ALEKSANDRA WYSOKIŃSKA

ZANIK PRYWATNOŚCI JAKO NARASTAJĄCY PROBLEM SPOŁECZEŃSTWA INFORMACYJNEGO

ABSTRACT. Aleksandra Wysokińska, *Zanik prywatności jako narastający problem społeczeństwa informacyjnego* [Loss of privacy as the growing problem of information society], edited by M. Baranowski, „Człowiek i Społeczeństwo", vol. XL, Poznań 2015, pp. 119-136, Adam Mickiewicz University Press. ISBN 978-83-232-2964-3, ISSN 0239-3271.

Since the beginning of its existence, the Internet has been almost synonymous with anonymity, giving unfettered opportunities to create a virtual identity. A lot has changed after the introduction of the era of Web 2.0. The network has become primarily a tool of communication with friends and loved ones, a place of socializing and a giant, constantly expanding photo gallery. People in society, along with benefiting from the growing possibilities of the web have divulged more and more information about themselves. Today, in a time of scandals revealing states spying on their own citizens, and social networks constantly changing their terms of privacy, no one believes in the anonymity of the Internet. This paper is aimed at presenting the most important issues related to the concept of network surveillance, with an emphasis on the problem of online privacy. The task is to draw the attention of researchers, who previously were neglecting the problem of the loss of privacy, which is not only applicable to the virtual life, but also has a significant impact on the functioning offline. Two directions here are the most visible. Users, for the privilege, comfort, or just entertainment, share on the network more and more detailed information about themselves. At the same time the giants of the Internet, as well as governments, increase the scope of their surveillance, which may stand up to even the most aware and cautious person. Changes occur extremely quickly, and this is why publications a few years or even months ago rarely mentioned about problem, and then only briefly, which may be caused by insufficient awareness about its importance and its possible impact on developing societies. However, we cannot forget about increasing the awareness of modern societies, which results in the emergence of tools for privacy protection created by the users themselves.

Aleksandra Wysokińska, Uniwersytet Łódzki, Instytut Socjologii, Katedra Socjologii Sztuki, ul. Prezydenta Gabriela Narutowicza 65, 90-131 Łódź, Poland, e-mail: ola.wysokinska@gmail.com

Historia i geneza pojęcia prywatności

Mówiąc o stopniowym zaniku prywatności dotykającym współczesne społeczeństwa, warto zacząć od historii tego pojęcia. Nie jest to historia zbyt długa, sięgająca zaledwie kilka dekad wstecz. Przez wiele stuleci prywatność nie była bowiem zaliczana do katalogu praw człowieka, o czym świadczy brak zapisów na jej temat choćby w polskiej Konstytucji 3 Maja czy w Konstytucji Stanów Zjednoczonych. Co ciekawe, dużo poważniej do tego zagadnienia podchodzą wyznawcy islamu, których święta księga Koran potępia np. podsłuchiwanie i podglądanie innych. Można też wspomnieć o komunistach traktujących prywatność jako zbędną w życiu człowieka czy o niedoskonałościach technologii komunikacyjnych (np. pierwsze dekady funkcjonowania telefonu), które nie pozwalały użytkownikom na prywatność jeszcze przez długie lata XX wieku. Podczas drugiej wojny światowej Europejczycy zaczęli doceniać wartość prywatności, która mogła stanowić kwestię życia lub śmierci, jako że informacje o wyznaniu czy pochodzeniu wykorzystywane były przy tworzeniu list skazanych na śmierć lub zsyłkę. Te bolesne doświadczenia znalazły odzwierciedlenie w stanowionym prawie i już w 1948 r. prawo do prywatności zostało włączone do katalogu praw człowieka i obywatela zawartych w Deklaracji ONZ. Wprawdzie dokument ten jest jedynie rezolucją, co pozbawia go mocy wiążącej, jednak przyjęta pięć lat później Europejska Konwencja Praw Człowieka daje już obywatelom ratyfikujących ją państw prawo do złożenia skargi do sądu międzynarodowego. Ochrona prywatności w europejskim prawie jest coraz silniejsza, o czym świadczą kolejne dokumenty uchwalane przez poszczególne rządy państw, a także Unię Europejską. Polski ustawodawca również dał obywatelom narzędzie, jakim jest ustawa o ochronie danych osobowych, oraz zapewnił pomoc ze strony Generalnego Inspektora Ochrony Danych Osobowych. Niestety takiego pakietu ochronnego nie daje prawo Stanów Zjednoczonych, a właśnie z tego kraju pochodzi większość technologicznych gigantów: Google, Facebook i Microsoft. Głównym punktem amerykańskiego ustawodawsta jest Konstytucja powstała w czasach, gdy prywatność nie była jeszcze traktowana jako wartość. Oczywiście w razie potrzeby jest ona uzupełniana poprawkami, artykułami czy wyrokami sądów, trzeba jednak pamiętać, że obowiązujące tam prawo precedensowe pozostawia duże pole do manewru w zakresie jego interpretacji.

W ostatnich latach nastąpiła pewna poprawa w obszarze ochrony prywatności internautów, związana prawdopodobnie ze wzrostem świadomości

ustawodawców. Nadal prym w tym zakresie wiedzie Unia Europejska, ale pojawiają się sposoby wpływania na firmy z rodowodem amerykańskim, czego przykładem są nowe regulacje zmuszające Google i podobne podmioty do respektowania tzw. prawa do bycia zapomnianym. Jeśli prawo to jest w mocy jedynie na terenie Wspólnoty, to daje nadzieję, że nie pozostaliśmy sami na polu boju o zachowanie prywatności.

