przedsiębiorstwa telekomunikacyjne powinny zatrzymywać i gromadzić dane umożliwiające identyfikację abonenta lub użytkownika. Takie działania miały być wymierzone przede wszystkim w przestępczość zorganizowaną oraz terroryzm[48].

Katalogi rejestrowanych danych miały umożliwić zebranie jak największej ilości informacji na temat okoliczności przesyłanych komunikatów. Twórcy dyrektywy zastrzegali co prawda, że nie chodzi o rejestrację samego komunikatu, jednak ilość rejestrowanych informacji przynosiła szeroką wiedzę na temat nadawców i odbiorców komunikatu (np. na temat ich przemieszczania się czy częstotliwości kontaktów).

---

47 Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (dyrektywa o zatrzymywaniu danych), Dz.U. L 105 z 13.05.2006.

48 „Dyrektywa 2006/24/WE dotycząca tzw. retencji danych telekomunikacyjnych nieważna – orzekł Trybunał Sprawiedliwości Unii Europejskiej", dostęp 24.04.2015, https://mac.gov.pl/aktualnosci/dyrektywa-200624we-dotyczaca-tzw-retencji-danych-telekomunikacyjnych-niewazna-orzekl.

Art. 6 określał czas przechowywania danych. Miał on trwać od 6 miesięcy do 2 lat, w zależności od potrzeby. Po tym okresie powinny być zniszczone.

Gromadzenie zbyt wielu danych oraz brak ściśle określonej kontroli nad zgromadzonymi danymi wywołało protesty wielu organizacji społecznych, ale także rządów. Spowodowało to różne reakcje na dyrektywę. Ponieważ niemiecki Federalny Trybunał Konstytucyjny uznał ją za sprzeczną z konstytucją, Niemcy odmówiły jej wdrożenia[49]. Wnioskodawcy z Irlandii i Austrii zaskarżyli dyrektywę do Trybunału Sprawiedliwości Unii Europejskiej. Trybunał wydał wyrok 8 kwietnia 2014 r. Sędziowie zwrócili uwagę na trzy grupy informacji, jakich pozyskanie umożliwia dyrektywa:

- wiedza, z jaką osobą i za pomocą jakiego środka komunikował się abonent lub zarejestrowany użytkownik,
- określenie czasu łączności oraz miejsca, z którego łączność ta została nawiązana,
- ustalenie częstości komunikowania się abonenta lub zarejestrowanego użytkownika z określonymi osobami w danym okresie[50].

Sędziowie uznali, że dane te rozpatrywane łącznie, mogą dostarczyć wielu informacji dotyczących życia prywatnego obywateli. Poza tym zatrzymywanie danych i przekazywanie ich agencjom rządowym stanowi ingerencję w prawa podstawowe do poszanowania życia społecznego i ochrony danych osobowych. Z drugiej jednak strony trybunał uznał, że zatrzymywanie danych nie narusza istoty praw podstawowych i rzeczywiście może się poważnie przyczynić do zwalczania przestępczości zorganizowanej i terroryzmu. Jednak przyjmując dyrektywę 2006/24/WE, Parlament Europejski wyraźnie naruszył zasadę proporcjonalności. Sędziowie trybunału zarzucili również dyrektywie, że nie wyznacza wyraźnych ram retencji danych i jest niedopracowana. Traktuje ona wszystkie elektroniczne środki łączności generalnie i nie różnicuje ich. Nie określa wyraźnie, kto i w jakim wymiarze będzie miał dostęp do zgromadzonych danych. Problem dotyczy także czasu przetrzymywania danych. Kto ma decydować, że jedne dane będą przetrzymywane dłużej, inne krócej? W końcu brak mechanizmów mających zabezpieczyć zbiory danych przed niewłaściwym wykorzystaniem i przetrzymywanie ich ponad czas wymieniony w dyrektywie[51]. Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej unieważniające dyrektywę 2006/24/WE powołuje się na *Kartę Praw Podstawowych Unii Europejskiej*. Art. 7 stoi na straży życia prywatnego i rodzinnego, natomiast art. 8 chroni dane osobowe[52]. Wszystkie wątpliwości związane z przepisami dyrektywy doprowadziły

