KULTURA – MEDIA – TEOLOGIA
2015 nr 20, s. 36-56.

Piotr Siuda, Uniwersytet Kazimierza Wielkiego w Bydgoszczy

Prywatność w Internecie – zarys perspektywy krytycznej

Internet Privacy – Outline of Critical Perspective

STRESZCZENIE:

Autor artykułu wychodzi z założenia, że mamy do czynienia z dwoma stanowiskami w badaniach internetu: optymistycznym i pesymistycznym. Krytycy wskazują na ekonomiczne i polityczne negatywne konsekwencje użycia Sieci, a obecnie coraz więcej uwagi poświęcają kwestii naruszeń prywatności w internecie. Badaniom na ten temat rzadko kiedy towarzyszy jednak próba ogólnego uporządkowania tego, jak wspomniane pogwałcenia postrzegają krytycy tego zagadnienia. To jest właśnie celem artykułu. Autor – posiłkując się różnymi doniesieniami akademickimi – pokazuje, jak krytycy konceptualizują prywatność internetową i jakie wyróżniają typy jej naruszeń oraz sposoby przeciwdziałania im. Omawiane zagadnienia są ważne, jeśli uznać (za krytykami), że skala naruszeń prywatności jest bardzo duża. Rzadko kiedy bada się opinie i zachowania użytkowników internetu związane z prywatnością online.

SŁOWA KLUCZOWE:

prywatność internetowa, krytyka internetu, prawo do prywatności, naruszenia prywatności, ochrona prywatności, edukacja medialna, badania internetu.

ABSTRACT:

The article claims that when it comes to studying the Internet, one can indicate two groups of researchers: the optimists and the pessimists. The later show the negative economic and political consequences of using the Web. Recently, these researchers have increasingly written about violations of the privacy of Internet users. However, a general critical framework for research on privacy violations remains lacking. The goal of this article is to propose such a framework. This article shows how pessimists conceptualize Internet privacy and what basic types of Internet privacy violation they indicate; how to protect online privacy is also discussed. The aforementioned issues are extremely crucial, particularly when considering (after the pessimists) the scale of the violations of Internet privacy and the lack of research regarding the opinions and behaviors of Internet users in regard to the infringement of online privacy.

KEYWORDS:

Internet privacy, Internet criticism, right to privacy, Internet privacy, violations of privacy, privacy protection, media literacy, Internet studies.

Medioznawcy, socjologowie czy kulturoznawcy badający internet nie mogą się zgodzić w jednoznacznej ocenie tego medium. Z jednej strony, mamy do czynienia z obozem tak zwanych optymistów, z drugiej strony - z krytykami. Ci pierwsi opisują erę internetu jako tę, która ma nieść ze sobą ekonomiczną i polityczną demokratyzację. Polityczni blogerzy mają wykrywać wszelkie nadużycia władzy[1], a konsumenci doświadczają swoistej emancypacji, mają bowiem wpływ na to, jak wyglądają dostarczane im usługi; są tak zwanymi dostarczycielami contentu, przyjmują zatem po części rolę producentów[2]. Krytycy mają inne zdanie – starają się wykazać, że internet może być raczej przyczyną politycznego zniewolenia[3], ale też wyzysku konsumentów za darmo pracujących na rzecz powiększania zysków kapitalistów[4].

Jednym z najnowszych trendów w krytyce Sieci jest podkreślanie, że wiele podmiotów bezkarnie gwałci prywatność użytkowników internetu i dlatego też używanie tego medium może przynieść wiele szkód społecznych, zarówno dla samych jednostek, jak i społeczeństw. Badacze reprezentujący nurt krytyczny różnią się poglądami odnoszącymi się do prywatności – zwracają oni uwagę na różne typy naruszeń oraz ich konsekwencje. Brakuje natomiast ogólnych spojrzeń podsumowujących i zarysowujących to, w jaki sposób kwestie omawianej prywatności są ujmowane przez krytyków. Celem artykułu jest właśnie uporządkowanie tych poglądów i syntetyczne ich przedstawienie – zarówno odnośnie do samych pogwałceń prywatności, jak i ochrony przed owymi naruszeniami. Dodatkowo, na zakończenie przedstawiam pewne postulaty dotyczące dalszych działań krytyków internetu mogących wzbogacić ich naukowe rozważania.

1. Od prywatności do prywatność w internecie

Kwestia prywatności użytkowników internetu jest podnoszona przez krytyków coraz częściej. Obecnie na całym świecie – w tym również w Polsce – obserwuje się wzrost obaw dotyczących naruszeń prywatności osób korzystających z Sieci[5]. O różnych nadużyciach informują między innymi dziennikarze[6], reprezentanci trzeciego sektora (w Polsce kwestie

1 Por. Y. Benkler, *Bogactwo sieci. Jak społeczna produkcja zmienia rynek i wolność*, Warszawa 2008.

2 Por. P. Siuda, *Kultury prosumpcji. O niemożności powstania globalnych i ponadpaństwowych społeczności fanów*, Warszawa 2012.

3 Por. E. Morozov, *The Net Delusion. The Dark Side of Internet Freedom*, New York 2011.

4 Por. J. Lanier, *Who Owns the Future?*, New York-London-Toronto-Sydney-New Delhi 2014.

5 H. Cho, M. Rivera-Sánchez, S.S. Lim, A *multinational study on online privacy: global concerns and local responses*, „New Media & Society" 2009 nr 11(3), s. 395-416.

6 R. Drzewiecki, *Systemy wyceny człowieka. Oto jak Big Data rządzi światem*, „forsal.pl" z 21.03.2014 r., http://forsal.pl/artykuly/785494,system-wyceny-czlowieka-oto-jak-big-data-rzadzi swiatem.html,2?fb_action_ids=777140545632304&fb_action_types=og.likes (dostęp: 18.03.2015 r.); M. Gajewski, *Podłe sztuczki Twittera*, „SPIDER'SWEB" (brak daty opubl.), http://www.spidersweb.pl/2012/02/podle-sztuczki-twittera-.html (dostęp: 17.03.2015 r.); P. Kusio, *Prawo do prywatności w Internecie*, „SPIDER'SWEB" (brak daty opubl.), http://www.spidersweb.pl/2012/07/prawo-do-prywatnosci-w-internecie.html (dostęp: 17.03.2015 r.); E. Lalik, A *Ty ile prywatności w sieci jesteś w stanie poświęcić dla wygody?*, „SPIDER'SWEB" (brak daty opubl.), http://www.spidersweb.pl/2012/08/ty-ile-jestes-stanie-poswiecic-dla-wygody.html (dostęp: 17.03.2015 r.); E. Lalik, *Żyję bez ciasteczek, ale to nie ma znaczenia*, „SPIDER'SWEB" (brak daty opubl.),

te podejmuje na przykład Fundacja Panoptykon) czy przedstawiciele administracji (w Polsce Generalny Inspektor Ochrony Danych Osobowych). Temat ten zaczyna być zatem ważny również dla naukowcó - krytyków dyskutujących nad koniecznością oraz najwłaściwszymi metodami zapewnienia ochrony obywateli Sieci,[7] co jest istotne z perspektywy dbałości o wolność obywatelską. Omawiane zagadnienia zaczynają być ważne również ze względu na kwestię praktyk rozlicznych instytucji posądzanych o naruszanie praw jednostek do prywatności. Wiele środowisk informuje o propozycjach zmiany prawa czy potrzebie podjęcia przez przedsiębiorstwa internetowe różnych działań samoregulacyjnych, czyli o samoograniczaniu się, jeśli chodzi o naruszenia prywatności internautów[8].

