FOLIA 266

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 9 (2019)
ISSN 2082-0917
DOI 10.24917/20820917.9.5

Emilia Musiał
Uniwersytet Pedagogiczny w Krakowie
ORCiD ID: 0000-0002-0517-1461

Prywatność w Sieci – wybrane zagadnienia

Wstęp

Każdy człowiek, niezależnie od wieku, ma prawo do prywatności – obszaru, w który bez pozwolenia nie wolno wkraczać. A zatem nikt bez naszej zgodny nie może naruszać naszej sfery cielesnej, terytorialnej, informacyjnej, czy też komunikacyjne.

Niewątpliwie jednak zmiany zachodzące we współczesnym świecie i rozwój technologii pozwalających na badanie ludzkich aktywności (zbieranie, gromadzenie i wyszukiwanie informacji dotyczących innych osób) zmieniają paradygmat prywatności i sprawiają, że bardzo silnie wzrasta konieczność prawnej ochrony ludzkiego prawa do prywatności.

Stąd istotne jawią się pytania o to, co jeszcze we współczesnym świecie jest prywatne, a co publiczne, czym jest prywatność, którą mamy chronić i jak chronić to, do czego nikt nie powinien mieć dostępu. I wreszcie co zrobić, by nasze dane były bezpieczne?

Pojęcie prawa do prywatności

Prawo do prywatności zalicza się do praw człowieka pierwszej generacji, a sfera prywatności życia jako odrębne dobro prawne podlega obecnie ochronie w większości współczesnych systemów prawnych[1]. W literaturze przedmiotu możemy zauważyć dwa główne podejścia do kategorii prywatności. Pierwsze podejście akcentuje konieczność zwiększenia form i zakresu poziomu ochrony prywatności. Drugie zaś pragnie ograniczyć sferę prywatności, uzasadniając to działalnością wyspecjalizowanych instytucji państwowych, zwalczających zagrożenia wymierzone w bezpieczeństwo społeczeństwa i całego państwa[2].

Kwestia prywatności wiąże się z interesem własnym jednostki, jej dobrem oraz działaniami podejmowanymi przez nią w celu ochrony tej wartości, stąd pojęcie to możemy definiować jako przestrzeń wolnego poruszania się, domena autonomicznej

[1] M. Pryciak, *Prawo do prywatności*, http://www.bibliotekacyfrowa.pl/Content/37379/011.pdf [dostęp: 10.11.2018].

[2] J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak, A. Preisner (red.), Wydaw. Sejmowe, Warszawa 2002, s. 278.

aktywności, która wolna jest od kontroli innych podmiotów. W zależności od systemu społeczno-kulturowego, w jakim funkcjonuje jednostka, sfera prywatności jest różnie określana w zakresie interakcji, stopnia dystansu i poziomu izolacji[3].

Warto zauważyć, że kategoria prywatności (*privacy*) jest koncepcją powstałą na gruncie prawa anglosaskiego. Po raz pierwszy charakterystyka prawa do prywatności pojawiła się w 1890 r. dzięki amerykańskim profesorom prawa – V. Brandeisowi i E. Warrenowi, którzy określili ją jako „uprawnienie do wyłączności, odrębności tajemnicy i samotności"[4]. Innym badaczem, który zajmował się zagadnieniem „prywatności" jest Joseph Kohler, który w 1907 roku zdefiniował to pojęcie – w odniesieniu do tajemnicy korespondencji – jako „swoboda rozporządzania informacjami na swój temat"[5].

Prawo do prywatności jest pojęciem bardzo złożonym i szerokim, trudno jest także znaleźć precyzyjną definicję pojęcia prywatności w systemach prawnych poszczególnych państw. W polskim piśmiennictwie naukowym odnajdujemy koncepcję prywatności A Kopffa, który twierdzi, że: „dobrem osobistym w postaci życia prywatnego jest to wszystko, co ze względu na uzasadnione odosobnienie się jednostki od ogółu służy jej do rozwoju fizycznej lub psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej"[6]. Dzielił on sferę życia prywatnego na dwie podsfery: sferę intymnego życia osobistego, czyli osobiste doznania każdego człowieka, o których jedynie wyjątkowo informuje osoby mu najbliższe (sfera ta powinna być w pełni chroniona przez przepisy prawa) oraz sferę prywatnego życia osobistego, do której zalicza się przeżycia osobiste lub rodzinne znane tylko osobom najbliższym oraz znajomym, z wyłączeniem osób trzecich (jej naruszenie może być usprawiedliwione przez powołanie się na „usprawiedliwione zainteresowanie").