Źródła problemu

W ciągu ostatnich 70 lat nastąpiła ogromna zmiana w postrzeganiu prawa do prywatności, jednak upowszechnienie Internetu i związane z tym zjawiska wymuszają na współczesnych społeczeństwach potrzebę ciągłego, dynamicznego dostosowywania się zarówno w kwestii mentalności, jak i rozwiązań prawnych. W obu tych obszarach mamy ogromny problem, by nadążyć za rzeczywistością wirtualną, co skrzętnie wykorzystują podmioty, w których interesie leży jak najszerszy dostęp do danych. Problem jest na tyle wielowymiarowy, że warto wyodrębnić i omówić jego najważniejsze aspekty.

Jak się wydaje, jednym z największych zagrożeń prywatności użytkowników Internetu są oni sami. Według danych Międzynarodowego Związku Telekomunikacyjnego z 2015 r. dostęp do Internetu ma już 43% ludzkości, uwzględniając zaś podział na kontynenty, można dostrzec, że w Ameryce Północnej wartość ta sięga prawie 90% i dynamicznie rośnie, co pozwala mówić o powszechnym dostępie do Sieci. Niestety wraz ze zwiększającym się zasięgiem Sieci nie idzie odpowiednia edukacja i wzrost świadomości. Wprawdzie w krajach rozwiniętych prowadzone są kampanie społeczne mające na celu zapoznanie społeczeństwa z ewentualnym niebezpieczeństwem, to jest to wciąż kropla w morzu potrzeb. Przede wszystkim należy przyjąć, że cokolwiek umieścimy w Internecie, zostaje tam na zawsze. Błędne jest przeświadczenie, iż zdjęcie czy komentarz usunięty z profilu przestaje istnieć, i jest przynajmniej kilka powodów, dla których tak się dzieje.

Prawo i korporacje przeciwko nam

Istnieją potwierdzone konkretnymi przypadkami obawy, że takie portale jak Facebook przechowują dane, które zostały usunięte przez użytkowników. Dobrym przykładem jest tu *casus* Maksa Schremsa, austriackiego studenta,

który po otrzymaniu od najpopularniejszego serwisu społecznościowego na świecie płyty CD z kompletem danych osobistych (każdy może zwrócić się z prośbą o wygenerowanie i przesłanie takiego pakietu informacji, która według prawa musi być spełniona) odkrył, że znajdują się tam fragmenty prywatnej korespondencji, która została przez niego usunięta. Kolejne doniesienia o podobnych zdarzeniach pozwalają sądzić, że informacje przesłane na serwery pozostają tam dłużej, niż byśmy sobie tego życzyli. Kilka lat temu miał miejsce swoisty wyścig między największymi dostawcami usług internetowych o to, komu najbardziej uda się skrócić czas, po jakim dane są trwale usuwane. Jednak takie zdarzenia jak to opisane wyżej podają w wątpliwość zapewnienia internetowych gigantów o skróceniu tego okresu do kilku miesięcy. O skali problemu może również świadczyć liczba poradników tłumaczących krok po kroku, jak możliwie skutecznie usunąć profile na portalach społecznościowych.

Sam fakt gromadzenia informacji to tylko wierzchołek góry lodowej – jeszcze większym zagrożeniem dla prywatności jest sytuacja prawna, w której wszystkie te dane mogą zostać upublicznione, bez obowiązku informowania o tym zainteresowanego. Wystarczy wspomnieć o amerykańskiej ustawie USA Patriot Act, wprowadzonej w niezwykle krótkim czasie po zamachach terrorystycznych 11 września 2001 r. Stanowi ona rewizję kilku poprzednich ustaw dotyczących prywatności i nadzoru, których w dużej mierze nie udało się uchwalić ze względu na protesty społeczne. Jednak w sytuacji zagrożenia terrorystycznego administracji George'a W. Busha bez problemu udało się zmienić prawo[1] bez debaty publicznej. USA Patriot Act znacząco rozszerza uprawnienia władz do ingerowania w dane prywatnej komunikacji. Krótko mówiąc, od tej pory instytucjom rządowym nie jest potrzebny nakaz sądowy, by uzyskać dostęp do prywatnych danych, wystarczy żądanie skierowane do podmiotów je przechowujących. Co więcej, jest ono połączone z zakazem informowania o tym fakcie inwigilowanej osoby. Postanowienia ustawy mogą zostać wykorzystane właściwie w każdej sytuacji, warunkiem jest jedynie udowodnienie, że dostęp do odpowiednich informacji przyniesie korzyść śledztwu, co otwiera ogromne pole do nadużyć. W związku z falą krytyki ustawa miała stracić ważność z końcem 2005 r., ale wiele jej przepisów obowiązuje do dziś. W ostatnim czasie zostały również ujawnione działania amerykańskiej Agencji Bezpieczeństwa Narodowego (National Security Agency – NSA) mające na celu inwigilację użytkowników Internetu.

[1] Zmianie uległo niemal 20 ustaw federalnych.

W gruncie rzeczy nie trzeba przywoływać tak skrajnych przykładów, jak rządy państw śledzące obywateli, gdyż problem zaczyna się znacznie wcześniej – w polityce prywatności firm internetowych, która przedstawiana jest użytkownikowi w formie regulaminu usługi, z której korzysta. Tajemnicą poliszynela jest to, że mało kto przy rejestrowaniu konta w nowej usłudze poświęca wystarczająco dużo czasu na przestudiowanie obowiązujących warunków, wiele osób nie sprawdza ich nawet pobieżnie. Skutkuje to żenująco niską świadomością praw, jakimi dysponują usługodawcy wobec naszych danych. W połączeniu z dość swobodnym podejściem internetowych gigantów do naszej intymności tworzy się bardzo niebezpieczna sytuacja. Tak brzmi fragment zasad prywatności Google'a:

> Możemy udostępniać informacje [prywatne, jeśli] wymaga tego prawo albo działamy w dobrej wierze, że udostępnianie, zachowanie lub ujawnienie tych informacji jest konieczne do ochrony praw, własności lub bezpieczeństwa Google, użytkowników firmy czy też społeczeństwa[2].

