Skutki sprawy Edwarda Snowdena dla prywatności danych w cyberprzestrzeni

Michał Grzelak

Na początku czerwca 2013 r. doszło do jednego z najważniejszych wydarzeń związanych ze sprawami bezpieczeństwa cyberprzestrzeni i znajdujących się w niej informacji. Tematyka ta, bliska zainteresowanym grupom ekspertów i hobbystów, za sprawą ujawnienia przez byłego pracownika amerykańskiego wywiadu informacji dotyczących gromadzenia danych przez służby specjalne USA, zainteresowała szerokie grono opinii publicznej i wywołała globalną dyskusję poświęconą kwestiom prywatności w internecie. Spowodowała reakcje i konkretne działania zainteresowanych stron – państwowych władz, międzynarodowych korporacji, a także indywidualnych użytkowników internetu. Większa przejrzystość i ograniczenie gromadzenia danych, a także wzrost społecznej świadomości w zakresie cyberbezpieczeństwa to pozytywne zmiany, jednak zdaniem wielu, są one wciąż niewystarczające.

Afera Edwarda Snowdena[1]

W pierwszych dniach czerwca 2013 r. amerykańska gazeta „The Washington Post"[2] oraz brytyjski „The Guardian"[3] opisały działający od 2007 r. tajny program wywiadowczy PRISM, powołując się przy tym na dokumenty przekazane przez Edwarda Snowdena, byłego pracownika Centralnej Agencji Wywiadowczej (*Central Intelligence Agency*, CIA) oraz Agencji Bezpieczeństwa Narodowego (*National Security Agency*, NSA). Celem ujawnionego progamu było umożliwienie amerykańskim służbom specjalnym dostępu do danych znajdujących się na serwerach dostawców usług internetowych

[1] W tej części wykorzystano fragment artykułu *Szpiegostwo i inwigilacja w Internecie*, M. Grzelak, „Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji", Difin 2014 r.

[2] *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, The Washington Post, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (dostęp: 25 stycznia 2015 r.).

[3] *NSA Prism program taps in to user data of Apple, Google and others*, "The Guardian", 7 czerwca 2013 r., http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data (dostęp: 25 stycznia 2015 r.).

(Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube oraz Apple), w tym gromadzenia danych o użytkownikach przez te służby. Dzięki PRISM mają one dostęp m.in. do nagrań audio i wideo, zdjęć, rozmów, poczty elektronicznej i innych danych użytkowników korzystających z serwisów należących do wymienionych korporacji, które po ujawnieniu informacji dotyczących programu masowej inwigilacji zaprzeczyły współpracy ze służbami czy wiedzy na ten temat. W przypadku PRISM wykorzystano fakt, że większość danych w ramach światowej komunikacji elektronicznej przechodzi przez serwery należące do amerykańskich firm. Stany Zjednoczone nie zaprzeczyły istnieniu programu inwigilacji, choć wskazano na pewne nieścisłości zawarte w prasowych publikacjach. Doniesienia wywołały prawdziwą burzę i falę oskarżeń pod adresem USA, jednak amerykańskie władze broniły PRISM. Dyrektor amerykańskiego wywiadu James Clapper stwierdził, że program jest zgodny z obowiązującym prawem (choć późniejsze orzeczenie sądu zdaje się kwestionować zgodność wybranych środków wywiadowczych z amerykańską konstytucją[4]) i nie może być użyty do umyślnego monitorowania obywateli USA lub innych osób mieszkających na terenie Stanów Zjednoczonych. Działanie PRISM koncentruje się bowiem na obywatelach państw trzecich, a zbierane dane są wykorzystywane do ochrony Stanów Zjednoczonych przed największymi zagrożeniami, np. terroryzmem. PRISM bronił również prezydent USA Barack Obama[5], który podkreślił, że mimo klauzuli tajności, program jest „przejrzysty" i zgodny z amerykańskim prawem[6]. B. Obama zapewnił, że administracja poszukuje rozwiązania, które uspokoi opinię publiczną, a także udowodni, że rozmowy i korespondencja amerykańskich obywateli nie są inwigilowane przez „wielkiego brata". PRISM najmocniej bronił ówczesny szef NSA gen. Keith Alexander[7], którego zdaniem program pozwolił udaremnić co najmniej 50 „terrorystycznych spisków", dlatego ujawnienie informacji na jego temat stanowi olbrzymią, niemożliwą do naprawienia szkodę dla USA i ich sojuszników.

[4] *NSA phone surveillance program likely unconstitutional, federal judge rules*, "The Guardian", 16 grudnia 2013 r., http://www.theguardian.com/world/2013/dec/16/nsa-phone-surveillance-likely-unconstitutional-judge (dostęp: 11 maja 2014 r.).

[5] *Obama defends secret NSA surveillance programs - as it happened*, "The Guardian", 7 czerwca 2013 r., http://www.guardian.co.uk/world/2013/jun/07/obama-administration-nsa-prism-revelations-live (dostęp: 3 lipca 2013 r.).

[6] Foreign Intelligence Surveillance Act, https://www.fas.org/irp/agency/doj/fisa/ (dostęp: 3 lipca 2013 r.).

[7] *Column: NSA and the Pandora's box of surveillance*, "Reuters", 24 czerwca 2013 r., http://www.reuters.com/article/2013/06/24/us-shafer-nsa-idUSBRE95N1GQ20130624 (dostęp: 3 lipca 2013 r.).

Zapewnienia przedstawicieli władz Stanów Zjednoczonych pozwalają sądzić, że dane gromadzone w ramach programu PRISM są wykorzystywane wyłącznie w celu zapewnienia bezpieczeństwa amerykańskich obywateli. Atmosfera „tajności" oraz społeczne obawy dotyczące inwigilacji na globalną skalę sprawiły jednak, że ujawnienie informacji na temat PRISM zdarło maskę niewinności z państwa, które dotąd uchodziło za sprzyjające wolności i bezpieczeństwu użytkowników globalnej sieci.

Działalność inwigilacyjna prowadzona przez wywiad elektroniczny USA nie dotyczy wyłącznie „zwyczajnych" obywateli. Powołując się na ściśle tajne dokumenty z 2010 r., również ujawnione przez E. Snowdena, niemiecki tygodnik „Der Spiegel"[8] napisał, że amerykańska Agencja Bezpieczeństwa Narodowego podsłuchiwała rozmowy telefoniczne przedstawicieli Unii Europejskiej, pracujących w biurach w Waszyngtonie i Nowym Jorku. NSA miała także infiltrować sieci komputerowe w tych placówkach, uzyskując dostęp do wewnętrznych dokumentów oraz poczty elektronicznej unijnych dyplomatów. Zdaniem „Der Spiegel", NSA próbowała również podsłuchiwać rozmowy telefoniczne w siedzibie Rady Unii Europejskiej w Brukseli. Dziennikarskie doniesienia wywołały gwałtowną reakcję europejskich urzędników[9] oraz przywódców państw członkowskich Unii, którzy domagali się stosownych wyjaśnień od Stanów Zjednoczonych[10], a szef Komisji Europejskiej José Manuel Barroso nakazał doraźne kontrole zabezpieczeń przed inwigilacją w budynkach instytucji oraz jej systemie komunikacji[11]. Brytyjski dziennik „The Guardian" sprecyzował, że na liście ujawnionej przez E. Snowdena znajdowało się 38 „celów", w tym ambasad należących do najważniejszych sojuszników Stanów Zjednoczonych[12]. Poza państwami członkowskimi UE, lista obejmowała m.in. Japonię, Koreę Południową i Turcję. Praktyki stosowane przez NSA i „manię zbierania informacji" porównano

[8] *Attacks from America: NSA spied on European Union offices*, "Der Spiegel", 29 czerwca 2013 r., http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html (dostęp: 1 lipca 2013 r.).

[9] *Spying 'out of control': EU official questions trade negotiations*, "Der Spiegel", 30 czerwca 2013 r., http://www.spiegel.de/international/europe/eu-officials-furious-at-nsa-spying-in-brussels-and-germany-a-908614.html (dostęp: 1 lipca 2013 r.).