---

49 Za niezgodną z konstytucją krajową uznały dyrektywę 2006/24/WE m.in. Bułgaria, Rumunia, Niemcy, Czechy i Węgry. Piotr Biernatowski, „Orzeczenie: Niekonstytucyjność retencji danych – wyrok czeskiego Trybunału Konstytucyjnego", dostęp 24.04.2015, http://www.prawaczlowieka.edu.pl/index.php?orzeczenie=f66b7dcd21696a-4242e1ff93608c405741802c92-b0.

50 Trybunał Sprawiedliwości Unii Europejskiej, „Wyrok w sprawach połączonych C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger i in.", dostęp 24.05.2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054pl.pdf.

51 Trybunał Sprawiedliwości Unii Europejskiej, „Wyrok w sprawach połączonych C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger i in.".

52 Karta Praw Podstawowych Unii Europejskiej, Dz.U. C 83/394 z 30.03.2010.

do tego, że sędziowie Trybunału Sprawiedliwości Unii Europejskiej w swoim wyroku z 8 kwietnia 2014 r. uznali dyrektywę o retencji danych za nieważną.

W tym samym roku trybunał wydał wyrok w sprawie korporacji Google. Już od dłuższego czasu zarzucano jej brak przejrzystości w polityce prywatności. Firma musiała tłumaczyć się na przykład z tego, że przez jakiś czas nie zamieszczała na stronie głównej linku do polityki prywatności[53].

Komisja Europejska wystąpiła z zarzutami wobec Google w kilku obszarach, z których najważniejsze dotyczyły praktyk monopolistycznych, stosowanych w przeglądarce internetowej. Szczególnej intensywności nabrał jednak spór wokół prawa do „bycia zapomnianym". Sprawa rozpoczęła się od skargi obywatela Hiszpanii – M.C. Gonzaleza. Poprosił on Google o usunięcie z wyników wyszukiwania linków do informacji sprzed kilkunastu lat, dotyczących jego zalegania ze spłatami za mieszkanie. Korporacja internetowa odmówiła. Wówczas sprawę przekazano do sądu i zaczęła przechodzić przez sądy kolejnych instancji, aż trafiła do Trybunału Sprawiedliwości Unii Europejskiej. W wyroku C-131/12 z 13 maja 2014 r. trybunał nakazał „przyjęcie środków koniecznych do usunięcia danych (…) oraz uniemożliwienie dostępu do tych danych w przyszłości"[54]. W związku z tym zobowiązał Google do „usunięcia z wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje, również w przypadku, gdy to imię czy nazwisko czy też te informacje nie zostały uprzednio czy też jednocześnie usunięte z tych stron internetowych, i w odpowiednim przypadku, nawet jeśli ich publikacja na tych stronach jest zgodna z prawem"[55].

Wyrok Trybunału Sprawiedliwości Unii Europejskiej zmusił Google w Europie do przyjęcia nowych procedur chroniących prywatność użytkowników Internetu. Po raz pierwszy internauta otrzymał narzędzie, którym może przeciwstawić się wielkiej internetowej korporacji, chroniąc swoją prywatność. Po wyroku trybunału Google przygotowało specjalny formularz służący składaniu wniosków o usunięcie linków z wyników wyszukiwania[56]. Mogą z niego korzystać obywatele 28 krajów Unii Europejskiej, a także mieszkańcy Islandii, Norwegii, Liechtensteinu i Szwajcarii. W ciągu jednego miesiąca funkcjonowania nowych rozwiązań (od 29 maja do 30 czerwca 2014 r.) wpłynęło 70 tys. wniosków ze wszystkich państw Unii dotyczących 267 550 linków. Z Polski wpłynęło

53 Anne Broache, „Google attacked over privacy policy visibility", dostęp 27.04.2015, http://www.cnet.com/news/google-attacked-over-privacy-policy-visibility.