Współcześnie część krytyków coraz intensywniej podkreśla niebezpieczeństwa wynikające z tego, że zbyt wiele informacji wpada w ręce przedsiębiorstw, które wykorzystują konsumentów[9]. Inni twierdzą, że nadużyć dopuszczają się poszczególne rządy, w tym przede wszystkim rząd USA, mogący śledzić internetową działalność obywateli wszystkich państw świata[10]. Wielu analityków zgodnie jednak podkreśla potrzebę edukowania osób korzystających z sieci tak, aby same dbały o własną prywatność[11] (oraz prywatność innych), aby nabyły one w tym względzie odpowiednie kompetencje. Krytycy podkreślają także, że zapewnienie prywatności powinno być obowiązkiem biznesu, ale też rządów, organizacji pozarządowych czy instytucji odpowiedzialnych za edukację medialną.

U podstaw owego „bicia na alarm" leży przekonanie, że obecnie można w internecie zdobyć na temat danego użytkownika praktycznie wszystkie informacje[12], łącznie z tym, ile zarabia, jakie ma poglądy polityczne, jakie książki czyta, które filmy i seriale

---

http://www.spidersweb.pl/2013/12/internet-bez-cookies.html (dostęp: 17.08.2014 r.); E. Mistewicz, *Czy można jeszcze zaufać Google i Facebookowi?*, „Forbes" z 04.11.2013 r., http://www.forbes.pl/czy-mozna-jeszcze-zaufac-google-i-facebookowi-,artykuly,165870,1,1.html (dostęp: 17.03.2015 r.).

7 Por. L. Andrews, I *Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*, New York 2011; T. Buchanan, C. Paine, A.N. Joinson, R. Ulf-Dietrich, *Development of measures of online privacy concern and protection for use on the Internet*, „Journal of the American Society for Information Science and Technology" 2007 nr 58(2), s. 157-165; A. Keen, *Digital Vertigo: How Today's Online Social Revolution Is Dividing, Diminishing, and Disorienting Us*, New York 2012; G. Kuczyński, *Ochrona prywatności w internecie*, „Marketing w praktyce" 2009 nr 3, s. 30-32; J. Lanier, *Who Owns the Future?*, New York 2013; R.H. Weber, *Internet of Things – New security and privacy challenges*, „Computer Law & Security Review" 2010 nr 26(1), s. 23-30; D. Wilusz, *Zagrożenia dla prywatności w Internecie. Przyszłości i możliwości jej ochrony*, w: R. Naskręcki, G. Pawłowski, A. Zabor, J. Morawska (red.), *Kształcenie w zakresie Internetu rzeczy*, Poznań 2011, s. 84-103.

8 J. Fernback, Z. Papacharissi, *Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies*, „New Media & Society" 2007 nr 9(5), s. 715-734.

9 Por. J. Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*, New Haven-London 2011.

10 Por. J. Gilliom, T. Monahan, *SuperVision: An Introduction to the Surveillance Society*, Chicago 2012; B.S. Krueger, *Government Surveillance and Political Participation on the Internet*, „Social Science Computer Review" 2005 nr 23(4), s. 439-452.

11 Por. P. Siuda, G.D. Stunża, A.J. Dąbrowska, M. Klimowicz, E. Kulczycki, R. Piotrowska, E. Rozkosz, M. Sieńko, K. Stachura, *Dzieci Sieci 2.0. Kompetencje komunikacyjne młodych*, Gdańsk 2013.

12 Por. W. Orliński, *Internet. Czas się bać*, Warszawa 2013, s. 106.

Dzisiaj konieczność zapewnienia prywatności rozumie się inaczej, utożsamiając ją z kontrolowaniem przez jednostkę tego, jakie informacje o niej samej komunikowane są innym. Chodzi zatem o osobistą prywatność informacyjną, a nie o inne rodzaje prywatności, na przykład ekonomiczną, gwarantowaną przedsiębiorcom.

ogląda, z kim się przyjaźni, jakie są jego hobby, z kim spędza noce. Wszystkie te dane – i wiele innych – są możliwe do odnalezienia w Sieci. Wiele serwisów komercyjnych gromadzi je i wykorzystuje, a, co ważne, często nie są bezpieczne nawet te osoby, którym wydaje się, że zawsze były ostrożne i nikomu nie ujawniały informacji o sobie.

Przyglądając się poglądom krytyków, uznać należy, że jako punkt wyjścia przyjmują oni istniejącą i rozpowszechnioną koncepcję prywatności (niektórzy robią to w sposób bezpośredni, kiedy jasno określają punkt wyjścia swoich rozważań, inni czynią to w domyśle)[13]. O prywatności jako prawie, które każdy człowiek powinien mieć zagwarantowane, badacze zaczęli mówić pod koniec XIX wieku, kiedy Samuel D. Warren i Louis D. Brandeis[14] napisali słynny artykuł zatytułowany *Prawo do prywatności*. Autorzy zdefiniowali owo prawo jako możliwość „bycia zostawionym samemu sobie"[15]. Dzisiaj konieczność zapewnienia prywatności rozumie się inaczej, utożsamiając ją z kontrolowaniem przez jednostkę tego, jakie informacje o niej samej komunikowane są innym. Chodzi zatem o osobistą prywatność informacyjną, a nie o inne rodzaje prywatności, na przykład ekonomiczną, gwarantowaną przedsiębiorcom. Dane na temat poszczególnych osób nie powinny być udostępniane innym bez zgody tych osób. Co więcej, ludzie muszą mieć wpływ na to, jak wykorzystuje się informacje na ich temat[16].

---

13 Por. D.J. Solove, *Conceptualizing Privacy*, „California Law Review" 2002 nr 90(4), s. 1087-1155.

14 S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, nr 4(5), s. 193-220.

15 A. Gajda, *What if Samuel D. Warren hadn't Married a Senator's Daughter: Uncovering the Press Coverage That Led to the Right to Privacy*, „Michigan State Law Review" 2008 nr 07-06; D. J. Glancy, *Invention of the Right to Privacy*, „Arizona Law Review" 1979 nr 21(1); J. Woo, *The right not to be identified: privacy and anonymity in the interactive media environment*, „New Media & Society" 2006 nr 8(6), s. 949-967.

16 E.W. Craig, M. Zeljkovic, A *personalized approach to web privacy: awareness, attitudes and actions*, „Information Management & Computer Security" 2011, nr 19(1), s. 53-73; G.S. Mesch, *Is Online Trust and Trust in Social Institutions Associated with Online Disclosure of Identifiable Information Online?*, „Computers in Human Behavior" 2012 nr 28(4), s. 1471-1477; D.J. Solove, *I've Got Nothing to Hide and Other Misunderstandings of Privacy*, „San Diego Law Review" 2007 nr 45, s. 745-772.

Warren i Brandeis zwrócili uwagę, że naruszenia prywatności wynikają przede wszystkim z działalności mediów (głównie prasy), ingerujących w codzienne życie człowieka i prezentujących jego sprawy osobiste dość często w sferze publicznej. Wspomniani autorzy zauważyli, że taka ingerencja w prywatność zaczęła się na dużą skalę w momencie wynalezienia maszyny drukarskiej.

Współczesna definicja prawa do prywatności się zmienia. Wychodząc od klasycznego ujęcia Warrena i Brandeisa, krytycy uznają, że wskutek powstania internetu mamy do czynienia z zupełnie inną sytuacją niż kiedyś. Sieć nie tylko powiększyła zakres osobistych informacji, które są zbierane i przetwarzane przez różne podmioty, ale również spowodowała, że zaczęto się ponownie zastanawiać, jak powinna dzisiaj wyglądać ochrona prywatności. Jeśli ujmować sprawę w sposób ogólny – tak, aby całościowo objąć różne pesymistyczne stanowiska – stwierdzić należy, że krytycy ujmują naruszenia prywatności internetowej jako wszelkie problematyczne aktywności sieciowe dotyczące zbierania, przechowywania, przetwarzania, przekształcania i udostępniania osobistych informacji o danych jednostkach.