Nie ulega jednak wątpliwości, że prywatność jest szczególnie istotnym i wrażliwym elementem określającym faktyczny i prawny status człowieka (jedna z podstawowych wartości pozamajątkowych, która wymaga poszanowania) i dlatego ochrona tego dobra jest przewidziana w podstawowych konwencjach międzynarodowych m.in. w Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji" (art. 8), a także w Konstytucji RP z 1997 r.: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym" (art. 47). Przepisy dotyczące poszanowania życia prywatnego i ochrony danych osobowych znajdują się również w Karcie praw podstawowych Unii Europejskiej jak również Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), które obowiązuje od dnia 25 maja 2018 roku. Warto zaznaczyć, że w Polsce nowe

[3] Ibidem.

[4] S.D. Warren, L. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, vol. IV, s. 193–220. Podaję za: M. Pryciak, op. cit.

[5] J. Braciak, op. cit.

[6] A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne*, [w:] *Studia Cywilistyczne: zbiór rozpraw z zakresu prawa cywilnego, prawa międzynarodowego prywatnego, prawa pracy oraz prawa procesowego cywilnego*, S.M. Grzybowski (red.), t. XX, PWN, Warszawa–Kraków 1972, s. 3–44.

regulacje w zakresie ochrony danych osobowych przyjęte na poziomie UE zapewnia podpisana przez Prezydenta dnia 10 maja 2018 r. ustawa o ochroni danych osobowych, która daje o wiele szerszą gamę środków, dzięki którym mamy kontrolę nad swoimi danymi osobowymi[7].

We współczesnym świecie kwestia prywatności i poufności naszych danych dotyczy także (a może przede wszystkim) naszej aktywności w internecie (internet stał się naszym przysłowiowym drugim domem, miejscem, gdzie nie tylko prowadzimy życie towarzyskie, ale także uczymy się i pracujemy). I tu m.in. naprzeciw wychodzą nam zmiany, które wprowadza RODO, a które dotyczą w dużej mierze Sieci. Każdy bowiem użytkownik internetu zyskuje narzędzia do świadomego zarządzania swoimi danymi osobowymi – kluczowa w tym względzie jest sama definicja danych osobowych, która w kontekście internetu i nowych technologii, została rozszerzona o adres IP i pliki *cookies*. RODO reguluje także kwestie związane z danymi osobowymi biometrycznymi (linie papilarne, skan źrenic czy twarzy) coraz częściej wykorzystywanymi jako kody dostępu do sprzętu IT.

Unijne przepisy o ochronie danych zapewniają ochronę danych osobowych zawsze, gdy dane te są gromadzone – np. przy zakupach przez internet, ubieganiu się o pracę lub składaniu wniosku o kredyt bankowy. Przepisy te stosuje się zarówno do przedsiębiorstw i organizacji (publicznych i prywatnych) z Unii Europejskiej, jak i spoza niej – takich jak *Facebook* czy *Amazon*, które oferują towary i usługi w UE. W unijnych przepisach o ochronie danych, zawartych w ogólnym rozporządzeniu UE o ochronie danych (RODO), opisano nie tylko różne sytuacje, w których przedsiębiorstwo lub organizacja może gromadzić lub ponownie wykorzystywać nasze dane osobowe, ale także sytuacje wymagające zgody na ich przetwarzanie i ewentualne jej wycofanie, umożliwiające sprzeciwienie się wykorzystywaniu danych do celów marketingu bezpośredniego, jak również skorygowanie nieprawidłowych danych osobowych, które Cię dotyczą.