54 Trybunał Sprawiedliwości Unii Europejskiej, „Wyrok Trybunału (wielka izba) z dnia 13 maja 2014 r.", dostęp 28.04.2015, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd796004328b0548beb8bedf2537dbb54d.e34KaxiLc3qMb40Rch0SaxuPchr0?text=&docid=152065&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=255813.

55 Trybunał Sprawiedliwości Unii Europejskiej, „Wyrok Trybunału (wielka izba) z dnia 13 maja 2014 r.".

56 Dostępny w polskiej wersji językowej na stronie: https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=pl.

1661 wniosków[57]. Każdy wniosek powinien być rozpatrywany indywidualnie, a wnioskodawca powinien poświadczyć swoją wiarygodność zeskanowanym dowodem osobistym[58].

Egzekwowanie „prawa do bycia zapomnianym" w Internecie to nie jedyny problem Google w Unii Europejskiej. Przeciwko praktykom monopolistycznym potentata internetowego wielokrotnie występował unijny komisarz ds. konkurencji J. Almunia. Zobowiązano firmę do przedstawienia zmian w funkcjonowaniu wyszukiwarki oraz innych produktów Google[59]. Zarzuca się korporacji, że promuje swoje portale na temat handlu, podróży i drobnej przedsiębiorczości. Google na swojej przeglądarce – jak wykazali pracownicy Federalnej Komisji Handlu USA – zmienia kryteria rankingów i usuwa lub obniża rangę wyników związanych z konkurencją[60]. W 2014 r. Parlament Europejski przyjął rezolucję, która może skutkować podziałem Google na mniejsze spółki na rynku europejskim. Nie była ona wymierzona wprost w Google, ale mówiła o podmiotach działających na rynku nowych technologii, zalecając, aby oddzielały swoje wyszukiwarki internetowe od innych oferowanych usług[61].

Ostry kurs wobec Google kontynuuje nowa unijna komisarz ds. konkurencji M. Vestager. Pani komisarz zainteresowała się także mobilnym systemem operacyjnym Android. W Stanach Zjednoczonych pojawiły się zarzuty, że problemy Google biorą się stąd, że jest amerykańską firmą. Vestager odpierała te zarzuty, twierdząc, że chodzi przede wszystkim o to, aby firmy z branży nowych technologii, funkcjonujące na terenie Unii Europejskiej, respektowały zasady unijnego prawa[62]. Firmie grozi grzywna wysokości nawet 6 mld euro[63].

Trzeba zaznaczyć, że działania dyscyplinujące podjęto nie tylko w stosunku do Google. Już w 2011 r. V. Reding, komisarz ds. sprawiedliwości, wymiaru sprawiedliwości i obywatelstwa ostrzegła Facebook i podobne serwisy oraz poparła prawo do „bycia zapomnianym w Internecie". W przemówieniu w Parlamencie Europejskim stwierdziła, że „mający siedzibę w USA serwis społecznościowy, który ma miliony aktywnych użytkowników w Europie, musi przestrzegać reguł obowiązujących w UE"[64]. Odnosząc

---

57 „1661 wniosków z Polski do Google o usunięcie danych z wyników wyszukiwania", *Rzeczpospolita* 4.07.2015, dostęp 25.07.2014, http://www.rp.pl/artykul/1123284-1661-wnioskow-z-Polski-do-Google-o-usuniecie-danych-z-wynikow-wyszukiwania.html.

58 „Google udostępnia formularz «bycia zapomnianym»", dostęp 2.06.2014, http://www.wirtualnemedia.pl/artykul/google-udostepnia-formularz-do-bycia-zapomnianym.

59 „Google musi odnieść się do zarzutów Komisji Europejskiej", dostęp 20.12.2012, http://www.wirtualnemedia.pl/artykul/google-musi-odniesc-sie-do-zarzutow-komisji-europejskiej.