[10] *Europeans voice anger over reports of spying by U.S. on its Allies*, "The New York Times", 1 lipca 2013 r., http://www.nytimes.com/2013/07/01/world/europe/europeans-voice-anger-over-reports-of-spying-by-us-on-its-allies.html (dostęp: 2 lipca 2013 r.).

[11] *Barroso orders security sweep after allegations of US spying*, "The European Voice", 1 lipca 2013 r., http://www.europeanvoice.com/article/2013/july/barroso-orders-security-sweep-after-allegations-of-us-spying/77721.aspx (dostęp: 2 lipca 2013 r.).

[12] *New NSA leaks show how US is bugging its European allies*, "The Guardian", 30 czerwca 2013 r., http://www.guardian.co.uk/world/2013/jun/30/nsa-leaks-us-bugging-european-allies (dostęp: 1 lipca 2013 r.).

do metod wykorzystywanych w czasach zimnej wojny. Pojawiły się nawet opinie, że Unia Europejska powinna skierować tę sprawę do międzynarodowych instytucji, a także zawiesić negocjacje z USA w sprawie utworzenia euroatlantyckiej strefy wolnego handlu.

Medialne doniesienia próbował neutralizować amerykański sekretarz stanu John Kerry, którego zdaniem wszystkie państwa prowadzą „wiele działań" w celu ochrony swojego bezpieczeństwa narodowego, a pomagają im w tym wszelkiego rodzaju informacje. Europejskich sojuszników uspokajał prezydent USA B. Obama, który powiedział, że jego administracja ocenia treść artykułów prasowych cytujących dokumenty dostarczone przez E. Snowdena i zapewnił, że we właściwym czasie Stany Zjednoczone dostarczą sojusznikom odpowiedzi na pytania w sprawie elektronicznej inwigilacji[13].

Od chwili ujawnienia informacji przekazanych przez E. Snowdena co pewien czas ukazują się kolejne publikacje oraz komentarze poświęcone skali przedsięwzięć i metod działania służb specjalnych w zakresie inwigilacji użytkowników internetu. Nadużycia w tym zakresie – jak się okazało – nie są wyłącznie domeną amerykańskiego wywiadu, a jego europejscy partnerzy również wykazują duże zainteresowanie danymi użytkowników, znajdującymi się w internecie. Pod wpływem pojawiających się doniesień, nawet komisarz UE do spraw sprawiedliwości, praw podstawowych i obywatelstwa Viviane Reding wezwała niektóre europejskie państwa do wprowadzenia zmian w ustawodawstwie w zakresie ochrony prywatności swoich obywateli, zarzucając im jednocześnie, że negatywnie oceniając działania amerykańskich służb, same wykazują się hipokryzją[14].

E. Snowden, starając się uniknąć postawienia go przed wymiarem sprawiedliwości Stanów Zjednoczonych, znalazł azyl na terenie Rosji, skąd kontynuuje walkę w obronie prawa obywateli do prywatności oraz wolności słowa w internecie. Fakt, że zdecydował się schronić w Rosji, w państwie, które zdaje się nie do końca podzielać ideały przyświecające amerykańskiemu demaskatorowi, oraz odmawia powrotu do USA, gdzie czeka go proces za ujawnienie ściśle tajnych materiałów[15], stanowi argument dla osób podważających czystość jego intencji. Ich zdaniem, gdyby demaskatorowi

[13] *U.S. seeks to calm European outrage over alleged spying*, "Reuters", 1 lipca 2013 r., http://www.reuters.com/article/2013/07/01/us-usa-eu-spying-idUSBRE95T09C20130701 (dostęp: 2 lipca 2013 r.).

[14] *EU justice chief attacks European "hypocrisy" on spying*, "Reuters", 28 stycznia 2014 r., http://www.reuters.com/article/2014/01/28/us-usa-security-eu-idUSBREA0R1JH20140128?feedType=RSS&feedName=topNews&utm_source=dlvr.it&utm_medium=twitter&dlvrit=992637 (dostęp: 30 stycznia 2014 r.).

[15] *White House: No amnesty for Snowden*, "USA Today", 16 grudnia 2013 r., http://www.usatoday.com/story/theoval/2013/12/16/obama-snowden-nsa-nsc-caitlin-hayden/4038753/ (dostęp: 11 maja 2014 r.).

faktycznie zależało na ograniczeniu masowej inwigilacji, zwróciłby się bezpośrednio do instytucji nadzorujących działalność służb specjalnych, a nie wywoływał międzynarodowy skandal godzący w dobre imię i bezpieczeństwo USA.

W sierpniu 2014 r. E. Snowden otrzymał trzyletnie pozwolenie na pobyt w Rosji[16], jednak władze Stanów Zjednoczonych niezmiennie oczekują jego powrotu do kraju, gdzie miałby zostać zatrzymany i osądzony. W grudniu 2014 r. niemiecka opozycja chciała, aby E. Snowden mógł przyjechać do Niemiec i osobiście zeznawać przed parlamentarną komisją badającą działania wywiadowcze Stanów Zjednoczonych, jednak wniosek w tej sprawie został odrzucony przez sąd. Pojawiały się opinie, że obecność E. Snowdena mogłaby pogorszyć relacje z USA oraz spowodować naciski dotyczące jego ekstradycji. W Niemczech panuje duże poparcie dla sprawy E. Snowdena, szczególnie, że zgodnie z ujawnionymi przez niego informacjami USA miały szpiegować m.in. kanclerz Angelę Merkel. Jak jednak wynika z przekazanych przez niemiecką prokuraturę informacji, nie udało się znaleźć dowodów, które potwierdzałyby te doniesienia, a prezentowane wcześniej przez prasę materiały nie były autentyczne[17].

Mimo wszelkich negatywnych skutków skandalu wywołanego przez E. Snowdena, należy przyznać, że spowodował one również pozytywne efekty. Pojawiające się kolejno doniesienia mówiące o powszechnym, masowym gromadzeniu prywatnych danych należących do zwykłych obywateli, uświadomiły użytkownikom globalnej sieci, jak bardzo dotyczą ich sprawy cyberbezpieczeństwa, dla wielu będącego dotąd abstrakcyjnym pojęciem. Po raz pierwszy bowiem jeden temat z zakresu cyberbezpieczeństwa – w pewnym stopniu – dotyczy niemal każdego użytkownika internetu i stał się przedmiotem uwagi międzynarodowej opinii publicznej, przez wiele tygodni, a nawet miesięcy znajdując się w czołówce nagłówków serwisów informacyjnych. Wpływ globalnej dyskusji okazał się wyjątkowo silny. Spowodował faktyczne zmiany w sposobie pracy amerykańskich służb, a także przełożył się na działania międzynarodowych korporacji zamieszanych w proceder cyfrowej inwigilacji. Należy zaznaczyć, że skala skutków i zmian w zakresie prywatności w cyberprzestrzeni jest ogromna, a omówione w artykule przykłady opisują tylko wycinek prac organizacyjnych

[16] *Russia gives Snowden 3-year residency*, "CNN", 7 sierpnia 2014 r., http://edition.cnn.com/2014/08/07/world/europe/russia-snowden-residency/ (dostęp: 25 stycznia 2015 r.).

[17] *Court rejects attempt to allow Edward Snowden into Germany*, "The Guardian", 12 grudnia 2014 r., http://www.theguardian.com/us-news/2014/dec/12/court-edward-snowden-germany-nsa (dostęp: 25 stycznia 2015 r.).

i legislacyjnych, prowadzonych przez wiele zainteresowanych podmiotów, instytucji międzynarodowych, władz państwowych czy korporacji.