2. Naruszenie prywatności internetowej

Patrząc na to, jakie działania – i których podmiotów – krytycy wskazują jako naruszające prywatność *online*, można mówić o trzech typach takich działań – ekonomicznych, politycznych i tych odbywających się w skali mikro. Poniżej zaprezentowane zostanie omówienie wszystkich trzech rodzajów naruszeń tak, jak widzą je akademicy krytycy. Przedstawiona typologia to jeden z elementów porządkowania omawianego tematu – takich zestawień wciąż brakuje w literaturze przedmiotu.

Naruszenia prywatności obejmują wykorzystanie szeregu różnych technik[17]. Krytycy Sieci reprezentujący nauki socjologiczne, medioznawstwo czy kulturoznawstwo przedstawiają mniej lub bardziej dokładniejsze ich opisy. Są to przede wszystkim: instalowanie plików *cookies* oraz tak zwanych *flash cookies*; technologie *non-cookies*[18] (na przykład przeglądarki nieużywające „ciasteczek"); nakłanianie do przechowywania danych w tak zwanej „chmurze"[19]; *scraping*, czyli technika, za pomocą której program komputerowy wydobywa dane z wyjścia innego programu; *deep-packet inspection* (DPI), pozwalająca analizować pakiety przesyłane przez Sieć pod względem ich treści; zdalnie instalowane keyloggery, czyli programy wykrywające to, co dana osoba pisze na klawiaturze.

---

17 Por. E. Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, New York 2011; E. Toch, Y. Wang, L.F. Cranor, *Personalization and Privacy: A Survey of Privacy Risks and Remedies in Personalization-Based Systems*, „User Modeling and User-Adapted Interaction" 2012 nr 22(102), s. 203-220.

18 Por. Barford, P., Canadi, I., Krushevskaja, D., Ma, Q., Muthukrishnan, S., *Adscape: harvesting and analyzing online display ads*, „WWW '14 Proceedings of the 23rd international conference on World wide web" 2014, s. 597-608.

19 Por. Ion, I. Sachdeva, N., Kumaraguru, P., Čapkun, S., *Home is safer than the cloud!: privacy concerns for consumer cloud storage*, „SOUPS '11 Proceedings of the Seventh Symposium on Usable Privacy and Security" 2011, artykuł nr 13.

Różne metody stosowane są z różną intensywnością i w przypadku różnych typów naruszeń. Na przykład użycie plików *cookies* jest niezbędne przy ekonomicznym marketingu behawioralnym i w związku z tym jest praktycznie powszechne (stosowane wobec każdego internauty). Użycie innych technik jest rzadsze (na przykład DPI lub keyloggery), choć warto zauważyć, że wszystkie one pozwalają odkrywać niezwykle „delikatne" informacje (różne metody dają dostęp do różnych danych). Przez zastosowanie wspomnianych technik można na przykład poznać: numer karty kredytowej podawany na stronie www, hasła sieciowe, długość i rozmówcę telefonicznego połączenia przez Skype, odwiedzone strony internetowe, czas pozostawania na nich, adres IP, treść wpisów i prywatnych wiadomości w serwisach społecznościowych oraz na prywatnych forach, zawartość e-maili i ich załączników, hasła wyszukiwania wpisywane do wyszukiwarek internetowych itd.

2.1. Naruszenia ekonomiczne

Działania te związane są z aktywnością wielkich przedsiębiorstw (na przykład Google, Facebook, Twitter), które – mając na uwadze swoje dobro – decydują się na monitorowanie działań internautów oraz wykorzystywanie danych umieszczanych przez nich w internecie. Chodzi tutaj przede wszystkim o tak zwany *behavioral advertising*, czyli praktyki odnoszące się do dostosowywania treści do konkretnego użytkownika w oparciu o historię jego internetowej aktywności[20]. Aby uzmysłowić sobie, o czym mowa, wystarczy przeprowadzić eksperyment – odwiedzić wybrany rodzaj serwisów internetowych, na przykład strony e-aptek. Zebrane informacje o takiej aktywności internauty zostaną sprzedane reklamodawcom chętnym polecać leki, a to znajdzie odzwierciedlenie w reklamach pojawiających się podczas surfowania uskutecznianego przez internautę. Warto zaznaczyć, że chociaż marketing behawioralny utożsamia się z personalizacją reklam, to – jak pokazują krytycy – coraz częściej dopasowywane są także inne przekazy, chociażby artykuły informacyjne czy treści rozrywkowe[21]. Warto również dodać, że krytycy Sieci nie deprecjonują analityki sieciowej rozumianej jako statystyczne mierzenie ruchu w danym serwisie. Każda firma chce bowiem wiedzieć, ile osób odwiedza tworzoną przez nią stronę WWW. Negatywnie ocenianie przez badaczy Sieci jest natomiast gromadzenie danych na temat każdego internauty i sprzedaż tych danych reklamodawcom.

Naruszenia ekonomiczne to jednak nie tylko *behavioral advertising*. Korzystanie z różnych serwisów i narzędzi internetowych pociąga za sobą konieczność ujawnienia wielu informacji o sobie, które potem mogą być wykorzystane do celów marketingowych lub jakichkolwiek innych. Firmy sieciowe są krytykowane za pozorny charakter oraz łamanie zasad prywatności[22] zmieniających się w coraz szybszym tempie na nieko-

[20] M. Lisiecki, M. Sowiński, *Targetowanie behawioralne – jak ominąć pułapki*, „Marketing w Praktyce" 2009 nr 8, s. 8-11.

[21] Por. J. Fernback, Z. Papacharissi, art. cyt., s. 715-734; C. Fuchs, *The Political Economy of Privacy on Facebook*, „Television & New Media" 2012 nr 13(2), s. 139-159.

[22] Pokazał to „The Wall Street Journal" w dochodzeniu dziennikarskim, w wyniku którego wyszło na jaw, że aplikacje facebookowe takie jak FarmVille czy Mafia Wars ujawniają ID danego użytkownika, a także

rzyść użytkowników i pozwalających na większe nadużycia. Każdorazowa zmiana tak zwanej „polityki prywatności" zwykle skutkuje zresetowaniem dotychczasowych ustawień internauty, co oznacza, że dane prywatne stają się publiczne[23].

Zdaniem krytyków Sieci zostaje w ten sposób naruszona prywatność nawet tych osób, które starają się dbać o bezpieczeństwo ich danych w internecie. Często nie pomaga występowanie w różnych miejscach pod pseudonimem, ponieważ programy kojarzące twarz (kolejna technika mogąca być używana do naruszania prywatności) bez problemu „odkrywają" prawdziwe imię i nazwisko danego człowieka, o ile był on tak nieostrożny, że gdzieś w internecie pojawiło się jego zdjęcie z faktycznymi danymi.

Prywatność użytkowników może być naruszana przez wielkie przedsiębiorstwa nawet wtedy, gdy ktoś nie używa produkowanych przez nie serwisów. Wystarczy przy zakładaniu konta na Facebooku potwierdzić zgodę na udostępnienie serwisowi hasła swojej skrzynki poczty elektronicznej w celu „zintegrowania kontaktów", wówczas do każdego e-maila, którego po takiej czynności użytkownik otrzyma będzie miał dostęp również Facebook[24].