60 Kordian Kuczma, „Jak nas oszukuje Google?", *Gazeta Finansowa* 27.03.2015, dostęp 29.04.2015, http://www.gf24.pl/22785/jak-nas-oszukuje-google.

61 Michał Żuławiński, „Parlament Europejski chce podziału Google'a", dostęp 27.11.2014, http://www.bankier.pl/wiadomosc/Parlament-Europejski-chce-podzialu-Google-a-7225439.html.

62 Joe Nocera, „Europe's Google Problem", *The New York Times* 28.04.2015, dostęp 11.03.2017, http://www.nytimes.com/2015/04/28/opinion/joe-nocera-europes-google-problem.html?ref=topics&_r=0.

63 Bartosz Węglarczyk, „Europa wydaje wojnę Google", *Rzeczpospolita* 14.04.2015, dostęp 29.04.2015, http://www.rp.pl/artykul/1193709.html.

64 „UE ostrzega Facebooka. Internauta ma prawo zostać zapomnianym", dostęp 18.03.2011, http://www.wirtualnemedia.pl/artykul/ue-ostrzega-facebooka-internauta-ma-prawo-zostac-zapomnianym.

się wprost do ochrony danych osobowych w przestrzeni cyfrowej powiedziała: „Chcę wyraźnie podkreślić, że ludzie powinni mieć prawo, a nie tylko możliwość, do wycofania swojej zgody na przetwarzanie danych. (…) To kontrolujące je podmioty będą musiały udowodnić, że muszą je przechowywać, a nie indywidualni użytkownicy, że nie jest to konieczne”[65].

Zakończenie

Ochrona prywatności w przestrzeni cyfrowej staje się jednym z kluczowych zagadnień w rozwoju nowych technologii. Tym bardziej, że coraz częściej stają się one łupem przestępców czy narzędziem wojny lub terroryzmu. Pojedynczy użytkownik sieci, który często nie czyta regulaminów zakładanych profili czy kont e-mail jest narażony na niebezpieczeństwa, z których często nie zdaje sobie sprawy. Dane osobowe stają się łakomym kąskiem zarówno dla wielkich korporacji internetowych (co przekłada się na całkiem wymierne, milionowe zyski z serwisów społecznościowych), jak i agencji rządowych.

Działania Unii Europejskiej w zakresie regulowania obecności danych osobowych w przestrzeni cyfrowej różnią się od tych podejmowanych za oceanem, co wynika w przeważającej części z innego podejścia do kształtowania przestrzeni ekonomicznej wolnego rynku handlu i usług. Stany Zjednoczone wystrzegają się daleko idących interwencji i ograniczeń, zwłaszcza w dziedzinie handlu i ładu korporacyjnego. Unia Europejska, zwłaszcza pod koniec pierwszej dekady XXI wieku, przyjęła klarowny kurs ograniczający ingerencję gigantów internetowych w sferę prywatności obywateli. Chodzi przede wszystkim o świadome podejmowanie decyzji. Jeżeli obywatel Unii chce się pozbyć części swojej prywatności, niech to czyni świadomie. Znalazło to swój wyraz zarówno w orzecznictwie prawnym, jak i w działaniach obywatelskich. Całkowicie kluczowe stały się tutaj dwa orzeczenia Trybunału Sprawiedliwości Unii Europejskiej z kwietnia i maja 2014 r.

Wydaje się, że została powstrzymana, zwłaszcza w Europie, daleko posunięta swoboda korporacji w zbieraniu informacji o konsumentach. Działania odpowiednich agencji rządowych są zdecydowane i przynoszą efekty[66]. Więcej dzisiaj zależy od samych użytkowników, którzy wciąż nie są świadomi swoich praw lub bardzo często podejmują działania ryzykowne w sieci. Niewątpliwe niezbędny jest nacisk społeczny na duże korporacje w kierunku przestrzeganiu polityki prywatności[67]. Agencje rządowe, mające

65 „UE ostrzega Facebooka. Internauta ma prawo zostać zapomnianym”.