Wpływ afery na działania władz

Zapowiadana stanowcza reakcja władz Stanów Zjednoczonych nastąpiła po ponad pół roku od pierwszych publikacji prasowych w sprawie działań NSA. W styczniu 2014 r. prezydent USA B. Obama zapowiedział początek reformy programów, których zadaniem jest zdobywanie informacji środkami wywiadu elektronicznego[18]. B. Obama podkreślił, że dostępne ogromne ilości danych służą identyfikacji konkretnych zagrożeń. Zaznaczył przy tym, że zaufanie amerykańskich obywateli i międzynarodowej społeczności jest istotne dla efektywności tych programów i zdolności władz do zapewnienia bezpieczeństwa. Dlatego zdecydował, że zasady gromadzenia metadanych rozmów telefonicznych (czas, miejsce, numery telefonów itp.) będą zmienione. Zgodnie z rekomendacjami, dane dotyczące połączeń będą przechowywane np. przez operatorów, a nie przez służby. Dostęp do nich zostanie ograniczony i będzie wymagał nakazu specjalnego sądu (U.S. Foreign Intelligence Surveillance Court, FISA Court). Wśród propozycji znalazły się także zmiany dotyczące innych programów, co ma zapewnić lepszą ochronę prywatności obcokrajowców, a prezydent B. Obama zapowiedział, że jeśli nie będzie ku temu nadzwyczajnych okoliczności dotyczących bezpieczeństwa kraju, Stany Zjednoczone nie będą monitorować komunikacji szefów państw i rządów amerykańskich sojuszników.

Propozycje B. Obamy spotkały się z różną oceną. Komisja Europejska przyjęła je z zadowoleniem, doceniając umiejętność dialogu i zrozumienia argumentów europejskich partnerów w zakresie zbierania danych na potrzeby wywiadu elektronicznego. Podkreślono jednocześnie, że istnieją sprawy wymagające dalszych prac i uszczegółowienia[19]. Tymczasem w opinii organizacji Human Rights Watch, zaproponowane zmiany są niewystarczające, m.in. w zakresie prawa obywateli państw trzecich do pełnej prywatności i ochrony elektronicznych środków komunikacji przed inwigilacją

[18] *Obama bans spying on leaders of U.S. allies, scales back NSA program*, "Reuters", 17 stycznia 2014 r., http://www.reuters.com/article/2014/01/17/us-usa-security-obama-idUSBREA0G0JI20140117 (dostęp: 30 stycznia 2014 r.).

[19] *Statement by European Commission Spokeswoman on U.S. President Obama's remarks on the review of U.S. intelligence programmes*, European Commission, Press Release Database 17 stycznia 2014 r., http://europa.eu/rapid/press-release_MEMO-14-30_en.htm (dostęp: 30 stycznia 2014 r.).

przez amerykańskie służby specjalne. Argumentem za takim rozwiązaniem ma być brak dowodów świadczących o tym, że masowe zbieranie danych faktycznie wpływa na poprawę bezpieczeństwa[20].

Fakt, że planowane rozwiązania dotyczą tylko części dyskutowanych problemów sugeruje, że głównym celem przedstawionych propozycji nie była głęboka reforma NSA i ograniczenie kompetencji służb, ale choć częściowe uspokojenie społecznej krytyki. Zaproponowane zmiany okazały się nieprecyzyjne oraz pozostawiają dużo miejsca do swobodnej interpretacji, zgodnej z „interesem bezpieczeństwa narodowego USA". Trudno uwierzyć, aby amerykańskie służby zaprzestały kontrowersyjnych praktyk inwigilacyjnych. Bardziej prawdopodobne są raczej działania mające na celu zawężenie kręgu osób dysponujących dostępem do tajnych informacji na temat prowadzonych programów i zebranych informacji, aby lepiej zabezpieczyć się przed ewentualnymi wyciekami, tak jak miało to miejsce w przypadku E. Snowdena.

Wprowadzanie skutecznych zmian legislacyjnych to trudne zadanie, ponieważ rozwój technologiczny jest tak dynamiczny, że nowo przyjęte prawo szybko staje się nieaktualne lub okazuje się zbyt szczegółowe i można je obejść, stosując udoskonalone rozwiązania techniczne. Przykładem jest przyjęte przez Unię Europejską „prawo do bycia zapomnianym", zgodnie z którym obywatele UE mogą zażądać od Google usunięcia z wyników wyszukiwania linków do stron zawierających informacje na ich temat. Google szybko dostosował się do regulacji, ale niechciane linki ukrywa tylko w wynikach wyszukiwania w obrębie domen państw należących do UE (google.pl, google.fr, google.de itd.). Użytkownik korzystający z wyszukiwarki w domenie google.com zobaczy niezmodyfikowane wyniki, dlatego Unia rozważa rozszerzenie przyjętych wcześniej regulacji. Google już teraz wskazuje na potencjalne problemy z wcieleniem ich w życie, bowiem nie można oczekiwać, że firma będzie ingerowała w wyniki wyszukiwania użytkowników na terenie państw, w których nie obowiązuje unijne prawo. Rozwiązaniem tego problemu może być uzależnianie wyników od fizycznej lokalizacji użytkownika (określanej np. na podstawie adresu IP, ale stosunkowo łatwo obejść taką formę kontroli) lub ograniczenie dostępu Europejczyków do wyszukiwarek o globalnym zasięgu. Prawo do zapomnienia jest wyrazem dyskusji, jaka toczy się na forum UE na temat prywatności w cyberprzestrzeni. Innym przykładem są działania Parlamentu Europejskiego,

[20] *Human Rights Watch says Obama not gone far enough on NSA reforms*, "Reuters", 21 stycznia 2014 r., http://www.reuters.com/article/2014/01/21/us-usa-security-rights-idUSBREA0K0BA20140121 (dostęp: 30 stycznia 2014 r.).

który wymógł na dostawcach sieciowych usług (głównie tych pochodzących z USA) lepszą ochronę danych należących do Europejczyków, co miało osłabić zdolności amerykańskich służb do masowej inwigilacji obywateli UE. Także w tym przypadku od początku wskazywano, że liczne wyjątki (np. dane użytkowników muszą być przechowywane na terenie UE, ale mogą być przetwarzane poza Unią) ograniczą skuteczność tych przepisów[21].

Największym wyzwaniem, przed jakim stoją obecnie instytucje Unii Europejskiej w obszarze ochrony prywatności swoich obywateli są prowadzone od kilku lat prace nad zmianą unijnych przepisów o ochronie danych osobowych. Niestety, na co wskazują monitorujące proces legislacyjny organizacje pozarządowe, na kolejnych jego etapach znacząco zmieniły się założenia projektu, stąd obawa, że standardy ochrony danych osobowych mogą ulec obniżeniu[22].

Pojawiające się po aferze E. Snowdena informacje medialne pozwalały sądzić, że masowa inwigilacja w internecie choć w niewielkim stopniu zostanie ograniczona lub poddana skuteczniejszemu nadzorowi. Jednak na początku stycznia 2015 r. doszło do wydarzeń, po których można się spodziewać kolejnej zmiany w podejściu do gromadzenia i analizy przez służby specjalne danych przesyłanych za pośrednictwem internetu. Po ataku terrorystycznym na siedzibę francuskiego tygodnika „Charlie Hebdo" doszło do spotkania ministrów spraw wewnętrznych państw UE, po którym podkreślono m.in. potrzebę współpracy służb z dostawcami internetu w celu identyfikacji i usuwania treści nawołujących do nienawiści i terroru[23]. Szczegóły działań w tym zakresie zostaną zapewne nakreślone w najbliższym czasie, można jednak spodziewać się, że jednym z warunków skuteczności nowych rozwiązań będzie ciągła analiza treści publikowanych w internecie. Jest też raczej pewne, że po usunięciu niepożądanych materiałów, ich autor nie uniknie zainteresowania służb walczących z terroryzmem. Także wypowiadający się po wydarzeniach we Francji szef brytyjskiego kontrwywiadu MI5 Andrew Parker podkreślał, że służby powinny mieć możliwość kontroli internetowych kanałów komunikacji, które dla terrorystów są nie tylko środkiem szerzenia radykalnej propagandy, ale też bieżącej komunikacji, gromadzenia

[21] *European Parliament votes on the data protection reform and the report on mass surveillance*, "EDRi", 12 marca 2014 r., https://edri.org/european-parliament-votes-data-protection-reform-report-mass-surveillance/ (dostęp: 25 stycznia 2015 r.).