Uzupełnieniem RODO i regulującym dodatkowo kwestie prywatności w Sieci jest rozporządzenie *ePrivacy* w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej uchylającego dyrektywę 2002/58/WE. Obecnie rozporządzenie *ePrivacy* jest wciąż w trakcie przygotowań, a jego celem jest wzmocnienie ochrony użytkowników tzw. urządzeń końcowych, czyli w szczególności komputerów, telefonów, smartfonów, czy tabletów przed nadmierną ingerencją w sferę ich prywatności[8]. Dostawcy usług łączności (np. dostawcy internetu czy dostawcy telekomunikacyjni), a także inne podmioty coraz częściej wykorzystują dane pozyskane z urządzeń końcowych, takie jak dane o historii przeglądarki, ruchu na stronach internetowych lub dane naszej lokalizacji w celu świadczenia dodatkowych usług i w celach marketingowych. Użytkownicy takich urządzeń powinni być zatem chronieni i mieć kontrolę nad swoimi danymi.

Warto zwrócić uwagę, że w informatyce prywatność stanowi pokrewny do anonimowości problem z zakresu bezpieczeństwa teleinformatycznego. Oprócz unormowań prawnych prywatność podlega także ochronie metodami technologicznymi,

[7] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, http://prawo.sejm.gov.pl/isap.nsf/ DocDetails.xsp?id=WDU20180001000 [dostęp: 10.11.2018].

[8] https://rodo.iab.org.pl/eprivacy/ [dostęp: 5.11.2018].

takimi jak kryptografia. Ponadto na rzecz prawa obywateli do prywatności w elektronicznym świecie działa założona w 1990 roku w Stanach Zjednoczonych pozarządowa organizacja *Electronic Frontier Foundation* (na uwagę zasługuje projekt badawczy *Panopticlick*, którego celem jest lepsze poznanie narzędzi i technik śledzenia online oraz testowanie dodatków, które mają chronić użytkownika przed inwazyjnym śledzeniem).

Czy istnieje prywatność w Internecie?

Fakty są niezaprzeczalne – internet jest dziś podstawą funkcjonowania świata. Wprawdzie nie we wszystkich jego częściach, ale liczba „połączonych" ludzi rośnie z roku na rok. Otóż, dostęp do Sieci mają już ponad 4 miliardy osób (53% naszej 7,5 miliardowej populacji). W Europie dostęp do internetu ma 80% populacji, a Polska z wynikiem 78% plasuje się na 24 miejscu w globalnym rankingu[9]. A do czego Polakom służy internet i co robimy w Sieci? Otóż wśród najczęściej podejmowanych aktywności znajdują się: przeglądanie witryn internetowych (84% badanych), wysyłanie poczty (83% badanych), odwiedzanie serwisów społecznościowych (69% badanych)[10].

Ponadto, jak się okazuje Polacy zaczęli dbać o prywatność w Sieci – coraz lepiej zdają sobie sprawę, że internet jest miejscem publicznym i sami powinni dbać w nim o swoją prywatność (90% internautów ma świadomość, że strony internetowe zbierają informacją o tym, co robią). Najnowszy raport *Prywatność w sieci* pokazuje, że znacznie w górę poszły takie parametry jak czyszczenie historii przeglądarek, kasowanie czy blokowanie *cookies* (wzrosła wiedza o tym czym są i do czego służą ciasteczka), znajomość regulaminów i Polityki Prywatności. Niestety na potęgę udostępniamy swoje dane w Sieci, nie tylko imię i nazwisko, ale i numery telefonów, kart czy PESEL[11].

Korzystanie z internetu nieuchronnie wiąże się z udostępnianiem informacji o sobie. Niektórymi dzielimy się świadomie, a innymi – mimowolnie, czasem nawet nie zdając sobie z tego sprawy. Przeglądamy portale internetowe, oglądamy filmy, zakładamy konta pocztowe, korzystamy z różnych aplikacji. Wszystko to dostępne jest na wyciągnięcie ręki i często darmowe. Jednak nie ma nic za darmo. Za wszystko bowiem trzeba zapłacić, a w dobie cyfryzacji walutą jest ludzka prywatność. I tak np. rejestrując się w darmowych serwisach płacimy naszymi danymi osobowymi, informacjami o nawykach, przyzwyczajeniach i zainteresowaniach (naszymi preferencjami) – wszystkim tym, co przez lata próbowaliśmy trzymać w tajemnicy. Dane, z pozoru rozsypane w bezładzie, pozostają jednak elementami układanki, z której korzysta wielu (ciekawscy, reklamodawcy, instytucje rządowe, organizacje przestępcze), niemalże bez ograniczeń.