Jak widać, firma pozostawia sobie duże pole do manewru i w tym kontekście jedynym zabezpieczeniem naszej prywatności jest motto „Don't be evil", które z czasem coraz bardziej traci na znaczeniu. A nie możemy zapominać, że decydenci serwisów internetowych podlegają jedynie swoim liderom i udziałowcom, co oznacza, iż nic nie stoi na przeszkodzie zmianom regulaminów, którym użytkownicy mogą sprzeciwić się jedynie poprzez rezygnację z usługi, co często wcale nie jest proste. Co więcej, podmioty takie jak Google dają sobie także prawo do „czytania" fragmentów wiadomości osób niekorzystających bezpośrednio z ich usług, a jedynie korespondujących z właścicielami skrzynki Gmail. Jeśli zdamy sobie sprawę, że poczta Google'a ma prawie pół miliarda aktywnych użytkowników[3], to dotrze do nas, iż ten internetowy gigant ma dostęp do informacji na temat znacznej części ludzkości jedynie za pomocą usługi pocztowej.

Nie chronimy swoich danych

Nieświadomość użytkowników przejawia się też wyjątkowo niefrasobliwym dzieleniem się informacjami na temat rodziny i znajomych. Po dekadzie funkcjonowania Facebooka i kilku latach obecności na rynku serwisów

[2] J. Battelle, *Szukaj. Jak Google i konkurencja wywołali biznesową i kulturową rewolucję*, Warszawa 2006, s. 151.

[3] 425 milionów to ostatnia znana wartość (stan na czerwiec 2012 r.).

społecznościowych, takich jak Twitter czy Instagram, można podać wiele przykładów osób, które nie doceniły potęgi Web 2.0. Lista przewinień jest imponująco długa: poczynając od nieostrożnych pracowników zamieszczających zdjęcia z alkoholowych libacji, przez nastolatki publikujące swoje nowe karty kredytowe, po kompromitujące wpadki agentów służb wywiadowczych. Wydaje się, że ignorancja w sferze ochrony własnej i cudzej prywatności nie omija ani osób prywatnych, ani firm. Oto kilka przykładów zaczerpniętych z publikacji pt. *Efekt Facebooka*:

> Pewien kanadyjski polityk [...] musiał wycofać się z wyborów, kiedy jedna z lokalnych gazet opublikowała znalezione na Facebooku zdjęcie, na którym było widać dwie osoby przymierzające jego bieliznę. Autor przemówień Baracka Obamy Jon Favreau został publicznie upokorzony, kiedy na pewnym blogu ukazało się zdjęcie przedstawiające go stojącego podczas przyjęcia obok wyciętej z kartonu sylwetki Hillary Clinton i trzymającego ręce na jej piersiach. Zostało ono umieszczone na Facebooku przez jego znajomego[4].

W Internecie bez trudu można znaleźć opisy podobnych sytuacji, niekiedy zabawnych, ale zwykle kończących się niepomyślnie dla bohaterów. Obecnie najbardziej widocznym problemem wydaje się publikowanie zdjęć, które nie powinny ujrzeć światła dziennego. Często są one niepodważalnym dowodem na łamanie prawa. Sytuacja mogłaby ulec poprawie, gdyby doszło do zmian w polityce działania serwisów, w których umieszczane są takie fotografie. Niestety portale społecznościowe nie wydają się zainteresowane działaniem na rzecz ochrony poufności danych swoich użytkowników – ich polityka prywatności świadczy o czymś całkiem innym. Najlepszym przykładem jest Facebook, który odmawia zmian w sposobie umieszczania znaczników[5], a nawet działa otwarcie na niekorzyść użytkowników poprzez odgórnie narzucane zasady prywatności.

Kompromitacja w Sieci może mieć poważne konsekwencje, ale równie dużym zagrożeniem wydaje się łatwość, z jaką sami udostępniamy na profilach informacje, które nie powinny być znane większej liczbie osób. Szczególnym przykładem tego zjawiska, obecnego głównie na mikroblogu Twitter, jest umieszczanie wpisów ze zdjęciami nowo nabytych kart płatniczych. W ten sposób miliony osób zyskują dostęp do takich danych, jak numer karty, imię i nazwisko posiadacza oraz data ważności, które w wielu

---

[4] D. Kirkpatrick, *Efekt Facebooka*, Warszawa 2011, s. 205.

[5] Obecnie użytkownicy mogą usunąć swój znacznik ze zdjęcia, ale często jest już za późno; serwis mógłby wprowadzić sposób zatwierdzania znaczników przez zainteresowanych przed publikacją wpisu.

transakcjach internetowych są niezbędne do realizacji płatności. Zdarzają się osoby jeszcze mniej rozsądne, zamieszczające nawet kod zabezpieczający wydrukowany na odwrocie dokumentu.

Źródło: https://twitter.com/NeedADebitCard [15.04.2014].

Ciekawy jest rozdźwięk między ostrożnością w życiu realnym a niefrasobliwością przejawianą w rzeczywistości wirtualnej. Tymczasem w momencie zagubienia lub kradzieży karty płatniczej jej zastrzeżenie jest jedną z pierwszych czynności, jakie należy wykonać. Zamieszczenie jej zdjęcia jest dalece bardziej niebezpieczne, gdyż poufne dane docierają do nieporównywalnie większej liczby osób, które mogą je wykorzystać. Publikowanie wizerunków kart płatniczych jest na tyle rozpowszechnione, że powstał profil @NeedADebitCard, którego właściciel „kolekcjonuje" *tweety* o takiej tematyce. Nie jest to jedyny sposób odnalezienia nieroztropnych internautów, często wpisy oznaczane są hashtagami #debit i #card, co stanowi niemal zaproszenie dla potencjalnego złodzieja. Najczęściej autorami tego typu postów są nastolatkowie, choć z wiekiem nie następuje niestety znaczący wzrost świadomości.