66 Na początku 2019 r. francuski urząd ochrony danych osobowych (*Commission nationale de l’informatique et des libertés* – CNIL) nałożył na Google karę w wysokości 50 mln euro za nieprzestrzeganie europejskich przepisów o ochronie danych osobowych. „Francja nakłada na Google 50 mln euro kary za łamanie przepisów RODO”, dostęp 22.01.2019, https://www.wirtualnemedia.pl/artykul/francja-naklada-na-google-50-mln-euro-kary-za-lamanie-przepisow-rodo-dlaczego.

67 Np. ujawniono fakty, że Facebook płacił swoim użytkownikom 20 dolarów miesięcznie za umieszczenie w ich urządzeniach specjalnej aplikacji – Facebook Research. Dzięki niej otrzymał dostęp do cennych informacji

chronić prawa obywatelskie, mają również dostęp do wielu wrażliwych informacji (jak np. dotyczących zdrowia obywateli), powinny działać transparentnie i podlegać kontroli organów posiadających społeczny mandat.

Ochrona prywatności w Internecie wciąż jednak staje przed kolejnymi wyzwaniami. W najbliższych latach takim wyzwaniem może stać się tzw. Internet rzeczy. Czy łatwo będzie ochronić życie prywatne człowieka, jeżeli informacje o nim będą przekazywać do sieci także urządzenia codziennego użytku? Na to znów będą musieli odpowiedzieć nie tylko użytkownicy tych urządzeń, ale również instytucje odpowiedzialne za ochronę naszej prywatności.

Bibliografia

„1661 wniosków z Polski do Google o usunięcie danych z wyników wyszukiwania". *Rzeczpospolita* 4.07.2015. Dostęp 25.07.2014. http://www.rp.pl/artykul/1123284-1661-wnioskow-z-Polski-do-Google-o-usuniecie-danych-z-wynikow-wyszukiwania.html.

Agencja Praw Podstawowych Unii Europejskiej, Rada Europy – Europejski Trybunał Praw Człowieka. *Podręcznik europejskiego prawa o ochronie danych*. Luksemburg: Urząd Publikacji Unii Europejskiej, 2014.

Altman Irvin, „Privacy Regulation: Culturally Universal or Culturally Specific?". *Journal of Social Issues* 3 (1977): 66–84. Dostęp 26.02.2017. http://courses.cs.vt.edu/cs6204/Privacy-Security/Papers/Privacy/Privacy-Regulation.pdf.

Barocas, Solon, Helen Nissenbaum. „Big Data's End Run around Anonymity and Consent". W: *Privacy, Big Data and the Public Good. Frameworks for Engagement*, red. Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, 44–75. New York: Cambridge University Press, 2014.

Biernatowski, Piotr. „Orzeczenie: Niekonstytucyjność retencji danych – wyrok czeskiego Trybunału Konstytucyjnego". Dostęp 24.04.2015. http://www.prawaczlowieka.edu.pl/index.php?orzeczenie=f66b7dcd21696a4242e1ff93608c405741802c92-b0.

Broache, Anne. „Google attacked over privacy policy visibility". Dostęp 27.04.2015. http://www.cnet.com/news/google-attacked-over-privacy-policy-visibility.

Brzozowska, Monika. *Ochrona danych osobowych w sieci*. Wrocław: Wydawnictwo Prescom, 2012.

Caspar, Johannes. „Sammlung der Daten von Nicht-Nutzern durch Facebook unzulässig". Dostęp 28.02.2017. https://www.datenschutz-hamburg.de/uploads/media/pressemeldung-2010-04-08__Facebook_Maengel_.pdf.