---

[9] https://www.internetworldstats.com/stats.htm [dostęp: 10.11.2018].

[10] *Do czego służy nam Internet*? https://www.zadluzenia.com/artykul/do-czego-sluzy-nam-internet/ [dostęp: 12.11.2018].

[11] *Prywatność w Sieci 2016/2017*, IAB Polska, https://www.iab.org.pl/wp-content/uploads/2017/03/ IAB_Polska_Prywatnosc_w_sieci_2016_2017_raport.pdf [dostęp: 10.11.2018].

Nie należy zapominać, że już samo wejście na dowolną stronę internetową uruchamia przepływ danych. Automatycznie zostają jej przesłane: nasz adres IP oraz informacje o przeglądarce (m.in. wersja, system operacyjny, język i czcionki). Ponadto prawdziwą kopalnią informacji o nas są nie tylko dane wpisane w profilu użytkownika, ale m.in. mechanizmy tj. ciasteczka, przyciski mediów społecznościowych, czy też same media społecznościowe, jak również urządzenia za pośrednictwem których łączymy się z internetem. Algorytmy analizując miejsca, do których udajemy się najczęściej, są w stanie dokładnie określić, gdzie mieszkamy, pracujemy, czy mamy dzieci i jeśli tak – w jakim są wieku[12]. Facebook potrafi śledzić nie tylko to, co użytkownicy robią online, lecz także gdzie przebywają w prawdziwym świecie i oferować te dane reklamodawcom. Google zaś, którego mottem jest „nie wyrządzać zła", udostępniło użytkownikom stronę, na której mogą sprawdzić archiwum informacji na swój temat – na przykład, jaką aplikację mieli uruchomioną na telefonie o danej godzinie wybranego dnia z ostatnich lat i gdzie wtedy przebywali, słowem możemy dotrzeć do informacji o tym, jak celnie Google analizuje nasze zachowania[13].

Warto pamiętać, że wiedza na temat naszych działań w Sieci służy różnym podmiotom (wykorzystują mechanizm zwany profilowaniem, który polega na kategoryzowaniu ludzi według cech i zachowań) do różnych celów. Z reklamami opartymi na profilowaniu możemy spotkać się w Sieci niemal na każdym kroku. Mogą być one dobrane do nas pod kątem wieku i płci, lajków i kliknięć (np. w portalach społecznościowym), oglądanych produktów (w sklepach internetowych), wyszukiwanych słów (w wyszukiwarkach) czy treści e-maili (w usługach poczty elektronicznej)[14].

Profilowanie w Internecie dotyczy nie tylko reklam, ale również wyszukiwanych informacji. Większość wyszukiwarek (np. Google, Bing) dopasowuje wyniki do użytkowników, bazując na historii zapytań – docierają do nas jedynie informacje zbieżne z naszymi poglądami i zachowaniami i stąd u dwóch różnych osób wyniki wyszukiwania dla tych samych fraz mogą znacząco się różnić. Tak właśnie działa efekt bańki filtrującej (ang. *filter bubble*). Jak zauważa Eli Pariser – twórca tego terminu – taka funkcjonalność wyszukiwarki na krótką metę może ułatwiać życie, ale na dłuższą – zamykać we własnym świecie i ograniczać horyzonty[15].

Słowem zostawiamy ślady, które widoczne są jak na dłoni, ale w zamian mamy np. dostęp do darmowego oprogramowania. By jednak każdy z nas sam mógł sprawdzić, jakie witryny internetowe i usługi śledzą nasze ruchy w Sieci i co z pozyskanymi danymi robią, polscy inżynierowie i kryptolodzy opracowali narzędzie dostępne

[12] *Prywatność w sieci – jesteś walutą*, https://questus.pl/blog/prywatnosc-jestes-waluta/ [dostęp: 10.11.2018].

[13] *Google otworzyło archiwum wiedzy na Twój temat*, https://www.antyradio.pl/Technologia/internet/Google-otworzylo-archiwum-wiedzy-na-Twoj-temat–9569 [dostęp: 11.11.208].

[14] *Co warto wiedzieć o śledzeniu i profilowaniu w sieci*? https://panoptykon.org/wiadomosc/co-warto-wiedziec-o-sledzeniu-i-profilowaniu-w-sieci [dostęp: 10.11.2018].