Oprócz tak skrajnie nieroztropnych działań można znaleźć wiele przykładów mniej oczywistych aktywności, którymi ułatwiamy okradzenie czy oszukanie nas. Świat realny i wirtualny przenikają się dziś do tego stopnia,

że z cyfrowej odsłony naszego życia korzystają nie tylko hakerzy i złodzieje danych. Wiele osób nie uświadamia sobie tego, że informując na bieżąco znajomych o wydarzeniach ze swego życia, ujawnia jednocześnie swój stan majątkowy, harmonogram dnia czy czas pobytu w domu osobom, wśród których mogą znajdować się potencjalni złodzieje. Za dowód może służyć doniesienie z 2010 r. o serii włamań z kradzieżami:

> Złodzieje, dzięki wpisom na Facebooku, wiedzieli, które domy są puste. Oszczędziło im to śledzenia posesji. Wystarczyło śledzenie aktualizacji statusów mieszkańców miasteczka. W ten sposób ci sami sprawcy dokonali 50 włamań z kradzieżą. Niektóre z ofiar tych kradzieży umieściły na Facebooku publiczną wiadomość z informacją, że nie będzie ich w domu w określonym czasie[6].

Jak donosi dalej serwis informacyjny, ofiary zostały pouczone, aby nie umieszczać lekkomyślnie tego typu wpisów, ale bez szeroko zakrojonej kampanii edukacyjnej takie sytuacje nadal będą miały miejsce.

Ostatni z grzechów popełnianych przez użytkowników Internetu to ignorancja w kwestii zabezpieczania dostępu do danych hasłami. Za sprawą wycieków danych znamy dziś najczęściej stosowane hasła. Zestawienie obejmujące pierwszą dziesiątkę pochodzące z ubiegłego roku prezentuje się następująco (od najbardziej popularnego): „123456", „password", „12345678", „qwerty", „abc123", „123456789", „111111", „1234567", „iloveyou" oraz debiutant „adobe123"[7]. Wydaje się niewyobrażalne, że w czasach, gdy na kontach mailowych czy wirtualnych dyskach przechowujemy tak wiele tak ważnych informacji, społeczeństwo nadal wykazuje się tak dalece posuniętą nieodpowiedzialnością. A problem słabych haseł jest znany i nagłaśniany od lat, przede wszystkim ze względu na oczywistość zagrożenia, ale także na łatwość, z jaką można zapobiec ewentualnym problemom. Informacje dotyczące stosowania skutecznych haseł od dawna znajdują się na listach porad dla początkujących użytkowników Sieci, a mimo to nie widać na tym polu znaczących zmian. Skalę problemu pokazuje obraz pochodzący ze shackowanej strony Kancelarii Prezesa Rady Ministrów.

A skuteczne hasło to nie tylko takie, które trudno złamać. Musi być również unikalne, stosowane tylko w jednym miejscu, do zabezpieczenia tylko jednego profilu, o czym również zapominają użytkownicy Sieci. Nawet

---

[6] http://www.bycseniorem.pl/Uwazajmy_na_co__co_piszemy_na_portalach_spolecznosciowych._Zlodzieje_wykorzystuja_Facebooka_34_n830 [21.04.2014].

[7] http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2014/04/oto-najgorsze-%28i-najczesciej-uzywane%29-hasla-2013-roku.aspx [22.04.2014].

Źródło: http://gadzetomania.pl/543,lata-mijaja-a-internauci-wciaz-nie-mysla-najgorsze-haslo-2013-roku-to [17.04.2014].

jeśli zastosujemy hasło długie, zawierające znaki specjalne i wielkie litery, nie możemy czuć się bezpieczni, jeśli używamy go do logowania się na kilka czy kilkanaście innych kont, a niestety takie postpowanie należy do powszechnych. Mimo zarzutów, jakie pojawiają się wobec internetowych gigantów, należy im przyznać, że zapewniają użytkownikom wysoki poziom zabezpieczeń, tylko nie każdy chce z tej możliwości skorzystać. Google oferuje uwierzytelnianie dwuczynnikowe[8], a także kontroluje logowania z podejrzanych adresów IP (np. z drugiej części półkuli), jednak skorzystanie z tych mechanizmów wymaga więcej czasu na logowanie się do usług, co sprawia, że cieszą się one powodzeniem nielicznych. Choć dobre zabezpieczanie internetowych profili może nie być postrzegane jako mające bezpośredni wpływ na ochronę naszej prywatności, to w czasach wycieków i kradzieży danych jest to jeden z elementów, które musimy mieć na uwadze.

Kluczowym elementem ochrony prywatności internautów jest więc ich świadome działanie oraz posiadanie chociaż minimalnej wiedzy na temat drogi, jaką przechodzą zamieszczane informacje, rąk, przez które przechodzą, i procesów, jakie ich dotyczą. Tylko szeroko zakrojone kampanie edukacyjne i ustawiczne uświadamianie internautów mogą wpłynąć na zahamowanie procesów prowadzących do zaniku prywatności w Sieci.

[8] Proces zakładający dwa etapy weryfikacji osoby próbującej uzyskać dostęp.

Choć istnieje wiele aspektów, na które przeciętny użytkownik nie ma wpływu, powinniśmy skupić swoje siły na zjawiskach będących w naszym zasięgu.

Internetowi giganci

Oczywiście oprócz przewin internautów ogromną odpowiedzialność za zanik naszej prywatności ponoszą firmy internetowe. Istotna dla zrozumienia problemu jest świadomość wagi informacji we współczesnym świecie. Nie bez powodu posługujemy się terminem „społeczeństwo informacyjne" – obecnie bowiem niemal każdy aspekt życia oparty jest na przesyłaniu, przetwarzaniu i przechowywaniu informacji, co w konsekwencji prowadzi do wzrostu jej wartości. Mam tu na myśli wartość materialną, możliwą do przeliczenia na realny zysk. Z tej okazji na niemały zarobek mogą liczyć przedsiębiorcy i pomysłowi pasjonaci, którzy mimo początkowo dobrych intencji dorabiają się na obrocie naszymi danymi. Oczywiście nie mogą się po prostu zwrócić z prośbą do milionów ludzi o udostępnienie poufnych informacji na ich temat, więc znajdują inne sposoby na dotarcie do nich. Najczęściej odbywa się to na zasadzie nieodpłatnego udostępniania usług, które magazynują prywatne dane oraz zawierają reklamy będące źródłem zarobku. Obecnie największe zatargi z internautami mają Google i Facebook, zapewne głównie ze względu na skalę prowadzonej działalności.