„Czy można podsłuchiwać rozmowy ze Skype? «Bez komentarza!»". Dostęp 24.07.2012. http://tech.wp.pl/kat,1009785,title,Czy-mozna-podsluchiwac-rozmowy-na-Skype-Bez komentarza,wid,14785021,wiadomosc.html?ticaid=114e48.

o użytkowaniu, jak np. wyszukiwanie hasła, prywatne wiadomości czy odwiedzane strony internetowe. „Facebook płacił użytkownikom 20 dol. miesięcznie za możliwość ich śledzenia. Apple cofa certyfikaty", dostęp 31.01.2019, https://www.wirtualnemedia.pl/artykul/facebook-placil-uzytkownikom-20-dol-miesiecznie-za-mozliwosc-ich-sledzenia-dlaczego.

Dijk van, Jan. *Społeczne aspekty nowych mediów.* Warszawa: Wydawnictwo Naukowe PWN, 2010.

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej). Dz.U. L 201 z 31.7.2002.

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (dyrektywa o zatrzymywaniu danych). Dz.U. L 105 z 13.05.2006.

Dyrektywa o ochronie danych. Dz.U. L 281 z 23.11.1995.

„Facebook największym zagrożeniem dla prywatności w Internecie". Dostęp 14.01.2014. http://www.wirtualnemedia.pl/artykul/facebook-najwiekszym-zagrozeniem-dla-prywatnosci-w-internecie.

„Facebook płacił użytkownikom 20 dol. miesięcznie za możliwość ich śledzenia. Apple cofa certyfikaty". Dostęp 31.01.2019. https://www.wirtualnemedia.pl/artykul/facebook-placil-uzytkownikom-20-dol-miesiecznie-za-mozliwosc-ich-sledzenia-dlaczego.

Farivar, Cyrus. „Facebook violates German law, Hamburg data protection official says". Dostęp 20.04.2015. http://www.dw.de/facebook-violates-german-law-hamburg-data-pro_tection-official-says/a-15290120.

„Francja nakłada na Google 50 mln euro kary za łamanie przepisów RODO. Dostęp 22.01.2019. https://www.wirtualnemedia.pl/artykul/francja-naklada-na-google-50-mln-euro-kary-za-lamanie-przepisow-rodo-dlaczego.

„Francja wzywa Twittera, Facebooka i Google do blokowania kont terrorystów". Dostęp 29.01.2015. http://www.wirtualnemedia.pl/artykul/francja-wzywa-twittera-facebooka-i-google-do-blokowania-kont-terrorystow.

„Google musi odnieść się do zarzutów Komisji Europejskiej". Dostęp 20.12.2012. http://www.wirtualnemedia.pl/artykul/google-musi-odniesc-sie-do-zarzutow-komisji-europejskiej.

„Google udostępnia formularz «bycia zapomnianym»". Dostęp 2.06.2014. http://www.wirtualnemedia.pl/artykul/google-udostepnia-formularz-do-bycia-zapomnianym.

„Google: prawie ćwierć miliona Niemców nie chce Street View". Dostęp 22.10.2010. http://www.wirtualnemedia.pl/artykul/google-prawie-cwierc-miliona-niemcow-nie-chce-street-view.

Gorman, Lyn, David McLean. *Media i społeczeństwo. Wprowadzenie historyczne*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, 2010.

„Grupa studentów walczy z Facebookiem". Dostęp 5.12.2012. http://www.wirtualnemedia.pl/artykul/grupa-studentow-walczy-z-facebookiem.

Gubernat, Barbara. „Europa przeciwko Facebookowi – przygotowania do decydującego starcia". Dostęp 1.03.2017. http://panoptykon.org/wiadomosc/europa-przeciwko-facebookowi-przygotowania-do-decydujacego-starcia.

Jasionek, Katarzyna. „Google czyta naszą pocztę – przypomina Microsoft". *Komputer Świat* 8.02.2013. Dostęp 19.04.2015. http://www.komputerswiat.pl/nowosci/programy/2013/06/google-czyta-nasza-poczte-przypomina-microsoft-wideo.aspx.