Krytycy Sieci negatywnie oceniają to, że wskutek praktyk zaliczanych do marketingu behawioralnego internauci coraz bardziej polegają na firmach pod względem wyboru przyswajanych informacji. W rezultacie może ucierpieć ich samostanowienie rozumiane w kategoriach autonomii dotyczącej konsumowanych przekazów. Proces podejmowania decyzji niekoniecznie musi się opierać na informacjach wyszukanych samodzielnie (przykładem mogą być zakupy w księgarni internetowej, gdzie dość trudno jest się „wyrwać" z kręgu polecanych książek). Zjawisko to może być problematyczne, ponieważ stopień swobody związanej z kontrolowaniem procesu przyswajania informacji jest ważnym czynnikiem kształtującym jednostkową tożsamość.

Joseph Turow w książce *The Daily You* zauważył to, co podkreśla wielu krytyków – skrupulatne „szpiegowanie" ludzi w internecie zmienia sposób postrzegania siebie oraz otaczającego nas świata[25]. Niestety nie są to zmiany na dobre; konsekwencje związane są przede wszystkim z dyskryminacyjnym potencjałem nowego sposobu zbierania i dostarczania wiedzy na temat konsumentów. Dzielenie ich na konkretne typy, w zależności od tego, co robią w Sieci – na przykład pod względem wydawanych w e-sklepach pieniędzy – ma powodować swoistą nierówność. Tylko niektórym – to znaczy tym przydzielonym do segmentu osób lepiej zarabiających – oferuje się sprzedaż luksusowych towarów, obniżki cenowe czy wyższe kredyty. Sytuacja taka skutkować ma obniżeniem samooceny tych, którym takie okazje się nie trafiają. To jednak nie wszystko, ponieważ w przyszło-

informacje o jego wieku, miejscu zamieszkania i pracy oraz zdjęcia; M. McWhertor, *Report: FarmVille 'Breaks' Facebook Privacy Rules, Sends Personal Info To Ad Firms*, „Kotaku" z 18.10.2010 r., http://kotaku.com/5667215/report-farmville-breaks-facebook-privacy-rules-sends-personal-info-to-ad-firms (dostęp: 17.03.2015 r.).

23 L. Andrews, dz. cyt.; R. Bendrath, M. Mueller, *The end of the net as we know it? Deep packet inspection and internet governance*, „New Media & Society" 2011 nr 13(7), s. 1142-1160.

24 W. Orliński, dz. cyt., s. 107.

25 J. Turow, dz. cyt.

> Krytycy Sieci negatywnie oceniają to, że wskutek praktyk zaliczanych do marketingu behawioralnego internauci coraz bardziej polegają na firmach pod względem wyboru przyswajanych informacji. W rezultacie może ucierpieć ich samostanowienie rozumiane w kategoriach autonomii dotyczącej konsumowanych przekazów.

ści będzie można wręcz mówić o wytworzeniu się specyficznej podklasy internetowych „przegranych". Ich horyzonty oraz okazje życiowe będą znacząco ograniczane. Powstają nowi sieciowi decydenci wpływający na życie wielu milionów ludzi na podstawie niejasnych często kryteriów, wśród których internetowa historia, dochody, miejsce zamieszkania czy wiek to te, o których możemy jedynie zgadywać, że są istotne[26].

Naruszenia prywatności mogą być według Turowa przyczyną totalnej fragmentaryzacji społecznej posuniętej do punktu, w którym podmiotem wszelkich działań – w tym dyskryminacyjnych – będą nie grupy, lecz jednostki. Czeka nas zanik zaufania i więzi międzyludzkich oraz wspólnych wszystkim ram społecznych wyznaczanych przez tradycyjne media (telewizja, radio, tradycyjna prasa, książki).

Przestaje mieć znaczenie fakt, czy informacje o konkretnym użytkowniku będą zbierane w sposób ujawniający jego imię i nazwisko, czy przyporządkuje mu się jedynie jakiś numer porządkowy; w obu przypadkach konsekwencje samego gromadzenia danych będą dla owego netizena identyczne.

Abstrahując od poglądów Turowa, należy zaznaczyć, że krytycy ubolewają nad tym, iż wielkie przedsiębiorstwa – łamiąc prywatność użytkowników – skutecznie znajdują luki w przepisach prawnych. Chociaż po drugiej wojnie światowej prawo do prywatności dołączono do katalogu praw człowieka i obywatela w Deklaracji ONZ z 1948 roku[27], to jednak Deklaracja ta nie ma charakteru wiążącego, co oznacza, że nie jest ona

[26] Podobnie stwierdziła Lori Andrews w książce I *Know Who You Are and I Saw What You Did*, dowodząc, że zniekształcony i uproszczony – bowiem stworzony na podstawie historii sieciowych poczynań – obraz człowieka, może zdecydować o ważnych życiowo sprawach. Na przykład wiele banków amerykańskich właśnie takimi środkami ocenia zdolność kredytową swoich klientów, co dobitnie pokazuje, że zamiast odzwierciedlać rzeczywistość, analizy behawioralne *online* mogą ją tworzyć. Innym, dość makabrycznym przykładem, jest sytuacja cierpiącej na depresję osoby, która na forum pomocowym zwierza się, że zamierza popełnić samobójstwo przez łyknięcie tabletek o nazwie X. Co otrzymuje w zamian? Reklamę kontekstową tabletek o nazwie X; L. Andrews, dz. cyt.

[27] 12 artykuł owej Deklaracji stwierdza, że „nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu

traktatem, lecz rezolucją – wyrazem dobrej woli. Pod względem stanu prawnego można wskazać wyraźne różnice między Stanami Zjednoczonym, a Unią Europejską pod względem ochrony prywatności – na Starym Kontynencie zdecydowanie bardziej restrykcyjnie podchodzi się do jej ochrony[28].

W USA prywatność chroniona jest przez zapis zawarty w czwartej poprawce do Konstytucji, przeciwdziałającej między innymi bezzasadnym rewizjom czy podsłuchom. Jest to jednak luźny zapis, a praktyka prawna odnosząca się do naruszeń prywatności ukształtowała się raczej pod wpływem precedensów oraz wpływowych tekstów, takich jak ten Warrena i Brandeisa.

Inaczej jest w Europie – Europejska Konwencja Praw Człowieka przyjęta w 1953 roku i ratyfikowana przez wszystkie kraje UE jest wiążąca i zakłada, że każdy ma prawo do „poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji" (artykuł 8 Konwencji). Dodatkowo, każde państwo Unii ma swoje własne ustawy o ochronie prywatności – w Polsce jest to „Ustawa o ochronie danych osobowych" z 1997 roku – co jest wynikiem przyjęcia w 1995 roku unijnej dyrektywy o ochronie prywatności. W Europie funkcjonują różne czuwające nad prywatnością instytucje – niemające swoich odpowiedników w Stanach Zjednoczonych Ameryki Północnej – takie jak chociażby European Data Protection Supervisor (w Polsce na podobnej zasadzie działa GIODO – Główny Inspektor Ochrony Danych Osobowych). Prawo europejskie obejmuje sankcjami nie tylko naruszających prywatność, ale również tych, którzy dane objęte ochroną udostępniają niepowołanym osobom nieintencjonalnie albo nie dbają o odpowiednie zabezpieczenie owych danych.

Dlaczego zatem wielkie firmy z USA naruszają prywatność nie tylko Amerykanów, ale również Europejczyków? Zdaniem krytyków – właśnie, dlatego że są z USA. Chociaż wszystkie posiadają siedziby także w Irlandii (głównie po to, aby uniknąć płacenia wysokich amerykańskich podatków), to jednak podlegają amerykańskiemu prawu, a w Stanach Zjednoczonych Ameryki Północnej procesy sądowe przeciwko cyberkorporacjom w sprawach o naruszenia prywatności są rzadkością. Jeśli nawet do tego dochodzi, przedsiębiorstwa często bronią się tłumaczeniem, że przecież użytkownicy zgadzają się z polityką prywatności danego serwisu, bo założyli na nim profil[29]. Europejczycy w zamian za darmowy dostęp do amerykańskich serwisów zrzekli się po prostu praw przysługujących im jako obywatelom UE.