Google Inc. rozpoczęło działalność 16 lat temu jako wyszukiwarka internetowa. Obecnie mimo oferowania wielu usług (wszystkie są bezpłatne) – od poczty, przez mapy, po mobilny system operacyjny – jego głównym źródłem dochodu są wpływy z reklam. Wiemy, jak w dzisiejszym natłoku informacji trudno dotrzeć do potencjalnego klienta, dlatego by zapewnić jak największą skuteczność przekazu reklamowego, należy go jak najbardziej spersonalizować. Do tego w dużej mierze służą informacje, jakie są uzyskiwane od użytkowników usług. Oprócz agregowania informacji o określonych grupach osób (które nierzadko sprzedawane są kolejnym podmiotom), Google stara się zbierać jak najwięcej możliwie szczegółowych informacji o każdym internaucie, by nakreślić jego profil. Dlatego też często regulaminy umożliwiają korzystanie z prywatnych danych. Sprawia to, że jesteśmy ustawicznie inwigilowani – na bieżąco śledzona jest nasza lokalizacja, czytana korespondencja, gromadzone są zapytania kierowane do wyszukiwarki. Zwykle spotyka się z przyzwoleniem zainteresowanych, gdyż magazynowanie danych wpływa znacząco na wygodę korzystania z Sieci – wystarczy wspomnieć o skuteczniejszym wyszukiwaniu czy auto-

matycznym wysyłaniu zdjęć do chmury. Nie ulega jednak wątpliwości, że na rzecz wygodniejszego i szybszego poruszania się po opartym na informacji świecie po kawałku oddajemy swoją prywatność. Opisany wcześniej problem braku poufności korespondencji osób korzystających z Gmaila (a także ich rozmówców korzystających z innych skrzynek) to tylko jeden przykład z bardzo długiej listy sygnowanej przez giganta z Mountain View. Co więcej, Google od dłuższego czasu nie ogranicza się tylko do serwisów działających w Sieci, obecnie dysponuje przeglądarką internetową, menedżerem plików graficznych, pakietem biurowym online, a nawet mobilnym systemem operacyjnym, mając dostęp do wszystkich przepływających przez nie danych. Przy wprowadzaniu co bardziej kontrowersyjnych rozwiązań lub poszerzaniu zakresu uprawnień pojawiają się głosy oburzenia ze strony internautów lub organizacji zajmujących się ochroną praw obywatela, ale zwykle realizowany jest ten sam scenariusz, który rzadko kiedy prowadzi do zmiany sytuacji na lepszą.

Prywatność czy wygoda?

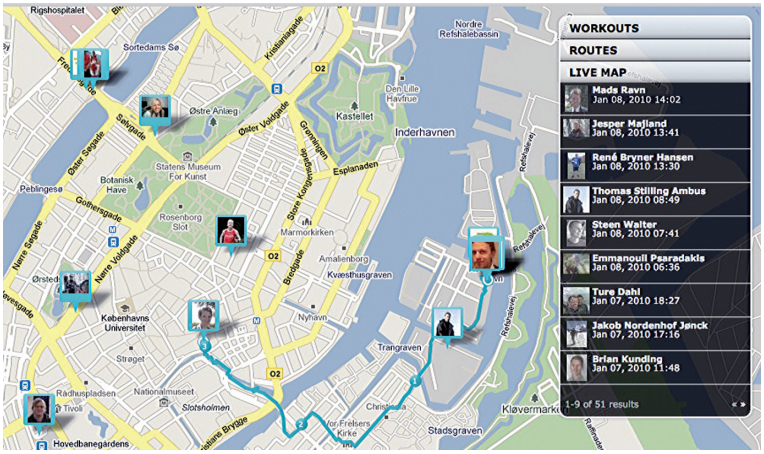
Istotny jest również aspekt „wymiany" prywatności na inne wartości, które stają się dla nas obecnie priorytetowe, jak chęć akceptacji, zdobycia popularności czy wygodniejszego życia. Wiele funkcji opierających się na gromadzeniu informacji służy nie tylko firmom oferującym usługi, ale znacząco wpływa na jakość korzystania z Sieci. Dobrym przykładem są „ciasteczka" (*cookies*), które cieszyły się ostatnio dużym zainteresowaniem użytkowników oraz mediów w związku z przepisami nakazującymi informować odwiedzających witryny www o ich wykorzystaniu. HTTP cookie to małe fragmenty tekstu krążące między przeglądarką a stroną internetową, dzięki którym – jak informuje serwis europa.eu:

> strona [...] może w ten sposób zapamiętać na dłużej czynności i preferencje internauty (takie jak nazwa użytkownika, język, rozmiar czcionki i inne opcje). Dzięki temu użytkownik nie musi wpisywać tych samych informacji za każdym razem, gdy powróci na tę stronę lub przejdzie z jednej strony na inną[9].

Każdy może więc zrezygnować z udostępniania pewnych informacji, ale przysparza sobie dodatkowej pracy przy przeglądaniu Sieci, toteż niewiele osób decyduje się na taki krok.

[9] http://europa.eu/cookies/index_pl.htm [24.06.2014].