[15] E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, http://hci.stanford.edu/courses/cs047n/ readings/The_Filter_Bubble.pdf [dostęp: 10.11.2018]. Przeczytaj więcej na: https://www.semtec.pl/banka-informacyjna-google-facebook/ [dostęp: 10.11.2018].

na stronie www.bringingprivacyback.com[16]. Jak zauważają twórcy tego narzędzi: „Każdego dnia firmy, którym oddaliśmy naszą prywatność, gromadzą informacje na nasz temat – czytają nasze wiadomości tekstowe, e-maile, oglądają nasze zdjęcia, śledzą każdy krok. Sami im na to pozwoliliśmy, akceptując regulaminy różnego typu aplikacji czy platform internetowych. Oddaliśmy im naszą prywatność, bo daliśmy sobie wmówić, że nie mamy innego wyjścia. Ale to nieprawda. Poprzez stronę www.bringingprivacyback.com chcemy uświadamiać ludzi, że mogą postawić granice i chronić swoją prywatność, zwłaszcza, że żyjemy w czasach, w których prywatność stała się walutą"[17].

Reasumując Sieć wie o nas znaczenie więcej niż to, co w sposób świadomy udostępniamy – właściwie można stwierdzić, że jesteśmy śledzeni na każdym kroku. Na podstawie różnych cyfrowych śladów można odgadnąć wiek, płeć, a nawet zidentyfikować konkretną osobę. Powinien o tym pamiętać każdy świadomy użytkownik internetu – także dziecko.

Jak zadbać o naszą prywatność w Sieci?

Internet z jednej strony dał nam wolność i szeroką platformę do wyrażania siebie, a z drugiej wpędził nas w pułapkę inwigilacji i utraty prywatności. Nie wszystko jest jednak stracone – prywatność w sieci jest możliwa, choć jej osiągnięcie wiąże się z instalacją wielu dodatkowych aplikacji i umiejętnością zacierania śladów, które zostawiamy w Internecie. Sam bowiem użytkownik musi zachowywać się w sposób odpowiedzialny i rozważny, unikając działań, które mogą umożliwić jego identyfikację lub wręcz zaszkodzić mu.

Na początek jednak musimy zdać sobie sprawę z kilku najczęściej popełnianych błędów w trakcie korzystania z Sieci, które zdradzają naszą tożsamość. I tak nie powinniśmy m.in.[18]:

1. logować się do wcześniej założonych kont z sieci Tor – będzie można powiązać nasz adres IP z nami jako użytkownikiem konta;
2. logować się na konta z dostępem do pieniędzy przez sieć Tor – nie ma sensu ukrywać swojej obecności w Internecie i logować się do tego typu usług, które m.in. wymagają naszej weryfikacji;
3. zmieniać typu wykorzystywanej sieci w trakcie trwania jednej sesji – bardzo łatwo powiązać adresy IP i czasy dostępu do serwerów;
4. przesyłać wrażliwych danych bez ich szyfrowania – przynajmniej pakujemy przesyłane pliki do archiwum i zabezpieczamy je hasłem;
5. otwierać nieznanych linków i plików – może to być pułapka prowadząca do zainfekowanej witryny;

[16] *Zobacz kto i dlaczego śledzi Cię w Internecie*, https://www.radiozet.pl/Nauka-i-Technologia/Technologia/ Zobacz-kto-i-dlaczego-sledzi-Cie-w-internecie [dostęp: 10.11.2018].

[17] M. Dyka, *Sprawdź, kto cię śledzi w Internecie*, https://www.legalniewsieci.pl/aktualnosci/sprawdz-kto-cie-sledzi-w-internecie [dostęp: 10.11.2018].

[18] K. Dziedzic, *Jak skutecznie zapewnić sobie anonimowość. Anonimowość w Internecie. Kompletny poradnik krok po kroku*. „Komputer Świat" 2018, nr 1 (95), s. 5–7.

6. podawać informacji na nasz temat online – atakujący mogą do nich dotrzeć i posłużyć się nimi w generatorach do łamania haseł;
7. stosować słabych haseł – silne hasło powinno mieć przynajmniej 12 znaków, w tym przynajmniej jedna duża litera, cyfra i znak specjalny.