Krytycy Sieci podkreślają, iż to, że koncerny z USA świadczące usługi w krajach Unii nie podlegają europejskiemu prawu, jest wynikiem dyktatu amerykańskiego utrwalonego w momencie, który uznaje się za kluczowy dla procesu komercjalizacji in-

imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu". P. Waszkiewicz, *Wielki Brat Rok 2010: Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne*, Warszawa 2010, s. 76.

28 W. Orliński, dz. cyt., s. 92-95.

29 S. Musil, *Google filing says Gmail users have no expectation of privacy*, „CNET" z 13.08.2013 r., http://www.cnet.com/news/google-filing-says-gmail-users-have-no-expectation-of-privacy (dostęp: 17.03.2015 r.).

> Prawo europejskie obejmuje sankcjami nie tylko naruszających prywatność, ale również tych, którzy dane objęte ochroną udostępniają niepowołanym osobom nieintencjonalnie albo nie dbają o odpowiednie zabezpieczenie owych danych.

ternetu. W 1995 roku Al Gore, zastępca Billa Clintona, zdecydował się na udzielenie sieciowym firmom kilku znaczących przywilejów mających wzmocnić ich pozycję i doprowadzić do rozkwitu przemysłu internetowego[30]. Miał on być zapewniony również przy pomocy bezkompromisowej postawy rządu amerykańskiego wobec państw europejskich. USA, wykorzystując niezwykle ostre posunięcia w sferze polityki zagranicznej i handlowej, zapewniły sobie przewagę przejawiającą się między innymi „nietykalnością" amerykańskich cyberfirm[31]. Taki status: „pozwala im na eksport danych z Europy – ten eksport nie musi dotyczyć fizycznego przeniesienia danych z serwera na serwer. Zmienia się tylko ich status prawny, przestają być chronione po europejsku[32], a zaczynają być po amerykańsku"[33].

2.2. Naruszenia polityczne

W wypadku naruszeń politycznych chodzi o ingerencję w prywatność dokonywaną przez instytucje państwowe używające Sieci do inwigilowania obywateli własnego państwa lub innych państw[34]. Gromadzenie informacji na temat mieszkańców danego kraju zawsze było jednym z podstawowych zadań współczesnego państwa. Jak zaznaczają krytycy Sieci, wraz z rozwojem technologii informacyjnych funkcja ta nabrała nowego wymiaru; nadzór nad jednostkami stał się łatwiejszy, szybszy i często niezawodny. Niektórzy krytycy podkreślają, że naruszenia polityczne znacznie różnią się od tych rynkowych. Pierwsze – w odróżnieniu od drugich – polegać mają po prostu na przełamywaniu zabezpieczeń komputera w celu inwigilacji (używane są zatem „ostrzejsze" techniki na-

[30] Jednym z głównych przywilejów było wyłączenie z odpowiedzialności za treści, które użytkownicy umieszczają w *social media*. Zgodnie z tym postanowieniem nie można pozwać danego koncernu za to, że jakiś użytkownik oczernił innego, umieszczając obraźliwe treści w serwisie prowadzonym przez owo przedsiębiorstwo; por. W. Orliński, dz. cyt., s. 157-159.

[31] Tamże.

[32] Trzeba dodać, że może to być furtką dla firm europejskich chcących naruszać prywatność Europejczyków. Jeśli nawet nie mogą one gromadzić i przetwarzać danych o użytkownikach, bo zabrania im tego prawo, wystarczy zlecić takie działania odpowiedniemu przedsiębiorstwu z USA.

[33] W. Orliński, dz. cyt., s. 109.

[34] J. Gilliom, T. Monahan, dz. cyt.; B.S. Krueger, art. cyt., s. 439-452.

ruszeń)[35]. Mimo to, wielu analityków zauważa, że sprawa wcale nie przedstawia się tak prosto. Twierdzą oni, że naruszenia polityczne są z ekonomicznymi mocno powiązane. Wielkie cyberkorporacje współpracują z rządami, dostarczając wszelkich danych, o które te proszą. Część krytyków Sieci często wiąże ze sobą naruszenia dokonywane przez rządy oraz te wynikające z potrzeb rynku (agencje rządowe, współpracując z firmami, mogą uzyskać wgląd w dane każdego użytkownika konkretnego serwisu czy narzędzia)[36].

O politycznym aspekcie pogwałceń coraz częściej donoszą media, pokazując, że obywatele wielu państw są szpiegowani na przykład pod pozorem walki z wrogiem zewnętrznym lub wewnętrznym, przeciwdziałania cyberprzestępczości, zwalczania szkodliwego oprogramowania (wirusy, *mallware*, *spyware i* inne) czy walki z piractwem (zapobieganie naruszeniom prawa autorskiego). Zaniepokojeni dziennikarze informują o bezprecedensowych zagrożeniach odnoszących się do zakresu, w jakim państwa ograniczają swobodę jednostek wskutek naruszania ich prawa do prywatności. Wśród krytyków Sieci zainteresowanie tym tematem uwidoczniło się zwłaszcza po tak zwanej „aferze Edwarda Snowdena". Ten trzydziestoletni informatyk wykonujący prace na zlecenie amerykańskiej NSA (Agencja Bezpieczeństwa Narodowego) został tak zwanym sygnalistą (ang. *whistleblower*), czyli osobą demaskującą oburzające postępowanie rządu. Snowden w maju 2013 roku zdecydował się ujawnić światu przy pomocy gazety „The Guardian" skalę sieciowej inwigilacji amerykańskich służb bezpieczeństwa. *Whistleblower* wyjawił między innymi prawdę o tak zwanym PRISM, czyli programie szpiegowania ludzi przez wgląd do danych zgromadzonych przez wielkie przedsiębiorstwa internetowe. Bohater afery w momencie publikacji informacji na temat NSA stał się w USA przestępcą – obecnie przebywa w Rosji, gdzie otrzymał tymczasowy azyl[37].

Krytycy są zgodni co do tego, że afera Snowdena potwierdziła to, o czym spekulowano już dość dawno – Stany Zjednoczone Ameryki na ogromną skalę inwigilują swoich obywateli, a także obywateli innych państw. Co ciekawe, czasami owo inwigilowanie może mieć szczytne cele – takie jak zwalczanie terroryzmu[38], czasami jednak powodowane jest motywami budzącymi niesmak. Na fali „objawień" Snowdena wyszło na jaw, że pracownicy NSA używają pozostających do ich dyspozycji narzędzi po to, aby szpiego-

35 Por. tamże.

36 Por. W. Orliński, dz. cyt.

37 M. Czarnecki, *Edward Snowden. To on ujawnił totalną inwigilację*, „wyborcza.pl" z 10.06.2013 r., http://wyborcza.pl/1,76842,14075994,Edward_Snowden__To_on_ujawnil_totalna_inwigilacje.html (dostęp: 17.03.2015 r.).

38 Przed ujawnieniem szczegółów na temat PRISM, argument, że naruszenia prywatności są konieczne, jeśli chce się skutecznie walczyć z terroryzmem, często wysuwany był przez polityków amerykańskich. Po zamachu w Nowym Yorku we wrześniu 2001 roku oraz po zamachach w Londynie (2004) i Madrycie (2005) zdanie takie podzielali nawet politycy europejscy. Moment, aby rozpocząć negocjacje z USA w sprawie ochrony prywatności obywateli państw UE, po prostu nigdy nie był dogodny; por. W. Orliński, dz. cyt., s. 111.

wać swoich obecnych lub potencjalnych partnerów[39]. Jak się okazało, praktyka ta miała nawet w agencji kryptonim – LOVEINT.