Pokrewnym problemem jest rosnąca popularność aplikacji monitorujących najróżniejsze aspekty naszego życia, takich jak Endomondo czy Runtastic, które pozwalają śledzić naszą aktywność sportową, lub też Forsquare, które ułatwia spotkania ze znajomymi. Aplikacje typu *sports tracker* zasługują na wyjątkową uwagę z tego względu, że gromadzą wyjątkowo dużo szczegółowych informacji na nasz temat. Już w podstawowym zakresie zapis treningu zawiera dokładny przebieg trasy, typ aktywności, prędkość poruszania się, a także płeć i wiek użytkownika (te ostatnie informacje, wraz z wagą i wzrostem, często wpisujemy sami, by poprawić działanie programu), bardziej zaangażowani mogą wyposażyć się w pulsometr, co wzbogaci zapis o nasze tętno, liczbę spalonych kalorii itp. Już ten zestaw informacji mówi o nas dużo, a jeśli zdamy sobie sprawę, że dane te można agregować (wiele osób monitoruje aktywność przez miesiące i lata), to zobaczymy, że na podstawie danych z jednej tylko aplikacji można opracować kompletny obraz człowieka, wraz ze stanem jego zdrowia i sposobami spędzania wolnego czasu. A należy pamiętać, że informacje te mogą zostać przekazane do innych podmiotów, takich jak chociażby towarzystwa ubezpieczeniowe.



Źródło: http://mda.pl/gdzie-jestes/ [19.04.2014].

W tym kontekście warto również wspomnieć o zjawisku zyskującym obecnie na popularności, a określanym mianem „Internet rzeczy" lub „Internet przedmiotów". Jest to koncepcja, wedle której zastosowania Sieci rozszerzają się na przedmioty, które mogą gromadzić, przetwarzać i wymieniać dane za pośrednictwem Internetu. Już teraz można obserwować rozwój pierwszych rozwiązań tego typu: sprzęty gospodarstwa domowego, instala-

cje grzewcze czy oświetleniowe sterowane za pomocą smartfona i „uczące się" naszych potrzeb, aktywnie się do nich dostosowujące. A w planach są już „inteligentne" lodówki czy deski do krojenia, które policzą, ile kalorii ma przygotowany przez nas posiłek lub zamówią w sklepie internetowym potrzebne produkty. Wizja takiego życia, wspieranego wszędzie przez urządzenia elektroniczne zdolne do komunikacji ze sobą i z użytkownikiem jest zarówno ekscytująca, jak i przerażająca. Nasza codzienna egzystencja stałaby się jeszcze prostsza, ale uczynilibyśmy następny krok w kierunku pozbywania się prywatności i kontroli nad własnym życiem. Ogromna ilość danych, której obecnie nie jesteśmy w stanie zarejestrować i rozpowszechnić, będzie na bieżąco trafiała do międzynarodowych koncernów dostarczających nam dobra i usługi. Teraz o takim permanentnie inwigilowanym świecie dyskutujemy w kategoriach fikcji naukowej, ale kwestią dekady lub dwóch może być to, że większość z nas nie będzie już miała wyboru. Realizację tego typu scenariuszy można obserwować już teraz, jednak na mniejszą skalę – nie będąc zarejestrowanym na portalach społecznościowych, mamy bowiem utrudniony kontakt ze światem oraz dostęp do informacji.

Inwigilacja

Problemem, który nie powinien pojawiać się w wolnym, demokratycznym świecie, jest śledzenie obywateli przez rządy państw. Pod koniec 2014 r. świat obiegły sensacyjne doniesienia o bezprawnych działaniach amerykańskiej Agencji Bezpieczeństwa Krajowego, a także współpracujących z nią podmiotów, głównie korporacji internetowych. Dowiedzieliśmy się, że dzięki rządowemu programowi PRISM wywiad Stanów Zjednoczonych ma dostęp do danych przechowywanych na serwerach gigantów pokroju Microsoftu, Yahoo! czy Apple oraz możliwość ich gromadzenia, co oznacza, że USA śledzi użytkowników Internetu z całego świata, pomijając jedynie własnych obywateli[10]. Przeraża w tym wypadku nie tylko skala nadużyć, ale także fakt dobrowolnej współpracy firm, które do tej pory uważane były za neutralne i przestrzegające prawa. W dalszej kolejności zostały ujawnione podsłuchy wielu polityków europejskich, w tym przywódców czołowych państw UE. W obliczu tych wydarzeń rząd USA zyskał łatkę światowego „Wielkiego Brata", jednak przy okazji media przypomniały, że autorami takich działań są również władze europejskie, z Polską na czele.

[10] Według prawa przedmiotem działań wywiadu nie mogą być osoby przebywające na terenie kraju.

O ile w czasach poprzedniego ustroju podsłuchiwanie obywateli nastręczało trudności i wymagało ewidentnych działań, o tyle dziś jest to tak proste, że straciło swój negatywny wydźwięk. Obecnie odpowiednie organy muszą jedynie zwrócić się do operatorów komunikacyjnych, którzy mają obowiązek przechowywania danych przez 24 miesiące, z prośbą o udostępnienie odpowiednich informacji. Fundacja Panoptykon na podstawie danych z UKE informuje, że w 2011 r. instytucje publiczne skorzystały z tej możliwości ponad 1,85 miliona razy, a możemy być pewni, że liczba ta znacząco wzrosła[11]. W tym względzie, o ile nie nastąpią zmiany w prawie, jesteśmy zupełnie bezsilni. Tak jak w przypadku USA Patriot Act, nasi przedstawiciele w rządzie podejmują decyzje, które dają im pełne prawo do inwigilacji.