Johnson, Deborah G. „Computer Ethics". W: *Academy and the Internet*, red. Helen Nissenbaum, Monroe E. Price, 143–167. New York, Washington, D.C./Baltimore, Bern, Frankfurt am Main, Berlin, Brussels, Vienna, Oxford: Peter Lang Inc., International Academic Publishers, 2004.

Karta Praw Podstawowych Unii Europejskiej. Dz.U. C 83/394 z 30.03.2010.

Kołodziejczyk, Łukasz. *Prywatność w Internecie*. Warszawa: Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, 2014.

Kuczma, Kordian. „Jak nas oszukuje Google?". *Gazeta Finansowa* 27.03.2015. Dostęp 29.04.2015. http://www.gf24.pl/22785/jak-nas-oszukuje-google.

K.U. przeciwko Finlandii, nr 2872/02 z 2 grudnia 2008 r. Dostęp 9.03.2017. http://www.prawaczlowieka.pl/precedens/aktualnosci/wyrok-w-sprawie-k-u-przeciwko-finlandii-ochrona-dobrego-imienia-przed-znieslawieniem-za-pomoca-in.html.

Nissenbaum, Helen. „A Contextual Approach to Privacy Online". *Daedalus, the Journal of the American Academy of Arts & Science* 4 (2011): 32–48. Dostęp 4.03.2017. https://www.amacad.org/multimedia/pdfs/publications/daedalus/11_fall_nissenbaum.pdf.

Nocera, Joe. „Europe's Google Problem". *The New York Times* 28.04.2015. Dostęp 11.03.2017. http://www.nytimes.com/2015/04/28/opinion/joe-nocera-europes-google-problem.html?ref=topics&_r=0.

O'Brien, Kevin J. „Austrian Law Student Faces Down Facebook". *The New York Times* 5.02.2012. Dostęp 20.07.2016. http://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html?

Parent, William. „Privacy: A Brief Survey of the Conceptual Landscape". *Santa Clara High Technology Law Journal* 1 (1995): 21–26.

Petronio, Sandra. „Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples". *Communication Theory* 4 (1991): 311–335.

Polke-Majewski, Karsten. „Ilse Aigner «Bei Facebook sehe ich viele Fragezeichen»". *Zeit* 20.09.2011. Dostęp 1.03.2017. http://www.zeit.de/digital/datenschutz/2011-09/aigner-facebook-datenschutz.

Rada Europy. „Europejska Konwencja Praw Człowieka". Dostęp 3.03.2017. http://www.echr.coe.int/Documents/Convention_POL.pdf.

Rand, Ayn. *The Fountainhead*. Overland Park: International Collectors Library, 1968.

Roy, Jim. „Polis and Oikos in Classical Athens". *Greece and Rome* 46 (1999): 1–18.

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych. Dz.U. L 8 z 12.1.2001.

„Sammelklage gegen Facebook eingebracht". Dostęp 21.04.2015. http://www.ots.at/presseaussendung/OTS_20140801_OTS0060/sammelklage-gegen-facebook-eingebracht.

Schmidt, Florian. „Datenschützer Caspar kritisiert Gesichtserkennung bei Facebook". *Computer Bild* 9.02.2013. Dostęp 28.02.2017. http://www.computerbild.de/artikel/cb-News-Internet-Gesichtserkennung-Facebook-Datenschutz-Johannes-Caspar-Gesichtserkennung-6259152.html.

Thomson, Judith J. „The Right to Privacy". *Philosophy and Public Affairs* 4 (1975): 295–314.

Trybunał Sprawiedliwości Unii Europejskiej. „Wyrok Trybunału (wielka izba) z dnia 13 maja 2014 r.". Dostęp 28.04.2015. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd796004328b0548beb8bedf2537dbb54d.e34KaxiLc3qMb40Rch0SaxuPchr0?text=&docid=152065&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=255813.

Trybunał Sprawiedliwości Unii Europejskiej. „Wyrok w sprawach połączonych C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger i in.". Dostęp 24.04.2015. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054pl.pdf.