Obecnie agencje największych zachodnich państw aktywnie ze sobą współpracują. Nawet jeśli przedstawiciele służb wywiadowczych jednego z krajów ograniczeni są prawem w naruszaniu prywatności obywateli własnego państwa, mogą poprosić o pomoc pracowników z innego kraju[40]. Na takiej zasadzie NSA kooperuje z angielskim SIS (Secret Intelligence Service), niemieckim Bundesnachrichtendienst czy francuską DGSE, czyli Generalną Dyrekcją Bezpieczeństwa Zewnętrznego[41].

2.3. Naruszenia w skali mikro

Przy charakteryzowaniu naruszeń prywatności *online* krytycy Sieci skupiają się nie tylko na dużych, łatwo identyfikowanych instytucjach takich, jak przedsiębiorstwa internetowe czy agencje rządowe. Naruszenie prywatności może być dokonywane również w skali mikro poprzez „małe" instytucje (szkoły, placówki zdrowia, małe firmy posiadające stronę www), pracodawcy, sąsiedzi, koledzy, przyjaciele czy zupełnie obce osoby (zarówno przeciętni obywatele, jak i cyberprzestępcy[42]).

Tego typu naruszenia mają być skutkiem intencjonalnego działania osób trzecich, w przypadku wszelkiego typu złośliwego wykorzystania przez kogoś informacji na temat danej osoby poprzez założenie strony www ujawniającej informacje dotyczące sfery prywatnej osoby. Takie naruszenie prywatności często wiąże się z nieostrożnością internautów, gdy na przykład ktoś opublikuje na Facebooku swoje kompromitujące zdjęcia. W literaturze znaleźć można wiele przykładów sytuacji, kiedy nieostrożność staje się podstawą naruszenia prywatności[43]. Nauczycielka zwolniona z pracy z powodu publikacji w serwisie społecznościowym wakacyjnego zdjęcia na plaży z trzymanym w ręku piwem; ofiara gwałtu, która z powodu swobodnych zdjęć została uznana za prowokatorkę i „ukarana" uniewinnieniem przez sąd sprawcy; pracodawca przeglądający profile potencjalnych pracowników i na podstawie opublikowanych zdjęć decydujący o przebiegu procesu rekruta-

---

39 S. Gorman, *NSA Officers Spy on Love Interests*, „The Wall Street Journal" z 23.08.2013 r., http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests (dostęp: 17.03.2015 r.).

40 Warto wspomnieć, że jeśli chodzi o obywateli Polski, to oczywiście – jako użytkownicy serwisów największych cyberkorporacji – mogą oni być poddani opisanej inwigilacji. Trudno natomiast ocenić jej skalę, tym bardziej że dokonywane przez różne media czy organizacje (Helsińska Fundacja Praw Człowieka, Fundacja Panoptykon) próby skłonienia polskiego rządu, aby ten ujawnił zakres procederu szpiegowania, spełzają na panewce; por. W. Orliński, dz. cyt., s. 27.

41 Tamże, s. 226.

42 V.R. Brown, E.D. Vaughn, *The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions*, „Journal of Business and Psychology" 2011 nr 26(2), s. 219-225; A.E. Marwick, D. Murgia-Diaz, J.G. Jr. Palfrey, *Youth, Privacy and Reputation (Literature Review)*, „Harvard Public Law Working Paper" 2010 nr 10; D.J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale 2007.

43 Por. L. Andrews, dz. cyt.; P. Siuda, G.D. Stunża (red.), *Dzieci sieci – kompetencje komunikacyjne najmłodszych: Raport z badań*, Gdańsk 2012.

cyjnego – to przykłady realnych sytuacji. Naruszeniom prywatności winna jest osoba stosująca cyberprzemoc czy zwalniająca z pracy na bazie zebranych przez siebie w internecie informacji, a nie na bazie oceny rzetelności wykonywanej pracy.

Naukowcy donoszący o naruszeniach prywatności skupiają się jednak przede wszystkim na sieciowych firmach i agencjach rządowych. Wydaje się, że mikroskala nie jest uznawana za równie istotną ze względu na to, że zachodzące w tej dziedzinie naruszenia nie mają tak szkodliwego wpływu na społeczeństwo. Jeśli przyjrzeć się sformułowanej w tym artykule definicji naruszeń prywatności sieciowej, nie sposób nie uznać, że jest nimi cyberprzemoc[44].

3. Sposoby ochrony prywatności internetowej

Akademiccy krytycy wskazujący na fakt naruszeń prywatności internautów przez wielkie korporacje oraz agencje wywiadowcze zwykle proponują rozwiązanie problemu przez wzmożoną kontrolę podmiotów ingerujących w prywatność[45], a także zmianę prawa na bardziej restrykcyjne (USA) lub poprzez skuteczne respektowanie obecnych już zapisów czy „wypowiedzenie posłuszeństwa" Stanom Zjednoczonym Ameryki Północnej (kraje europejskie). Odpowiednie ustawy powinny gwarantować prywatność użytkowników – groźba państwowej kontroli i surowe kary za łamanie regulacji mogłyby wesprzeć działania na rzecz ochrony tych wartości.

W sferze ekonomicznej krytycy postulują nadzór nad nowomedialnymi przedsiębiorstwami. Potrzebne są regulacje rządowe, które ograniczą nadużycia w sferze naruszeń prywatności. Gdyby monopol informacyjny, jaki zdobywają wielkie firmy, zrównoważony był odpowiednimi działaniami rządowymi, wówczas Sieć pozostałaby nieskomercjalizowana i nie przestałaby być dobrem wspólnym[46], jak ma to miejsce w obecnych czasach. Krytycy podkreślają, że należy tym procesom położyć kres przy pomocy prawa. Konieczna jest ich zdaniem również mniej formalna kontrola – naukowcy oraz aktywiści powinni znacznie częściej badać tę tematykę i pisać coraz więcej o skutkach naruszania prywatności. Środowisko naukowców może bowiem edukować różne grupy społeczne i w ten sposób zwiększać również świadomość internautów.

Wywieranie presji na koncerny przez „złą prasę" i zwracanie uwagi na problem prywatności przynieść może jeszcze jeden skutek, jakim jest samoregulacja, czyli dobrowolna rezygnacja ze śledzenia internautów. Raczej wątpliwe jest całkowite jego ograniczenie, bardziej prawdopodobny scenariusz przewiduje swoistą emancypację użytkowników. Dzisiaj, próbując zagwarantować sobie prywatność, użytkownik Sieci sam musi o nią zadbać, wyłączając na przykład opcję *cookies w* przeglądarce. Jednym słowem fir-

[44] Być może należałoby podjąć więcej badań na temat związku naruszeń ekonomicznych z pogwałceniami w skali mikro; chociażby zastanowić się, czy wielkie przedsiębiorstwa nie powinny być odpowiedzialne za to, co na swoich profilach umieszczają poszczególni użytkownicy (na przykład oznaczanie na zdjęciach innych osób bez ich pozwolenia).

[45] L. Andrews, dz. cyt.; J. Turow, dz. cyt.

[46] Por. R.W. McChesney, *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*, New York 2013.

> Potrzebne są regulacje rządowe, które ograniczą nadużycia w sferze naruszeń prywatności. Gdyby monopol informacyjny, jaki zdobywają wielkie firmy, zrównoważony był odpowiednimi działaniami rządowymi, wówczas Sieć pozostałaby nieskomercjalizowana i nie przestałaby być dobrem wspólnym.

my wymuszają, aby internauci sami „odcinali się" (*opt-out*) od praktyk behawioralnych. Zdaniem krytyków, mogłoby to jednak wyglądać inaczej. Korporacje – pod wpływem tendencji samoregulacyjnych – uznać powinny konieczność pełnego poinformowania o marketingu behawioralnym i uzyskiwania zgody internautów na jego użycie (*opt-in*). Po wejściu na daną stronę użytkownik winien być powiadomiony o naruszeniu prywatność i wyrazić na owo naruszenie zgodę.