Oddolne próby ochrony prywatności

Na szczęście niezwykle szybki rozwój technologii i wzrost wiedzy na jej temat w społeczeństwie daje nam nowe sposoby ochrony prywatności – dobrymi przykładami są takie inicjatywy, jak sieć Tor i firma Silent Circle. Nazwa Tor to akronim słów *the onion router*, które informują o sposobie działania tej sieci komputerowej – wykorzystuje ona trasowanie cebulowe, będące wielowarstwowym szyfrowaniem przesyłanych komunikatów, dzięki czemu możliwe jest zapobieżenie analizie ruchu sieciowego, a tym samym zachowanie anonimowości przez użytkowników. Tor został zaprezentowany już dekadę temu, ale jego popularność gwałtownie wzrosła w ciągu ostatnich lat ze względu na zainteresowanie mediów (a ostatnio także władz amerykańskich) skupionych na działalności przestępczej, głównie na serwisie Silk Road. Obraz tego rozwiązania prezentowany przez media jest godny uwagi – zazwyczaj jest ono pokazywane jako siedlisko zła i występku, zaś pomijany jest jego pozytywny aspekt, czyli możliwość ochrony prywatności. Nie dziwi to, gdyż internauci są jedynymi, w których interesie to leży. Warto również podkreślić, że korzystanie z Tora wymaga pewnych poświęceń, gdyż jest to sieć pozbawiona pewnych rozwiązań oraz potrzebująca odpowiedniego oprogramowania. Obecnie ochrona prywatności w Sieci nie jest bowiem „standardem", ale wymaga pewnego wysiłku. Podobnie jest w przypadku usług dostarczanych przez firmę Silent Circle, która oferuje bezpieczną, szyfrowaną komunikację pomiędzy platformami. Aktualnie

[11] http://technowinki.onet.pl/aktualnosci/jak-bardzo-jestesmy-inwigilowani/7qghn [19.04.2014].

wśród jej produktów można znaleźć klienta poczty e-mail, kodowane wiadomości SMS, a także rozmowy głosowe i wideo, dostępne w wiodących systemach mobilnych i desktopowych. Ostatnio został również zaprezentowany smartfon, który domyślnie korzysta z powyższych rozwiązań. Nadal jednak jest to rozwiązanie płatne i niełatwe do wdrożenia na dużą skalę, co skutkuje niewielką popularnością.

Jedna tożsamość

O ile wszystkie powyższe problemy są ze sobą dość ściśle powiązane, o tyle występuje jeszcze jedno zjawisko, które jest coraz bardziej widoczne w Sieci i ma ogromny wpływ na zanik prywatności, a stanowi interesujący przedmiot badań dla socjologa – jest nim jedna tożsamość. Gdy funkcjonujemy w różnych kontekstach i różnych grupach osób, mamy dla każdej z nich przygotowaną inną twarz, maskę, jakby powiedział Erving Goffman. Przed rodziną czy pracownikami nie chcemy zwykle odsłaniać swojego oblicza przeznaczonego dla znajomych, z którymi organizujemy huczne imprezy. Ten sposób myślenia i funkcjonowania został przeniesiony do Sieci w początkowym okresie jej funkcjonowania. Najpierw ukrywaliśmy się za nickami, które pomagały maskować naszą tożsamość, następnie w erze pierwszych portali społecznościowych zaczęliśmy występować pod prawdziwym imieniem i nazwiskiem, lecz nadal mogliśmy kształtować naszą sieciową tożsamość, gdyż często były to serwisy specjalistyczne i zamiast materialnych atrybutów przedstawialiśmy odpowiedni zestaw informacji na swój temat (nie tylko w formie profilu, ale też np. komentarzy). Sytuacja zmieniła się diametralnie w ciągu ostatnich kilku lat. Przede wszystkim na scenę wkroczył Facebook, którego założeniem jest maksymalna transparentność. Jego twórca, Mark Zuckerberg, w rozmowach z dziennikarzami wielokrotnie podkreślał, że pragnie zbudować jedną tożsamość, do której różnych aspektów będą miały dostęp wszystkie osoby, jakie znamy. Coraz większy nacisk kładziony jest na ten element, co skutkuje m.in. tym, że bardzo trudna jest zmiana danych na pseudonim (zamiast prawdziwego imienia i nazwiska). Niektórzy próbują się przed tym bronić, zapraszając do znajomych jedynie rodzinę i bliskich lub manipulując ustawieniami prywatności. Jednak nie każdy potrafi sobie z tym poradzić, a pokusa dzielenia się ze światem naszymi przemyśleniami czy sukcesami jest tak silna, że mało kto decyduje się na taki krok. W tę samą stronę zmierza druga potęga Internetu – Google. Firma ta od lat z powodzeniem rozwija kolejne usługi,

z których korzystają setki milionów internautów. Do niedawna każdy z profili funkcjonował osobno, jako niezależny byt, w wielu (np. YouTube) do identyfikacji wystarczał nick. Czasy te skończyły się po utworzeniu portalu społecznościowego Google+, który jest sercem i łącznikiem profili w pozostałych usługach. Sprawiło to, że nasze aktywności z różnych obszarów zostały połączone i przyporządkowane do konkretnej osoby, możliwej do zidentyfikowania z imienia i nazwiska, a także wielu innych danych. Oczywiście wprowadzenie tak dużych zmian, mimo że następowało stopniowo, spotkało się z oburzeniem internautów, chyba największym na YouTube, gdzie do tej pory panowała duża swoboda. Ale na krytyce się skończyło. Mimo wielu deklaracji o usuwaniu profili Google nie zanotowało znaczącego odpływu użytkowników ze swoich usług. Zadziałał tu ten sam mechanizm, o którym wspomniałam w kontekście zmian w ustawieniach prywatności – mamy bowiem do czynienia ze swoistym oligopolem, gdzie najważniejsze usługi sieciowe są tworzone i nadzorowane przez kilka korporacji. Kiedy warunki przez nie proponowane stają się dla nas niekorzystne, stajemy wobec sytuacji, że po pierwsze włożyliśmy wiele pracy w stworzenie profilu, po drugie nie mamy wystarczająco dobrej alternatywy, co sprawia, że niewiele osób gotowych jest do zrezygnowania z usługi, która w znaczący sposób narusza prywatność.