Jak więc zachować prywatność w Sieci i zamazać zostawione za sobą ślady? Przede wszystkim pierwszą i najważniejszą linią obrony przed wścibskimi oczami jest bezpieczne i anonimowe połączenie z internetem – nie tylko bardzo ryzykowne bywa korzystanie z publicznych Wi-Fi w parkach czy kawiarniach, ale oazą bezpieczeństwa nie jest nawet domowe stałe łącze (dostęp do przeglądanych przez nas stron ma nasz dostawca usług internetowych).

Jedną z dostępnych opcji jest *Virtual Private Network*, czyli w skrócie VPN. Prywatność w Sieci w przypadku VPN zapewniana jest przez szyfrowanie połączenia oraz tworzenie specjalnego wirtualnego „tunelu" wewnątrz internetu. Wśród wad tej technologii trzeba wymienić często występujące spowolnienie łącza i fakt, że dostępne aplikacje tworzące VPN w większości są dostępne po wykupieniu abonamentu.

Kolejny sposób na zapewnienie prywatności w Sieci to korzystanie z tzw. serwerów *proxy*. Mówiąc prosto, serwer tego typu jest pośrednikiem, który wykonuje pewne czynności za klienta. To rozwiązanie pozwala na ukrycie naszego adresu IP. Należy jednak pamiętać, że wiele publicznie dostępnych serwerów pośredniczących przekazuje oryginalny adres klienta do serwera docelowego, przechowują dzienniki połączeń umożliwiające w razie potrzeby zidentyfikowanie klienta i w końcu w większości dostęp do tego typu anonimizerów jest płatny[19].

By skuteczniej ukryć ślady przesyłanych danych warto skorzystać z techniki nazywanej *routingiem* cebulowym lub trasowaniem cebulowym w skrócie nazywanym Tor (ang. *The Onion Router* – angielskie słowo „cebula" w nazwie ma związek z wielowarstwową strukturą tej sieci). Aby połączyć się z „cebulowym internetem", należy ściągnąć i zainstalować specjalny program – np. *Vidalia*. Przydatna może okazać się dedykowana przeglądarka Tor Browser.

Kolejną linią obrony przed wścibskimi oczami innych jest przeglądarka internetowa. Tu przede wszystkim istotna jest umiejętność korzystania ze standardowych przeglądarek, czyli włączenie specjalnego trybu anonimowego (w Chrome jest to okno *incognito*, w Firefoksie okno prywatne), jak również zainstalowanie rozszerzeń i nakładek na przeglądarkę, które chronią prywatność w Sieci (np. dodatek *DoNotTrackMe*, który blokuje zapisywanie *cookies* lub popularny *AdBlock*, który uniemożliwia próby wyświetlania reklam). Bardziej radykalnym krokiem jest korzystanie z niestandardowej przeglądarki, która gwarantuje prywatność w Sieci (np. *SRWare Iron*, *DuckDuckGo*, czy też *JonDoFox*).

Możliwa do osiągnięcia w pewnym stopniu prywatność jest także w przypadku poczty elektronicznej. Jeśli chcemy ustrzec się przed skanowaniem naszych maili (w konsekwencji na naszej skrzynce widnieją spersonalizowane reklamy) możemy szyfrować wiadomości wysyłane za pomocą standardowych skrzynek (np. *Gmail*)

[19] R. Sokół, *Jak pozostać anonimowym w sieci. Omijaj natrętów w sieci – chroń swoje dane osobowe*, Wydaw. Helion, Katowice 2015, s. 13–14.

albo postawić na jeden z wielu bezpiecznych serwisów pocztowych. W przypadku wybrania pierwszej opcji należy zastanowić się nad instalacją rozszerzenia do Chrome o nazwie *SecureGmail* lub w przypadku korzystania z programu pocztowego *Thunderbird* (spokrewnionego z przeglądarką Firefox) zainstalować nakładkę o nazwie *Enigmail*. W kontekście bezpiecznych skrzynek poczty elektronicznej, gwarantujących prywatność w Sieci, można wymienić np. *Hushmaila*, który występuje w wersjach darmowych i płatnych.