[22] *Popsuta reforma ochrony danych*, Fundacja Panoptykon, 4 marca 2015 r., http://panoptykon.org/wiadomosc/popsuta-reforma-ochrony-danych (dostęp: 9 marca 2015 r.).

[23] *Internet and border monitoring needed to thwart further attacks*, "Daily Mail", 11 stycznia 2015 r., http://www.dailymail.co.uk/wires/afp/article-2905691/Internet-border-monitoring-needed-thwart-attacks.html (dostęp: 12 stycznia 2015 r.).

środków finansowych, a także przygotowań i planowania ataków[24]. Podobnego zdania jest premier Wielkiej Brytanii, Dawid Cameron, który opowiedział się za zmianami w prawie, które uniemożliwią terrorystom komunikowanie się w cyberprzestrzeni. Aby tak się stało, zdaniem brytyjskiego premiera, służby specjalne powinny mieć uprawnienia pozwalające na dostęp do wszystkich wiadomości, jakie wysyłane są przez internet. Obecnie na przeszkodzie służbom stoją pewne kanały komunikacji – aplikacje i usługi – które uniemożliwiają przechwytywanie oraz bieżącą analizę treści prywatnych wiadomości (szyfrowanie) lub szybko usuwają przesłane treści, uniemożliwiając dotarcie do archiwalnych wiadomości. Takie podejście spotkało się z szybką reakcją użytkowników internetu, którzy obawiają się np. delegalizacji niektórych kanałów komunikacji internetowej[25]. Mimo że cel przyświecający propozycji ministrów jest jasny i powinien być zrozumiały dla społeczeństwa, europejskie władze muszą przygotować konkretne propozycje działań z dużą uwagą, ostrożnością i przejrzystością, aby nie wzbudzały wątpliwości w obszarze prywatności zwykłych obywateli. Tym bardziej, że oprócz kontroli internetowych treści wśród propozycji zmian znajduje się także utworzenie systemu pozwalającego na wymianę danych o europejskich pasażerach lotniczych.

Istotne jest pytanie, czy ujawnienie metod stosowanych przez służby specjalne w ramach wywiadu elektronicznego wpłynęło na bezpieczeństwo narodowe? Informacje przekazane przez E. Snowdena zwiększyły świadomość nie tylko zwykłych użytkowników, ale też przestępców i terrorystów, pomagając im lepiej chronić się przed działaniami służb. Pojawiły się sygnały, że działania E. Snowdena pozwoliły terrorystom poznać narzędzia i zakres działań inwigilacyjnych, co faktycznie wpłynęło na zmianę ich sposobów komunikacji. Bezpośrednim tego skutkiem było ograniczenie możliwości służb w zakresie gromadzenia informacji wywiadowczych, a pośrednim śmierć ludzi – ofiar działań terrorystów, których nie udało się powstrzymać[26]. Zmiana sieciowych zachowań dotyczy nie tylko terrorystów, ale też zwykłych przestępców, którzy po opublikowaniu informacji dostarczonych

[24] *Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI) at Thames House*, MI5, 8 stycznia 2015 r., https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html (dostęp: 12 stycznia 2015 r.).

[25] *Spies should be able to monitor all online messaging, says David Cameron*, "The Telegraph", 12 stycznia 2015 r., http://www.telegraph.co.uk/technology/internet-security/11340621/Spies-should-be-able-to-monitor-all-online-messaging-says-David-Cameron.html (dostęp: 16 stycznia 2015 r.).

[26] *Snowden leaks cost lives, say terror experts: Extremists 'changed their tactics after fugitive's leaks about intelligence operations*', "Daily Mail", 25 listopada 2014 r., http://www.dailymail.co.uk/news/article-2849605/Snowden-leaks-cost-lives-say-terror-experts-Extremists-changed-tactics-fugitives-leaks-intelligence-operations.html (dostęp: 25 stycznia 2015 r.).

przez E. Snowdena zaczęli używać bezpieczniejszych kanałów komunikacji, co pozwoliło im zniknąć z pola widzenia służb. Wymusiło to konieczność rozwoju nowych technik i narzędzi służących monitorowaniu internetu[27].

Działania korporacji zaangażowanych w masową inwigilację

Interesująco prezentują się działania podjęte przez wielkie koncerny informatyczne, które sprawa E. Snowdena połączyła z inwigilacyjnymi działaniami prowadzonymi przez amerykański wywiad elektroniczny. Choć zgodnie z prasowymi doniesieniami, korporacje miały być nieświadome charakteru swojego uczestnictwa w procederze gromadzenia danych użytkowników i ich wykorzystywania do celów wywiadowczych, to globalne poruszenie z pewnością wpłynęła na wizerunek i zaufanie klientów firm będących „na usługach Wielkiego Brata". W myśl zasady „dobre złego skutki", czas kryzysu został jednak zręcznie wykorzystany do umocnienia rynkowej pozycji internetowych gigantów, a nawet prób przejęcia klientów korzystających z usług konkurencji. Sprawne działania wizerunkowe oraz szybka reakcja na zmianę potrzeb użytkowników pozwoliły firmom odciąć się od wątpliwych etycznie działań amerykańskich służb wywiadowczych. Tak więc firmy, którym wcześniej zarzucano masowe gromadzenie informacji na temat odbiorców swoich produktów, stanęły na froncie walki o prawo do prywatności po stronie obrońców obywateli inwigilowanych przez władze. Jeszcze w sierpniu 2013 r. w Białym Domu odbyły się, poświęcone ochronie prywatności, spotkania prezydenta B. Obamy z przedstawicielami firm zajmujących się nowoczesnymi technologiami[28]. W grudniu 2013 r. największe firmy sektora IT (m.in. AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter oraz Yahoo!) wystosowały do prezydenta Stanów Zjednoczonych list, w którym wezwały do ściślejszej kontroli inwigilacyjnych działań służb specjalnych i dostępu władz do prywatnych danych. W ich przekonaniu, obowiązujące zasady naruszają prawa obywateli zawarte w amerykańskiej konstytucji i podważają zaufanie użytkowników-klientów korporacji. Dlatego, zdaniem

[27] *Revealed: How British spies have lost track of our most dangerous criminals after Snowden revealed GCHQ's tactics*, "Daily Mail", 22 grudnia 2014 r., http://www.dailymail.co.uk/news/article-2883088/How-British-spies-lost-track-dangerous-criminals-Snowden-revealed-GCHQ-s-tactics.html (dostęp: 25 stycznia 2015 r.).

[28] *Microsoft, Google, Yahoo! talk privacy with President Obama*, "Social Times", 12 sierpnia 2013 r., http://socialtimes.com/microsoft-google-yahoo-talk-privacy-with-president-obama_b134107 (dostęp: 28 stycznia 2014 r.).

sygnatariuszy, amerykańskie władze powinny wykorzystać nadarzającą się okazję i zreformować funkcjonujący system[29]. Wiceprezes Microsoft, Brad Smith przekonywał pod koniec stycznia 2014 r., że jest to właściwy czas na szeroką dyskusję poświęconą inwigilacji oraz przyjęcie międzynarodowej konwencji regulującej dostęp władz państwowych do danych użytkowników. Jego zdaniem, prywatność jest elementem zbioru praw człowieka, nie może być jednak traktowana w sposób skrajny, uniemożliwiający władzom np. walkę z terroryzmem[30]. Kilka miesięcy później sprzeciwiał się władzom USA, które wymagały od Microsoftu dostępu do treści prywatnych wiadomości email znajdujących się na serwerach w Irlandii (aby lepiej chronić prywatność swoich zagranicznych klientów, Microsoft zdecydował się przenieść ich dane na serwery poza terytorium Stanów Zjednoczonych. Miało to pomóc w odbudowie zaufania klientów do jakości i bezpieczeństwa produktów firmy[31]). Argumentował przy tym, że poufność danych przechowywanych w cyberprzestrzeni powinna podlegać takiej samej ochronie prawnej jak ochrona informacji zapisanych np. na papierze czy przesyłanych tradycyjnymi kanałami komunikacji[32].