Jeśli chodzi o naruszenia polityczne, tu również krytycy piszą o potrzebie większej kontroli służb specjalnych oraz uchwaleniu odpowiednich ustaw. Równie ważna ma być samoregulacja, czyli ograniczanie szpiegowania jako stojącego w jawnej sprzeczności z poszanowaniem prawa do prywatności. Do tej pory nie ten system nie sprawdził się (wspomniana afera LOVEINT), a funkcjonariusze służb inwigilujący swoich partnerów nie ponieśli żadnych konsekwencji[47].

Warto w tym momencie zauważyć, że – w związku z tym, że rządowe naruszenia są mocno związane z ekonomicznymi – ograniczanie naruszeń przez regulacje prawne może okazać się według krytyków trudne. Jeśli dla służb specjalnych z USA – a to one najmocniej inwigilują internautów – paliwem napędowym są informacje dostarczane przez cyberkorporacje, to tak naprawdę trudno się spodziewać, że rząd amerykański zainteresowany będzie wprowadzaniem ustaw godzących w interesy sieciowych koncernów. Chcąc ochraniać interesy konsumentów, związałby sobie tak naprawdę ręce i pozbawiłby się świetnego narzędzia mającego zapewniać „bezpieczeństwo narodowe". Krytycy alarmują, że istnieje swoiste zamknięte koło, bowiem nikomu, kto narusza prywatność, nie opłaca się tak naprawdę ograniczać szpiegowania.

Być może dlatego część krytyków wskazuje na inne rozwiązania, opierające się na kształtowaniu odpowiednich postaw i wyrabianiu kompetencji samych internautów, a polegające na oddolnym przeciwdziałaniu naruszeniom. Nie wierzą weń zwolennicy regulowania prawnego, ponieważ dowodzą, że działania oddolne są mało skuteczne, a poza tym odpowiedzialność za poczynania koncernów nie może być przerzucana na

[47] Por. W. Orliński, dz. cyt., s. 214-215.

poszczególnych użytkowników[48]. Mimo to, propozycje takie się pojawiają[49]. Warto przy tym zaznaczyć, że nabywanie kompetencji ma być następstwem zarówno odpowiedniej edukacji formalnej, jak i nieformalnej. Umiejętności mają być wyrabiane w szkole, ale też wskutek działań samokształcących oraz w wyniku obcowania z innymi internautami (różne kompetencje można nabyć w różny sposób).

Wyróżnić można trzy główne grupy kompetencji:

Troska – chodzi tutaj o swoisty namysł nad własną prywatnością i podejmowanie prostych działań wynikających z owego namysłu. Każdy użytkownik powinien starać się określić, czy jest wystarczająco chroniony. Jeśli stwierdzi, że nie jest, może podawać fałszywe dane przy zakładaniu profili na portalach społecznościowych. Internauta powinien dbać o to, aby samemu nie prowokować naruszeń w skali mikro, czyli zwracać uwagę na to, co udostępnia innym (szczególnie obcym) osobom, odpowiednio reagować na cyberprzemoc, dbać o prywatność innych użytkowników, nie oznaczać ich na zdjęciach na Facebooku bez pytania o zgodę. Mowa jest zatem przede wszystkim o umiejętnościach „miękkich", w wypadku których nie potrzebna jest jakakolwiek wiedza informatyczna[50].

Technologia – chodzi tu o sprawne posługiwanie się komputerem i internetem oraz znajomość używanych serwisów czy oprogramowania[51]. Liczy się wiedza, jakie ustawienia serwisów społecznościowych zastosować, aby nie wystawiać się na naruszenia w skali mikro. Można jednak „walczyć" także z naruszeniami ekonomicznymi czy politycznymi. Dzięki „zbijaniu" *cookies* (użycie specjalnych programów, odpowiednie konfigurowanie przeglądarek) prawdopodobne jest uniknięcie marketingu behawioralnego. Dodatkowo, różne programy mogą spowodować, że internauta utrudni zadanie tym, którzy chcieliby go inwigilować.

Aktywizm – chodzi o specyficzną postawę „polityczną", to znaczy świadome rezygnowanie z usług koncernów naruszających prywatność. W duchu aktywizmu utrzymane jest na przykład nieużywanie internetu mobilnego na tabletach czy smartfonach, a więc urządzeniach, na których nie można instalować oprogramowania chroniącego przed naruszeniami. Aktywista nie przechowuje swoich danych w tak zwanej chmurze. Oznacza to praktycznie „oddanie" owych danych firmom inwigilującym go. Mając do wyboru serwis społecznościowy prowadzony przez koncern sieciowego (np. Facebook) lub inny „mniejszy", zawsze wybiera ten drugi. Aktywista to również osoba interesująca się sprawami prywatności internetowej oraz posiadająca na ten temat sporą wiedzę. Może też partycypować w jakiej organizacji pozarządowej walczącej o przestrzeganie prawa do prywatności, a także głosuje w wyborach na osoby i partie opowiadające się za jej ochroną[52].

---

48 Por. tamże, s. 255.

49 Por. P. Siuda, G.D. Stunża, A.J. Dąbrowska, M. Klimowicz, E. Kulczycki, R. Piotrowska, E. Rozkosz, M. Sieńko, K. Stachura, dz. cyt.

50 Por. tamże.

51 Por. tamże.

52 Por. W. Orliński, dz. cyt., s. 267-268.

Zakończenie (o propozycji badania użytkowników)

Wcześniejsze rozważania pokazują, że krytycy ujmują naruszenia prywatności jako stojące w sprzeczności z podstawowym prawem każdego człowieka do ochrony własnej prywatności. Zwracającą oni uwagę na ewentualne groźne następstwa naruszeń, na przykład represje polityczne, osłabienie demokracji, wzrost nierówności społecznych, pogorszenie się jakości życia poszczególnych ludzi, obniżenie ich samooceny itd. Nie kwestionując takiego osądu, warto zauważyć, że jego siła mogłaby zostać wzmocniona, jeśli okazałoby się, że sami użytkownicy Sieci również postrzegają naruszenie własnej prywatności jako coś zatrważającego. Alarmujący akademiccy analitycy rzadko kiedy uwzględniają zdanie samych internautów, tak jakby przyjęli stanowisko, że z racji „wrodzonego" charakteru prawa do prywatności nie ma sensu przejmować się opiniami ludzi. Nie należy się ich zdaniem tymi opiniami zajmować, tym bardziej, że użytkownicy prawdopodobnie nie zdają sobie sprawy z tego, co dla nich samych jest dobre (ochrona prywatności), a co złe (naruszenia prywatności).

Spojrzenie na kwestie prywatności sieciowej z perspektywy internautów faktycznie jest rzadkością. Badań podejmujących ten temat wciąż jest za mało, a istniejące analizy traktują problem pobieżnie. Nieobecna jest w tych badaniach refleksja o deklaratywnym charakterze opinii nieprzekładających się na faktyczne zachowania ludzi[53]. Zaznaczyć trzeba, że wiele opisywanych w literaturze przedmiotu dociekań jest – z racji czasu, w jakim były prowadzone – po prostu nieaktualnych[54], a ponadto dotyczą wybranych państw, głównie Stanów Zjednoczonych Ameryki Północnej[55].