Nie wolno zapominać, że cieszące się ogromną popularnością portale społecznościowe także wystawiają naszą prywatność na wielkie niebezpieczeństwo. Aby ustrzec się przed wścibskimi oczami, albo w ogóle nie korzystać z serwisów tego typu, albo niezwykle ostrożnie i oszczędnie udzielać się w ich ramach. Pamiętaj, że media społecznościowe zazwyczaj umożliwiają dostosowanie stopnia prywatności. Na Facebooku możesz łatwo określić, kto może zobaczyć to, co publikujesz na swojej tablicy i piszesz na swój temat w ogólnych informacjach profilowych, a jeśli chcemy wyszukać wpisy, które mogą negatywnie rzutować na naszą reputację przydatna może okazać się aplikacja *SimpleWash*. Gdybyśmy jednak zapragnęli pójść krok dalej i usunąć nasze konta na różnych portalach, to możemy skorzystać ze strony *JustDeleteMe*, której jedną z funkcji jest generator fałszywych tożsamości.

Pragnąc otoczyć swoją prywatność w Sieci (przejąć kontrolę nad swoimi danymi) jeszcze grubszym murem, warto także zajrzeć m.in. na stronę projektu *Prism Break*, gdzie znajduje się aktualizowana baza aplikacji dosyć odpornych na próby inwigilacji ze strony amerykańskich służb specjalnych, zainstalować program do kasowania plików z dysku twardego (np. *File Shredder DiskWipe* czy *HDDErase*), który uniemożliwi dotarcie do naszych plików wrzuconych do systemowego kosza, czy też zapoznać się ze stroną Cyfrowa Wprawka, na której znajdziemy m.in. artykuły tłumaczące jak świadomie i bezpiecznie korzystać z nowych narzędzi komunikacji oraz dbać o swoją i innych prywatność w Sieci (projekt Fundacji Panoptykon, https://cyfrowa-wyprawka.org/projekt), pamiętając o znajomości ustawień, dzięki którym możemy zarządzać ochroną naszej prywatności (np. strona Moje Konto Google).

Podsumowanie

W Internecie rozmawiamy z bliskimi, opłacamy rachunki, robimy zakupy – to tam przeniosła się spora część naszego życia – i dlatego warto uświadomić sobie fakt, iż nie ma tu prywatności. Cała nasza aktywność online może być rejestrowana i analizowana, a my możemy, co najwyżej zwiększać poziom trudności i zasobów potrzebnych do skutecznego nas inwigilowania.

Ważne jest zatem przestrzeganie podstawowych zasad dotyczących bezpieczeństwa w Internecie. I chociaż na pierwszy rzut oka stosowanie się do nich wszystkich byłoby trudne, to w rzeczywistości wszystko jest kwestią wdrożonych nawyków, które znacząco mogą utrudnić śledzenie naszych poczynań w Sieci. Wszyscy bowiem powinniśmy poważnie traktować kwestię własnej prywatności i dbać o to, by ważne dane nie wpadły w niepowołane ręce.

Ponadto, nie ulega wątpliwości, że jest jeszcze wiele do zrobienia w temacie edukacji i informowania internautów o zagrożeniach i ochronie ich bezpieczeństwa (przede wszystkim przez podmioty kształtujące środowisko cyfrowe), jak i kontroli nad ich danymi pozostawianymi w Sieci. Optymistyczne jest to (jak pokazują wyniki badań), że sami użytkownicy internetu wyraźnie wykazują takie zapotrzebowanie i istotne braki aktualnie w tych kwestiach.

Bibliografia

Braciak J., *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak, A. Preisner (red.), Wydaw. Sejmowe, Warszawa 2002.

Co warto wiedzieć o śledzeniu i profilowaniu w sieci? https://panoptykon.org/wiadomosc/co-warto-wiedziec-o-sledzeniu-i-profilowaniu-w-sieci [dostęp: 10.11.2018].

Do czego służy nam Internet? https://www.zadluzenia.com/artykul/do-czego-sluzy-nam-internet/ [dostęp: 12.11.2018].

Dyka M., *Sprawdź, kto cię śledzi w Internecie*, https://www.legalniewsieci.pl/aktualnosci/sprawdz-kto-cie-sledzi-w-internecie [dostęp: 10.11.208].