Yahoo! – w odpowiedzi na inwigilacyjne nadużycia władz – zdecydowało o wprowadzeniu kryptograficznych rozwiązań, dzięki którym dane użytkowników pozostaną niedostępne dla służb (lub przynajmniej utrudnią ich przeglądanie na masową skalę)[33]. Ponadto szefowa koncernu Marissa Mayer wezwała prezydenta B. Obamę do większej przejrzystości zasad, na jakich NSA zbiera informacje o użytkownikach, aby pomóc odzyskać ich zaufanie[34].

---

[29] *NSA spying: Facebook, Google, Twitter demand controls*, "CBC News", 9 grudnia 2013 r., http://www.cbc.ca/news/world/nsa-spying-facebook-google-twitter-demand-controls-1.2456259 (dostęp: 28 grudnia 2013 r.).

[30] *Time for an international convention on government access to data*, "Microsoft on the Issues", 20 stycznia 2014 r., http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/01/20/time-for-an-international-convention-on-government-access-to-data.aspx (dostęp: 30 stycznia 2014 r.).

[31] *Microsoft to shield foreign users' data*, "Financial Times", 22 stycznia 2014 r., http://www.ft.com/cms/s/0/e14ddf70-8390-11e3-aa65-00144feab7de.html (dostęp: 30 stycznia 2014 r.).

[32] *Privacy is not dead: Microsoft lawyer prepares to take on US government*, "The Guardian", 14 grudnia 2014 r., http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government (dostęp: 25 stycznia 2015 r.).

[33] *Yahoo Mail to support end-to-end PGP encryption by 2015*, "PC World", 8 sierpnia 2014 r., http://www.pcworld.com/article/2462852/yahoo-mail-to-support-end-to-end-pgp-encryption-by-2015.html, (dostęp: 25 stycznia 2015 r.).

[34] *Yahoo CEO Marissa Mayer Calls For NSA Transparency*, "TIME", 22 stycznia 2014 r., http://business.time.com/2014/01/22/yahoo-ceo-marissa-mayer-calls-for-nsa-transparency/#ixzz2rY5JKNP8 (dostęp: 30 stycznia 2014 r.).

Wagę szyfrowania danych podkreślał też szef rady nadzorczej Google, Eric Schmidt, którego zdaniem jest to jedyny sposób na uniemożliwienie służbom specjalnym (nie tylko amerykańskim, ale też np. chińskim czy północnokoreańskim), monitorowania klientów Google, jak również ominięcie cenzury obowiązującej w niektórych państwach[35]. Ostatecznie Google wprowadziło rozwiązania umożliwiające indywidualnym użytkownikom szyfrowanie poczty elektronicznej[36].

Firmy sektora technologicznego decydowały się też upublicznić informacje dotyczące liczby zapytań, jakie otrzymują od służb specjalnych[37]. Właściciel platformy mikroblogowej Twitter postanowił nawet zaskarżyć do sądu przepisy zabraniające informowania o skali zainteresowania użytkownikami serwisu przez służby występujące z wnioskami o dostęp do ich danych[38].

Korporacje – m.in. Microsoft, Google, Apple, Twitter, Dropbox, LinkedIn, Evernote oraz Facebook – zdecydowały się także wspólnie wspierać ustawę „USA Freedom Act", której celem ma być zwiększenie przejrzystości procedur oraz działania służb specjalnych w zakresie gromadzenia danych użytkowników[39]. Projekt ustawy, który cieszył się również poparciem Białego Domu, został jednak zablokowany w amerykańskim Senacie z powodu obaw części senatorów, których zdaniem nowe prawo uczyniłoby Stany Zjednoczone bardziej podatne na ataki terrorystów[40].

Internetowi giganci ratowali swoją reputację. Część z nich przyłączyła się jednak do walki o prawa użytkowników w zakresie prywatności w wymiarze większym, niż wynikało to z potrzeb wizerunkowych. Nie odmawiając szczerości intencji przyświecających działaniom korporacji, należy jednak zaznaczyć, że wiele tych zabiegów jest niestety przejawem hipokryzji. Internetowi giganci, jak Google, Facebook, Yahoo! czy Microsoft, utrzymują

[35] *Schmidt says encryption will help Google penetrate China*, "Wall Street Journal", 23 stycznia 2014 r., http://blogs.wsj.com/digits/2014/01/23/schmidt-says-encryption-will-help-google-penetrate-china/ (dostęp: 30 stycznia 2014 r.).

[36] *Google now offers end-to-end encryption on email*, "Gizmodo", 4 czerwca 2014 r., http://gizmodo.com/google-now-offers-end-to-end-encryption-on-email-1585831839 (dostęp: 25 stycznia 2015 r.).

[37] *Microsoft, Google, Yahoo, and others release government data request details*, "The Verge", 3 lutego 2014 r., http://www.theverge.com/2014/2/3/5374596/microsoft-google-yahoo-and-others-release-government-data-request (dostęp: 25 stycznia 2015 r.).

[38] *Twitter idzie na wojnę z rządem USA*, "Chip", 8 października 2014 r., http://www.chip.pl/news/wydarzenia/prawo-i-polityka/2014/10/twitter-idzie-na-wojne-z-rzadem-usa (dostęp: 25 stycznia 2015 r.).

[39] *Apple, Microsoft, Google, LinkedIn and Yahoo back US Freedom Act*, "The Inquirer", 18 listopada 2014 r., http://www.theinquirer.net/inquirer/news/2382022/apple-microsoft-google-linkedin-and-yahoo-back-us-freedom-act (dostęp: 25 stycznia 2015 r.).

[40] *Senate Republicans block USA Freedom Act surveillance reform bill*, "The Guardian", 19 listopada 2014 r., http://www.theguardian.com/us-news/2014/nov/18/usa-freedom-act-republicans-block-bill (dostęp: 25 stycznia 2015 r.).

swoją silną pozycję rynkową m.in. dzięki produktom i usługom, które oferują końcowym użytkownikom bezpłatnie i to w globalnej skali. Firmy te nie są jednak instytucjami charytatywnymi, a ze swojej działalności czerpią wielomiliardowe zyski. Dzieje się tak dlatego, że zarobkowym polem ich aktywności jest nie tylko dostarczanie informatycznych rozwiązań – wyszukiwarek, poczty elektronicznej, map i nawigacji, komunikatorów internetowych czy serwisów społecznościowych – ale też handel danymi, bezustannie gromadzonymi od użytkowników, którzy każdym kliknięciem przesyłają informacje dotyczące swoich zakupowych preferencji, zainteresowań, gustu muzycznego, czytanych książek, oglądanych filmów, położenia geograficznego, kręgu znajomych, a nawet osobistych finansów czy stanu zdrowia. Wszystkie zebrane dane pozwalają internetowym firmom tworzyć profile użytkowników, wykorzystywane w celu precyzyjnego dostarczania (*targetowania*) reklam konkretnych produktów specyficznej grupie docelowej. Dlatego użytkownicy (każdy dobrowolnie akceptuje regulaminy serwisów internetowych, zazwyczaj nawet ich nie czytając) nie otrzymują niczego za darmo. Płacą wirtualną walutą – swoją prywatnością – dzięki czemu dostawcy „darmowych" usług mogą zarabiać prawdziwe pieniądze. Mechanizm ten, choć powszechnie znany i budzący kontrowersje, funkcjonuje od lat i raczej nie zapowiada się, aby miał ulec zmianie. Użytkownicy przyzwyczaili się, że w internecie wszystko (lub prawie wszystko) jest darmowe i trudno znaleźć alternatywę dla wyszukiwarki Google, poczty Gmail czy serwisu społecznościowego Facebook, a próby wprowadzania płatnych usług zazwyczaj kończyły się komercyjnym fiaskiem. Wydaje się, że taki układ odpowiada wszystkim zaangażowanym stronom.