Kolejnym krokiem na drodze połączenia wszystkich naszych wirtualnych tożsamości wydają się usługi typu Facebook Connect. Ich stosowanie prowadzi do tego, że danymi z portalu Facebook identyfikujemy się w wielu innych zakątkach Sieci, które do tej pory pozwalały na zachowanie pewnej anonimowości. Co więcej, robimy to z własnej woli i niezwykle chętnie, gdyż jest to rozwiązanie bardzo wygodne. Powoli jednak pozbywamy się prywatności na rzecz oszczędności czasu poświęconego na zarejestrowanie nowego profilu. Co gorsza, budujemy w ten sposób potęgę Facebooka na dwa sposoby. Przede wszystkim dajemy portalowi dostęp do kolejnych porcji danych, które obecnie są dla takich firm największą wartością. Dodatkowo budujemy swoje przywiązanie do serwisu, dzięki czemu jesteśmy mniej skłonni do rezygnacji z jego usług, kiedy warunki stają się mniej korzystne[12].

Podsumowanie

Oczywiście nie są to wszystkie problemy, z jakimi musi zmagać się obecnie człowiek funkcjonujący w społeczeństwie informacyjnym i sądzę, że

[12] Po usunięciu konta na FB, usuwane są wszystkie konta z nim powiązane.

katalog zagrożeń może się zwiększyć w najbliższej przyszłości ze względu na bardzo dynamiczny rozwój technologii. Starałam się skupić na najważniejszych w chwili obecnej problemach, które wydają mi się najbardziej palące i wymagające zmiany, ale jest jeszcze kilka kwestii, których nie poruszyłam, ważnych dla współczesnego użytkownika Internetu, jak chociażby wyszukiwanie behawioralne, przestępczość internetowa czy *wearables*. Spokojni nie mogą pozostać też ci, którzy unikają kontaktu z Siecią, bowiem postępująca cyfryzacja rzeczywistości oddziałuje na wszystkich (czego przykładem są choćby systemy państwowe związane z ewidencją danych czy służbą zdrowia).

Po przedstawieniu tych spostrzeżeń pozostaje postawić pytanie: Czy prywatność jest zjawiskiem historycznym? Jak pisałam we wstępie, prawo do prywatności, choć tak dziś ważne, jest dość nową ideą. Obserwując przemiany mentalności współczesnych społeczeństw, można dojść do wniosku, że następuje jej stopniowa dewaluacja na rzecz innych wartości, które mogą świadczyć o chęci powrotu do pierwotnych społeczności. Może wskutek retrybalizacji, o której pisał Marshall McLuhan, zrzeczemy się prawa do posiadania sfery życia niedostępnej dla znajomych i obcych? A może to jedynie kryzys, który prywatność przeżywa z powodu zachłyśnięcia się zdobyczami techniki i możliwościami Web 2.0? Niewątpliwie jest to zjawisko ciekawe i warte śledzenia przez badaczy społecznych. Pozostaje liczyć, że w najbliższych latach uda się osiągnąć *consensus* pozwalający komfortowo funkcjonować we współczesnym świecie na styku rzeczywistości realnej i wirtualnej.

Literatura

Battelle J., *Szukaj. Jak Google i konkurencja wywołali biznesową i kulturową rewolucję*, Warszawa 2006.

Brandt R.L., *Potęga Google'a. Poznaj sekrety Larry'ego i Sergeya*, Kraków 2011.

Castells, M., *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, Poznań 2003.

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

Gogłoza W., *Prawo do prywatności w społeczeństwie informacyjnym*, https://wgogloza.files.wordpress.com/2007/12/prywatnosc2.pdf [16.06.2015].

Kirkpatrick D., *Efekt Facebooka*, Warszawa 2011.

Moglen E., *Wolność w chmurze i inne eseje*, Warszawa 2013.

Orliński W., *Internet. Czas się bać*, Warszawa 2013.

Vincent G., *Historia życia prywatnego*, Wrocław 2006.

http://antyweb.pl/krol-jest-nagi-nowe-fakty-zwiazane-z-inwigilacja-w-sieci/# [29.03.2014].
http://en.wikipedia.org/wiki/Global_Internet_usage [16.04.2014].
http://en.wikipedia.org/wiki/Silent_Circle_%28software%29 [20.04.2014].
http://europa.eu/cookies/index_pl.htm [24.06.2014].
http://gadzetomania.pl/543,lata-mijaja-a-internauci-wciaz-nie-mysla-najgorsze-haslo-2013-roku-to [17.04.2014].
http://m.technologie.gazeta.pl/internet/1,113033,10522170,Facebook_przechowuje_usuniete_przez_uzytkownikow_dane_.html [13.04.2014].
http://pl.wikipedia.org/wiki/HTTP_cookie [24.06.2014].
http://pl.wikipedia.org/wiki/Tor_%28sie%C4%87_anonimowa%29 [20.04.2014].
http://tech.wp.pl/kat,1009785,title,Inwigilacja-w-sieci-jak-dzialaja-technologiczni-giganci,wid,16424601,wiadomosc.html?ticaid=112ffd [29.03.2014].
http://technowinki.onet.pl/aktualnosci/jak-bardzo-jestesmy-inwigilowani/7qghn [19.04.2014].
http://www.bycseniorem.pl/Uwazajmy_na_co__co_piszemy_na_portalach_spolecznosciowych._Zlodzieje_wykorzystuja_Facebooka_34_n830 [21.04.2014].
http://www.dobreprogramy.pl/Blackphone-pokazany-podczas-MWC-deklaracje-producenta-okazaly-sie-mocno-na-wyrost,News,52542.html [20.04.2014].
http://www.internetworldstats.com/stats.htm [13.04.2014].
http://www.polskieradio.pl/42/259/Artykul/940306,Ochrona-danych-osobowych-kontra-afera-PRISM-[19.04.2014].
http://zaufanatrzeciastrona.pl/post/najpopularniejsze-serwery-w-sieci-tor-wedlug-wyciekow-zapytan-dns/ [29.06.2014].
https://twitter.com/NeedADebitCard [15.04.2014].
http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2014/04/oto-najgorsze-(i-najczesciej-uzywane)-hasla-2013-roku.aspx [22.04.2014].