„UE ostrzega Facebooka. Internauta ma prawo zostać zapomnianym". Dostęp 18.03.2011. http://www.wirtualnemedia.pl/artykul/ue-ostrzega-facebooka-internauta-ma-prawo-zostac-zapomnianym.

Warren, Samuel, Louis D. Brandeis. „The Right to Privacy". *Harvard Law Review* 5 (1890). Dostęp 16.04.2015. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Węglarczyk, Bartosz. „Europa wydaje wojnę Google". *Rzeczpospolita* 14.04.2015. Dostęp 29.04.2015. http://www.rp.pl/artykul/1193709.html.

Westin, Alan. „Social and Political Dimensions of Privacy". *Journal of Social Issues* 2 (2003): 431–453. Dostęp 24.02.2017. http://www.privacysummersymposium.com/reading/westin.pdf.

„Zuckerberg: Facebook powinien być dostępny dla dzieci poniżej 13. roku życia". Dostęp 25.05.2011. http://www.wirtualnemedia.pl/artykul/zuckerberg-facebook-powinien-byc-dostepny-dla-dzieci-ponizej-13-roku-zycia.

„Zuckerberg: prywatność już nie jest normą społeczną". Dostęp 12.01.2010. http://www.wirtualnemedia.pl/artykul/zuckerberg-prywatnosc-juz-nie-jest-norma-spoleczna.

Żuławiński, Michał. „Parlament Europejski chce podziału Google'a". Dostęp 27.11.2014. http://www.bankier.pl/wiadomosc/Parlament-Europejski-chce-podzialu-Google-a-7225439.html.

Streszczenie

Człowiek zawsze starał się oddzielać sferę działalności publicznej od sfery prywatnej, domowej. Czynili to już starożytni. Było to też w jakimś sensie wyznacznikiem postępu cywilizacyjnego. Nowożytne ujęcie problemu prywatności datuje się na koniec XIX wieku, kiedy próbę jej wyodrębnienia jako osobnego prawa podjęli S. Warren i L. Brandeis.

Podejście do prywatności zmieniło się jednak całkowicie pod wpływem rozwoju Internetu drugiej fali i mediów społecznościowych. Dla korporacji internetowych prywatność przestała być normą społeczną. Obywatele poczuli się zagrożeni. Stąd działania podjęte w Unii Europejskiej na rzecz ochrony prywatności w cyfrowym świecie. Mają one na poziomie poszczególnych państw szereg charakterystycznych cech (np. w Niemczech).

Natomiast na poziomie ogólnounijnym chodzi przede wszystkim o działania służące harmonizacji prawa oraz wywieraniu skutecznej presji na wielkie korporacje internetowe. W większości przyjmowane rozwiązania gwarantują dużo wyższy poziom ochrony prywatności w cyfrowym świecie, aniżeli ma to miejsce np. w Stanach Zjednoczonych.

Słowa kluczowe: Internet, media społecznościowe, prywatność, Unia Europejska

Abstract

MEDIA POLICY OF THE EUROPEAN UNION WITH RESPECT TO PRIVACY ISSUE IN NEW MEDIA

Man has always tried to separate the public sphere from the private one. It was practised in the ancient times. It was also a determinant of the civilisation progress. The modern approach to the issue of privacy dates back to the late nineteenth century, when S. Warren and L. Brandeis attempted to isolate it in the form of a stand-alone law.

The approach to privacy has been entirely changed under the influence of the second wave of the Internet and the growth of social media. For the Internet corporations privacy are not the social norm any longer. People feel threatened. Hence, the actions have been taken by the European Union to protect privacy in the digital world. At the level of individual states they have a number of specific characteristics (e.g. in Germany). However, at the EU level it is primarily all about measures which are to harmonise the laws which exert effective pressure on the large Internet corporations. The majority of the adopted solutions guarantee a far higher level of protection privacy in the digital world than it is in the United States, for example.

Keywords: Internet, social media, privacy, European Union