Konstrukcja globalnej sieci sprawia, że przesyłane za jej pośrednictwem dane pozostawiają cyfrowe ślady i przechowywane są (poza pewnymi wyjątkami) na serwerach dostawców usług, zgodnie z zasadą, że „internet nie zapomina". Zmiany legislacyjne w zakresie inwigilacji w dużej mierze polegają na modyfikowaniu przepisów określających, na jakich zasadach i komu dane będą udostępnianie. Skoro i tak są one gromadzone przez firmy, służbom wystarczy względnie łatwy do nich dostęp. Stale rosnąca liczba danych przesyłanych przez internet sprawia jednak, że niemożliwa lub bardzo trudna i kosztowna jest bieżąca analiza wszystkich dostępnych informacji, szczególnie jeśli są one zaszyfrowane. Tak więc służby specjalne mogą ograniczać się tylko do określonych obszarów – danych należących do osób będących w polu zainteresowania, np. podejrzanych o terroryzm lub inną nielegalną działalność.

Społeczeństwu trudno jednak zaakceptować fakt, że służby, podległe regulacjom władz państwowych i działające z definicji w interesie bezpieczeństwa narodowego, mogą mieć wgląd w ich prywatne informacje. Jednocześnie to, że te same informacje są przedmiotem handlu między korporacjami, które czerpią z tego tytułu ogromne zyski, nie budzi już tak ogromnego zaniepokojenia i burzliwej debaty publicznej. Odrębną kwestią jest pytanie, jak gromadzone latami dane mogą zostać użyte np. w sytuacji przejęcia firmy, będącej w posiadaniu informacji o milionach użytkowników lub zmiany modelu biznesowego korporacji, która w pogoni za zyskiem zdecyduje wykorzystać swoje zasoby informacyjne w celach innych niż reklamowe. Doświadczenie uczy, że gdy w grę wchodzi duży zysk, etyczne rozterki często schodzą na dalszy plan.

Warto przypomnieć, że obecni piewcy walki o ochronę prywatności jeszcze kilka lat temu wprost sugerowali zmierzch powszechnego prawa jednostek do utrzymania osobistych informacji w tajemnicy. W 2009 r. szef rady nadzorczej Google, E. Schmidt przekonywał, że klienci usług jego firmy nie powinni przejmować się tym, jakie informacje na ich temat są gromadzone i komu przekazywane. Dodał, że jeśli ktoś „nie chce, aby inni wiedzieli o tym, co robi, może w ogóle nie powinien tego robić", a wszyscy muszą mieć świadomość, że zgodnie z obowiązującym prawodawstwem przechowywane dane mogą zostać udostępnione nie tylko przypadkowym osobom przeszukującym zasoby sieci czy „wścibskim znajomym", ale również odpowiednim władzom[41]. Także związany z Google Vinton Cerf, nazywany jednym z „ojców internetu", jest zdania, że „prywatność może stać się anomalią" i coraz trudnij będzie ją zachować. Podczas konferencji „Internet of Things – Privacy and Security in a Connected World" w listopadzie 2014 r. – a więc już po ujawnieniu rewelacji E. Snowdena – powiedział, że to zachowanie samych użytkowników wyrządza największe szkody ich prywatności[42]. Założyciel serwisu Facebook, Mark Zuckerberg już w 2010 r. tłumaczył, że gdyby zależało to od niego, wszystkie zamieszczane przez użytkowników informacje domyślnie byłyby publiczne. W opinii M. Zuckerberga, normy społeczne nieustannie ewoluują, a ludziom obecnie zależy, żeby udostępniane przez nich informacje trafiały do jak najszerszego grona odbiorców[43].

[41] *Google CEO on privacy: 'If you have something you don't want anyone to know, maybe you shouldn't be doing it'*, "Huffington Post", 18 marca 2010 r., http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html (dostęp: 28 stycznia 2014 r.).

[42] *Vint Cerf: 'Privacy may be an anomaly'*, CNET, 20 listopada 2013 r., http://news.cnet.com/8301-1009_3-57613120-83/vint-cerf-privacy-may-be-an-anomaly/ (dostęp: 28 stycznia 2014 r.).

[43] *Facebook's Zuckerberg says the age of privacy is over*, "Readwrite", 9 stycznia 2010 r., http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~oueYmrLz00gp64 (dostęp: 28 stycznia 2014 r.).

Wypowiedzi osób, od których w dużej mierze zależy sposób, w jaki ludzie korzystają z internetu wskazują, że prywatność użytkowników nie znajduje się na szczycie listy ich priorytetów. Wręcz przeciwnie, więcej szczegółowych informacji osobistych pozwala tworzyć jeszcze dokładniejsze profile i skuteczniej trafiać z ofertą do odbiorców, którzy z dużą dozą prawdopodobieństwa klikną sugerowany link czy reklamę. A każde kolejne kliknięcie to zyski dla przedsiębiorstwa.

Jedno jest pewne, poddając się wygodzie oferowanej przez „darmowe" sieciowe produkty i usługi, ludzie są gotowi udostępniać olbrzymie ilości osobistych informacji. Dostęp do zebranych danych, czas ich przechowywania i zakres użycia nieprędko przestaną być przedmiotem dyskusji. Działania podjęte przez dostawców usług i operatorów sieci społecznościowych, których celem było wzmocnienie ochrony prywatności użytkowników (np. domyślne szyfrowanie przesyłanych wiadomości czy szyfrowanie danych w pamięci smartfonów) służą jednak ogólnemu podniesieniu poziomu bezpieczeństwa informacji w cyberprzestrzeni. Nie tylko wzmocniły pozycję użytkowników wobec stosujących masową inwigilację służb, ale też wobec zwykłych cyberprzestępców.

Zmiany w zachowaniu użytkowników internetu

Nie jest łatwo przełożyć zmianę zachowania czy konkretne działania podejmowane przez indywidualnych internautów na ogół zachowań użytkowników globalnej sieci, których łączną liczbę szacuje się już na ponad 3 miliardy. Spojrzenie na zmianę zachowań sieciowych użytkowników cyberprzestrzeni po opublikowaniu informacji przekazanych przez E. Snowdena dają jednak wyniki badań przeprowadzonych na dużych grupach internautów. Badanie CIGI-Ipsos Global Survey on Internet Security and Trust[44], przeprowadził na przełomie października i listopada 2014 r. think-tank Centre for International Governance Innovation (CIGI) w 24 krajach (w tym USA, Wielkiej Brytanii, a także w Polsce) na grupie około 23 tys. osób. Wynika z niego, że informacje ujawnione przez E. Snowdena skłoniły użytkowników internetu do zmiany zachowań sieciowych służących ich bezpieczeństwu. Dotyczy to m.in. częstszych zmian haseł chroniących dostępu do portali internetowych czy usług (39 proc.), a także omijania

[44] *CIGI-Ipsos Global Survey on Internet Security and Trust*, CGI, https://www.cigionline.org/internet-survey (dostęp: 25 stycznia 2015 r.).

pewnych stron internetowych lub aplikacji (43 proc.). Kolejne zmiany zachowań dotyczą zwiększonej samokontroli publikowania informacji online (28 proc.), ograniczenia kontaktów w internecie (18 proc.), a nawet zamykania profili w mediach społecznościowych (11 proc.) czy rzadszego korzystania z internetu (10 proc.). Tylko 24 proc. badanych zadeklarowało, że ich zachowania nie zmieniły się. Zdecydowana większość badanych (64 proc.) zadeklarowała, że bardziej niż rok temu martwi się o swoją prywatność, a 39 proc. badanych podjęło działania, aby ją lepiej chronić.