Dziedzic K., *Jak skutecznie zapewnić sobie anonimowość. Anonimowość w Internecie*. *Kompletny poradnik krok po kroku*. „Komputer Świat" 2018, nr 1 (95).

Google otworzyło archiwum wiedzy na Twój temat, https://www.antyradio.pl/Technologia/Internet/Google-otworzylo-archiwum-wiedzy-na-Twoj-temat-9569 [dostęp: 11.11.208].

https://rodo.iab.org.pl/eprivacy/ [dostęp: 5.11.2018].

https://www.internetworldstats.com/stats.htm [dostęp: 10.11.2018].

https://www.semtec.pl/banka-informacyjna-google-facebook/ [dostęp: 10.11.2018].

Kopff A., *Koncepcja prawa do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne*, [w:] *Studia Cywilistyczne: zbiór rozpraw z zakresu prawa cywilnego, prawa międzynarodowego prywatnego, prawa pracy oraz prawa procesowego cywilnego*, S.M. Grzybowski (red.), t. XX, PWN, Warszawa–Kraków 1972.

Pariser E., *The Filter Bubble: What the Internet Is Hiding from You*, http://hci.stanford.edu/courses/cs047n/ readings/The_Filter_Bubble.pdf [dostęp: 10.11.2018].

Pryciak M., *Prawo do prywatności*, http://www.bibliotekacyfrowa.pl/Content/37379/011.pdf [dostęp: 10.11.2018].

Prywatność w sieci – jesteś walutą, https://questus.pl/blog/prywatnosc-jestes-waluta/ [dostęp: 10.11.2018].

Prywatność w Sieci 2016/2017, IAB Polska, https://www.iab.org.pl/wp-content/uploads/2017/03/ IAB_Polska_Prywatnosc_w_sieci_2016_2017_raport.pdf [dostęp: 10.11.2018].

Sokół R., *Jak pozostać anonimowym w sieci. Omijaj natrętów w sieci – chroń swoje dane osobowe*, Wydaw. Helion, Katowice 2015.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, http://prawo.sejm.gov.pl/isap.nsf/ DocDetails.xsp?id=WDU20180001000 [dostęp: 10.11.2018].

Warren S.D., Brandeis L., *The Right to Privacy*, „Harvard Law Review" 1890, vol. IV.

Zobacz kto i dlaczego śledzi Cię w Internecie, https://www.radiozet.pl/Nauka-i-Technologia/Technologia/ Zobacz-kto-i-dlaczego-sledzi-Cie-w-internecie [dostęp: 10.11.2018].

Privacy on the Web – selected problems

Abstract

The development of new technology makes that information about us is collected on a massive scale. Almost every our activity leaves a trail (e.g. credit cards). Especially a lot of these trails we leave using the internet.
So the subject of the development are problems of data protection and privacy on the Web. It's good to know that when we publish information about yourself, we are giving up privacy particles – we lose of information control.
In the article also noted that the first and last names should be avoided, as well as an address or phone number. Be careful to not sent information sensitive and intimate (e.g. health status) or confidential (e.g. PIN to your account).
In addition, we do not always decide for ourselves what information about us is on the Net. Sometimes, someone makes this decision for us. In this situation, we have the right to react – expect others to respect our privacy. We should also respect the privacy of others.
In a word, we forget about our security on the web. Meanwhile, to protect your privacy in the virtual world, you do not have to spend money or try hard. It's enough to follow a few simple rules.

Słowa kluczowe: prywatność, tożsamość, ochrona danych, profilowanie, bańka filtrująca, ślady w Sieci

Key words: privacy, identity, data security, profiling, filter bubble, marks on the Web

Emilia Musiał
doktor nauk pedagogicznych, adiunkt w Instytucie Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego w Krakowie. Wśród jej zainteresowań naukowych znajdują się zagadnienia dotyczące wykorzystania nowych mediów w dydaktyce wraz z towarzyszącymi temu zjawisku szansami i zagrożeniami. Autorka licznych artykułów naukowych ukazujących nowe media nie tylko jako instrumenty edukacyjne czy narzędzia realizowania negatywnych zachowań, ale również jako środowisko socjalizacyjne czy wychowawcze. E-mail: emilia.musial@up.krakow.pl