W badaniu zapytano także, kto zdaniem badanych powinien zajmować się utrzymaniem (administrowaniem) internetu. Według większości (57 proc.) powinna być to wielopodmiotowa i ponadnarodowa instytucja, w której skład wchodziłyby np. przedsiębiorstwa, eksperci (inżynierowie) oraz organizacje pozarządowe, którzy wspólnie reprezentowaliby interesy obywateli oraz władz. Jednocześnie tylko 36 proc. badanych uważa, że to Stany Zjednoczone powinny odgrywać istotną rolę w zarządzaniu globalną siecią. 72 proc. ankietowanych chciałoby, aby ich osobiste dane były przechowywane na terenie ich własnego kraju, co wydaje się istotne w świetle zabiegów władz Unii Europejskiej, aby dane Europejczyków znajdowały się na serwerach zlokalizowanych w Europie. Jednocześnie ponad 60 proc. jest zaniepokojonych faktem, że służby państw innych niż USA potajemnie monitorują ich aktywność w internecie[45].

Kolejne badanie, przeprowadzone przez Catherine Tucker z amerykańskiego MIT oraz zajmującego się kwestiami inwigilacji Alexa Marthewsa, polegało na analizie zapytań, jakie użytkownicy wpisywali w wyszukiwarce Google. Badanie wykazało, że po ujawnieniu informacji dotyczących masowej inwigilacji przez NSA, internauci poddali się „autocenzurze" podczas przeszukiwania zasobów internetu. Po analizie danych okazało się, że drastycznie zmalała liczba zapytań, w których występowały hasła uznawane za „krępujące" czy „prywatne". Jak zauważają badacze, te wyniki zdają się potwierdzać wzrost świadomości użytkowników w zakresie internetowego nadzoru władz. Ich zdaniem, użytkownicy mogli zrezygnować z wyszukiwania „wstydliwych" haseł lub zdecydowali się użyć w tym celu innej niż Google wyszukiwarki internetowej, oferującej lepszą ochronę prywatności. Przykładem jest wyszukiwarka „DuckDuckGo", której twórcy podkreślają, że nie gromadzi danych o użytkownikach. Liczba zapytań kierowanych do

[45] *After the Snowden leaks, 700M move to avoid NSA spying*, "Computerworld", 15 grudnia 2014 r., http://www.computerworld.com/article/2859477/after-the-snowden-leaks-700m-move-to-avoid-nsa-spying.html (dostęp: 25 stycznia 2015 r.).

tej wyszukiwarki wzrosła o 90 proc. w ciągu pierwszych dwóch tygodni od ujawnienia rewelacji E. Snowdena[46].

Wszystkie powyższe czynniki towarzyszą poczuciu utraty kontroli nad prywatnością. Amerykański think-tank Pew Research Center wskazał, że badani są raczej niechętni do rozmów na temat inwigilacji, NSA czy sprawy E. Snowdena za pomocą mediów społecznościowych[47]. Wolą na te tematy rozmawiać „twarzą w twarz". Użytkownicy internetu są bardziej świadomi tego, że media społecznościowe to sfera publiczna, a prezentowane opinie czy treści mogą trafić do odbiorców, którzy nie byli ich pierwotnymi adresatami. 91 proc. badanych Amerykanów jest zdania, że użytkownicy utracili kontrolę nad tym, jak ich osobiste dane są gromadzone i wykorzystywane przez korporacje. 70 proc. badanych wyraziło obawy o dostęp władz do danych gromadzonych przez firmy, a 64 proc. uważa, że władze powinny uregulować zasady, na jakich korporacje udostępniają prywatne informacje stronom trzecim (np. reklamodawcom). Wszystkim tym obawom towarzyszy świadomość delikatnej równowagi między prywatnością a potrzebą udostępniania osobistych informacji w zamian za darmowy dostęp do sieciowych usług (55 proc.). Co ciekawe, w ogólnym odczuciu Amerykanów, najbezpieczniejszy środek komunikacji stanowi telefon stacjonarny (67 proc.)[48].

Wzrosła świadomość, ale pozostały potrzeby informacyjne możliwe do zaspokojenia jedynie przez narzędzia, które z reguły nie gwarantują prywatności, a użytkownicy godzą się na takie zasady z wygody lub braku alternatyw. Ci, którzy sądzą, że nie mają nic do ukrycia, bez skrępowania publikują prywatne treści, w tym osobiste dane np. na portalach społecznościowych. Jeśli istnieją dwa sposoby wykonania czynności – np. wysłania wiadomości czy przechowywania danych – przy czym jeden z nich jest bezpieczny, ale uciążliwy, a drugi mniej bezpieczny, ale prosty w użyciu, jest niemal pewne, że większość użytkowników (nawet tych świadomych zagrożeń) wybierze rozwiązanie prostsze. Przykładem jest historia wicepremiera Federacji Rosyjskiej Arkadija Dworkowicza, który padł ofiarą cyberprzestępców. Złodzieje wykradli służbowe dokumenty (m.in. analizy dotyczące budżetu Rosji), które wicepremier przechowywał na prywatnej skrzynce email. Zgodnie z wypowiedziami, jakie pojawiły się po incydencie, rosyjscy

[46] *Post Snowden, Google users change habits*, "All Analytics", 7 lutego 2014 r., http://www.allanalytics.com/author.asp?section_id=1437&doc_id=273952 (dostęp: 25 stycznia 2015 r.).

[47] *Did Edward Snowden really change America?*, "The Cheat Sheet", 13 października 2014 r., http://wallstcheatsheet.com/politics/did-snowden-really-change-america.html/?a=viewall (dostęp: 25 stycznia 2015 r.).

[48] *US privacy confidence at new low, survey indicates*, "BBC", 12 listopada 2014 r., http://www.bbc.com/news/technology-30004304 (dostęp: 25 stycznia 2014 r.).

urzędnicy używają prywatnej poczty do celów służbowych z wygody i jest to powszechna praktyka umożliwiająca pracę poza biurem[49].

Powolne tempo wdrażania regulacji prawnych służących ochronie prywatności, a także zmienny i niepewny charakter zjawiska, jakim jest masowa inwigilacja i inne formy nieuprawnionego dostępu do prywatnych danych sugerują, że dla zwykłych użytkowników skuteczną metodą ochrony może być samokontrola i powściągliwość w zamieszczaniu osobistych informacji w sieci. Niezmiernie ważna jest także świadomość istniejących zagrożeń dla prywatności, a więc ciągłe samokształcenie, oraz stosowanie się użytkowników do zasad bezpieczeństwa teleinformatycznego. Taka „osobista higiena" zachowania w cyberprzestrzeni dla większości z nich będzie stanowiła pierwszą linię ochrony prywatności w konfrontacji z przestępcami czy firmami handlującymi danymi osobowymi. Konieczna jest także trwała zmiana świadomości i zrozumienie, że każda umieszczona w internecie informacja może pewnego dnia trafić w niepowołane informacje. Ryzyko to jest szczególne, ponieważ raz umieszczone w sieci dane bardzo trudno skutecznie z niej usunąć[50].

Podsumowanie

Bezustannie rosnąca ilość informacji przesyłanych drogą elektroniczną, a także postęp technologiczny w dziedzinie gromadzenia i analizy dużych zbiorów danych sprawił, że globalna sieć stała się dla służb specjalnych nieocenionym źródłem informacji, pozwalającym lepiej i szybciej identyfikować zagrożenia. Jak w przypadku większości nowo powstałych technologii, ich pozytywny wpływ na życie ludzi wiąże się także z ryzykiem nadużyć. Demaskatorska historia E. Snowdena potwierdza tę tezę odnosząc się do internetu i powiązanych z nim technologii teleinformatycznych. Historia ta pokazuje też, jak istotne są „czynnik ludzki" i emocje w sytuacjach, które zdają się mieć wymiar czysto techniczny. Zarówno pobudki działań E. Snowdena, jak i reakcje międzynarodowej społeczności na ujawnione programy amerykańskich służb wynikają z ludzkich potrzeb prywatności i poczucia bezpieczeństwa.

[49] *Wyciek e-maili rosyjskiego wicepremiera – trzymał rządową korespondencję na GMailu*, Niebezpiecznik.pl, 22 lipca 2014 r., http://niebezpiecznik.pl/post/wyciek-e-maili-rosyjskiego-wicepremiera-trzymal-rzadowa-korespondencje-na-gmailu/ (dostęp: 25 stycznia 2015 r.).

[50] *W internecie umieszczamy o jedną informację za dużo. I są „efekty"*, wyborcza.pl, 5 marca 2015 r., http://wyborcza.pl/1,75248,17520070,Kazdy_z_nas_jest_nagi.html?pelna=tak (dostęp: 9 marca 2015 r.).

Działania E. Snowdena są inaczej oceniane przez każdą z zainteresowanych stron. Zdaniem amerykańskich władz, jednostka nie powinna decydować o upublicznieniu tajnych informacji, tylko dlatego, że nie zgadza się z polityką swojego rządu. Nagminność takich działań mogłaby skutecznie utrudnić władzom możliwość zapewnienia bezpieczeństwa obywateli. Ponadto całkowita prywatność danych znajdujących się w cyberprzestrzeni stwarzałaby pole do nadużyć ze strony czujących się bezkarnie osób lub grup prowadzących działalność zagrażającą bezpieczeństwu państwa.

Osoby popierające demaskatorską działalność E. Snowdena uważają, że mają prawo wiedzieć, w jakim stopniu państwo ingeruje w ich prywatność oraz czy robi to z absolutnej konieczności, czy tylko „na wszelki wypadek", dlatego że może.

Niezależnie od tego, jak zakończy się afera wywołana przez E. Snowdena, istotny jest wpływ jego działań na władze najpotężniejszego państwa na świecie, wymuszające częściową zmianę obowiązujących reguł gry.

Przyjęte przez amerykańską administrację zmiany raczej nie spowodują zaprzestania inwigilacyjnej działalności, ale skupią się na uniemożliwieniu podobnych wycieków w przyszłości. Masowa inwigilacja jest zbyt skutecznym narzędziem, aby służby mogły z niego łatwo zrezygnować. Do informacji na temat programów będzie miało dostęp mniej osób, w tym pracowników kontraktowych, niebędących etatowymi pracownikami służb, przy zachowaniu dodatkowych środków bezpieczeństwa i poufności informacji.

E. Snowden stał się celebrytą oraz swego rodzaju symbolem kultury masowej. Z uwagi na problemy z moralną oceną jego działań, nie jest jednak symbolem jednoznacznym, a mimo wzrostu świadomości użytkowników internetu w zakresie działań służb specjalnych oraz początkowego oburzenia i faktycznej zmiany postaw części użytkowników, większość przeszła nad tym faktem do porządku dziennego.

Mimo to, uporządkowanie i wprowadzenie jasnych reguł korzystania z internetu jest koniecznością. To właśnie brak przejrzystych regulacji i zasad funkcjonowania w cyberprzestrzeni sprawił, że stała się ona sferą przyjazną przestępcom oraz terrorystom, wykorzystującym cechy internetu – brak granic, poczucie anonimowości – do działalności szkodzącej ogółowi społeczeństwa. Regulacje powinny jednak w równym stopniu dawać prawa i nakładać ograniczenia na wszystkie podmioty obecne w cyberprzestrzeni. Mówi się o potrzebie debaty nad ustaleniem granic między wolnością i prawem do prywatności a koniecznością kontroli zapewniającej bezpieczeństwo użytkowników, jednak ta debata trwa już od dłuższego czasu. Trudno wskazać jej koniec, ponieważ dyskusja na ten temat to proces,

w którym wszystkie zaangażowane strony będą podawały argumenty broniące własnego punktu widzenia i kierunku rozwoju regulacji. Niezaprzeczalnie, na mocnej pozycji w tej debacie znajdują się władze, państwowe instytucje i organizacje międzynarodowe, w których mocy jest tworzenie prawa. Pozycja silniejszego wymaga jednak zdolności do zrozumienia, samoograniczenia i etyki działania. Ważne, aby przyjmowane prawo było przejrzyste, nie prowadziło do nadużyć i służyło obywatelom. W przeciwnym razie, tak jak po aferze spowodowanej rewelacjami E. Snowdena, społeczeństwo utraci zaufanie do cyberprzestrzeni jako narzędzia komunikacji i coraz częściej będzie poddawało swoje działania autocenzurze, świadome inwigilacji, ograniczając aktywności w sieci lub przenosząc ją na inne obszary. Sektor prywatny wyrasta w tej dyskusji na strażnika równowagi. Z jednej strony korporacje muszą działać w granicach obowiązującego prawa, z drugiej zaś ich zyski płyną od użytkowników, którzy w różny sposób – gotówką czy informacjami – gotowi są płacić za cyfrowe produkty i usługi. Masowy odpływ użytkowników obawiających się inwigilacji z pewnością nie będzie służył interesom ponadnarodowych korporacji, dlatego muszą wykorzystywać swój potencjał, wiedzę i doświadczenie, w sposób etyczny, służący nie tylko krótkoterminowym zyskom, ale też budowie zaufania. Rola społeczeństwa w debacie wymaga przede wszystkim zaangażowania, gdyż pasywna postawa może być dla pozostałych stron sygnałem przyzwolenia na nadużycia. Udział w dyskusji wymaga też zrozumienia, że bycie obywatelem, także w cyberprzestrzeni, wiąże się z prawami, ale i też z obowiązkami oraz odpowiedzialnością za swoje działania.

Dyskusja poświęcona bezpieczeństwu w cyberprzestrzeni od pewnego czasu toczy się również w polskim społeczeństwie i dotyczy m.in. kwestii poufności prywatnych danych, jakie użytkownicy umieszczają w internecie. Napływające z wielu stron doniesienia o incydentach komputerowych przedostały się już do zbiorowej świadomości, czego przejawem jest zmiana podejścia władz państwowych, sektora prywatnego, organizacji pozarządowych, ale też zwykłych obywateli do spraw cyberbezpieczeństwa. Debacie o granicach swobody działania i prawa do prywatności, a także potrzebie kontroli służącej zapewnieniu bezpieczeństwa cyberprzestrzeni musi towarzyszyć kooperacja wszystkich zaangażowanych stron. W przypadku Polski, owocem takiej współpracy okazała się opublikowana w styczniu 2015 r. Doktryna cyberbezpieczeństwa RP[51]. W pracach nad nią uczestniczyły m.in.

[51] *Doktryna cyberbezpieczeństwa RP*, Biuro Bezpieczeństwa Narodowego, 22 stycznia 2015 r., http://www.bbn.gov.pl/pl/wydarzenia/6336, Doktryna-cyberbezpieczenstwa-RP.html (dostęp: 25 stycznia 2015 r.).

instytucje państwa, przedstawiciele sektora prywatnego oraz reprezentujące obywateli organizacje pozarządowe. Ich współpraca stała się kluczem do powstania tego dokumentu, jest też ideą przyświecającą osiąganiu zapisanych w nim celów, w tym społecznego porozumienia w zakresie bezpieczeństwa cyberprzestrzeni i poufności znajdujących się w niej danych. Co ważne dla przyszłej równowagi między prawem do prywatności a bezpieczeństwem, Doktryna wskazuje, że podejmowane działania powinny być prowadzone z uwzględnieniem „ochrony praw człowieka i obywatela, a także poszanowaniem prawa do wolności słowa oraz prywatności"[52]. Środki bezpieczeństwa powinny być dobierane proporcjonalnie do zagrożenia, a znacząca rola w utrzymaniu tej równowagi należy do sektora obywatelskiego, który uczestnicząc w pracach legislacyjnych i organizacyjnych ma możliwość monitorowania działań instytucji państwowych, aby bez wątpliwości służyły wszystkim zainteresowanym stronom.

[52] *Ibidem.*

Recenzje

Ryszard M. Czarny: *High North – między geografią a polityką,*
Paweł Turowski

Mike Winnerstig: T*ools of Destabilization. Russian Soft Power and Non-military Influence in the Baltic States,*
Anna Madej

Andrew Wilson: *Ukraine Crisis. What it Means for the West,*
Przemysław Pacuła

Łukasz Jureńczyk: *Wojna z talibami i Al-Kaidą. Afganistan w latach 1994–2012,*
Paweł Malendowicz