Ewentualne badania powinny się więc zwrócić w stronę badania nie tylko opinii użytkowników, ale także powinny za cel postawić sobie analizę ich rzeczywistych zachowań[56]. Analizy te powinno ponadto odpowiedzieć na szereg ważkich pytań: czy internauci mają coś przeciwko naruszaniu ich prywatności, a jeśli tak, to czy ich obawa przed naruszeniami przekłada się na sposoby korzystania z Sieci polegające na dbałości o prywatność? Czy zachowania internautów dotyczące ochrony prywatności *online* są nie-

---

53 Por. J.A. Castańeda, F.J. Montoso, T. Luque, *The dimensionality of customer privacy concern on the internet*, „Online Information Review" 2007 nr 31(4), s. 420-439; T. Dinev, P. Hart, M.R. Mullenb, *Internet privacy concerns and beliefs about government surveillance – An empirical investigation*, „The Journal of Strategic Information Systems" 2008 nr 17(3), s. 214-233.

54 Por. D. O'Neil, *Analysis of Internet Users' Level of Online Privacy Concerns*, „Social Science Computer Review" 2001 nr 19(1), s. 17-31.

55 Por. T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, *Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States*, „Journal of Global Information Management" 2006 nr 14(4); E. Garde-Perik, P. Markopoulos, B. Ruyter, B. Eggen, W. Ijsselsteijn, *Investing Privacy Attitudes and Behavior in Relation to Personalization*, „Social Science Computer Review" 2008 nr 26(1), s. 20-43.

56 Por. I. Bilogrevic, M. Jadliwala, I. Lam, I. Aad, P. Ginzboorg, V. Niemi, L. Bindschaedler, J-P. Hubaux, *Big Brother Knows Your Friends: On Privacy of Social Communities in Pervasive Networks*, „Pervasive Computing Lecture Notes in Computer Science" 2012 nr 7319, s. 370-387; J. Turow, M. Hennessy, *Internet privacy and institutional trust: insights from a national survey*, „New Media & Society" 2007, nr 9(2), s. 300-318.

świadome, co oznacza, że nie są zaplanowane i przygotowane, lecz przypadkowe? Czy internauci są chętni, aby dobrowolnie „zrzekać się" swojej prywatności w zamian za korzyści, jakie przynieść mogą naruszenia? Czy zdaniem internautów lepsze są tradycyjne metody regulacji cyberfirm („odgórnie" narzucone prawa), czy może należy „promować" aktywności mogące być określonymi mianem „oddolnych" (ukrywanie własnej tożsamości; podawanie fałszywej tożsamości itp.)?

Niedostrzeganie użytkowników jest błędem nie tylko, dlatego że wskutek różnych badań wzmocnione mogłoby zostać stanowisko naukowców krytykujących naruszenia (jeśli okazałoby się, że ludzie są oburzeni praktykami cyberkorporacji czy rządów). Wydaje się, że takie badania mogłyby mieć poważne zastosowanie praktyczne, bowiem każde działanie mające na celu zmianę obowiązujących regulacji lub edukowanie ludzi powinno uwzględniać to, jak prywatność pojmują internauci i jak się zachowują w Sieci. W tym względzie szczególnie zaznacza się potrzeba prowadzenia częstych badań, bowiem środowisko sieciowe ciągle się zmienia pod wpływem wprowadzania nowych funkcjonalności. Niewątpliwie można wyobrazić sobie sytuację, kiedy politycy, przedstawiciele trzeciego sektora czy osoby odpowiedzialne za edukację medialną „użyją" rezultatów różnych badań do planowania działań dotyczących ochrony prawa do prywatności[57] czy edukowania młodych ludzi[58].

Możliwe jest również, że w toku badań zostanie udowodnione, że użytkownicy Sieci nie mają problemu z pozbawianiem się swojej prywatności w zamian za darmowe usługi internetowe. Krytycy inwigilacji zapewne jednak nie zmienią zdania w tej kwestii, jednak mogłaby zostać wówczas znacznie osłabiona siła ich argumentów. Nawet jeśli miałoby się tak stać, to badania opinii i zachowań użytkowników internetu należy przeprowadzać choćby dlatego, że bazując na ich wynikach, można by zacząć tworzyć nową koncepcję prywatności. Wydaje się, że obecnie – mimo niezwykle silnego zainteresowania krytyków sprawami prywatności internetowej – nieobecna jest pogłębiona i systematyzująca rozważania refleksja teoretyczna na temat prywatności *online*. Badania opinii i zachowań internautów mogłyby zapełnić owe braki, pozwalając jednoznacznie zdecydować, czy internauci powinni się bać tego, o czym coraz intensywniej donoszą krytycy Sieci. ■

BIBLIOGRAFIA:

Andrews L., I *Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*, New York 2011.

Barford P., Canadi I., Krushevskaja D., Ma Q., Muthukrishnan S., *Adscape: harvesting and analyzing online display ads*, „WWW '14 Proceedings of the 23rd international conference on World wide web" New York 2014, s. 597-608.

[57] Por. A. Rogacka-Łukasik, *Naruszenie dóbr osobistych w Internecie oraz ich ochrona na podstawie ustawy o świadczeniu usług drogą elektroniczną*, „Roczniki Administracji i Prawa" 2012 nr 12, s. 233-252.

[58] Por. P. Siuda, G.D. Stunża, A.J. Dąbrowska, M. Klimowicz, E. Kulczycki, R. Piotrowska, E. Rozkosz, M. Sieńko, K. Stachura, dz. cyt.

Bendrath R., Mueller M., *The end of the net as we know it? Deep packet inspection and internet governance*, „New Media & Society" 2011 nr 13(7), s. 1142-1160.

Benkler Y, *Bogactwo sieci. Jak społeczna produkcja zmienia rynek i wolność*, Warszawa 2008.

Bilogrevic I., Jadliwala M., Lam I., Aad I., Ginzboorg P., Niemi V., Bindschaedler L., Hubaux J-P., *Big Brother Knows Your Friends: On Privacy of Social Communities in Pervasive Networks*, „Pervasive Computing Lecture Notes in Computer Science" 2012 nr 7319, s. 370-387.

Brown V.R., Vaughn E.D., *The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions*, „Journal of Business and Psychology" 2011 nr 26(2), s. 219-225.

Buchanan T., Paine C., Joinson A.N., Ulf-Dietrich R., *Development of measures of online privacy concern and protection for use on the Internet*, „Journal of the American Society for Information Science and Technology" 2007 nr 58(2), s. 157-165.

Castańeda J.A., Montoso F.J., Luque T., *The dimensionality of customer privacy concern on the internet*, „Online Information Review" 2007 nr 31(4), s. 420-439.

Cho H., Rivera-Sánchez M., Lim S.S., A *multinational study on online privacy: global concerns and local responses*, „New Media & Society" 2009 nr 11(3), s. 395-416.

Craig E.W., Zeljkovic M., A *personalized approach to web privacy: awareness, attitudes and actions*, „Information Management & Computer Security" 2011, nr 19(1), s. 53-73.

Czarnecki M., *Edward Snowden. To on ujawnił totalną inwigilację*, „wyborcza.pl" z 10.06.2013 r., http://wyborcza.pl/1,76842,14075994,Edward_Snowden__To_on_ujawnil_totalna_inwigilacje.html (dostęp: 17.03.2015 r.).

Dinev T., Bellotto M., Hart P., Russo V., Serra I., *Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States*, „Journal of Global Information Management" 2006 nr 14(4), s. 1-13.

Dinev T., Hart P., Mullenb M.R., *Internet privacy concerns and beliefs about government surveillance – An empirical investigation*, „The Journal of Strategic Information Systems" 2008 nr 17(3), s. 214-233.

Drzewiecki R., *Systemy wyceny człowieka. Oto jak Big Data rządzi światem*, „forsal.pl" z 21.03.2014 r., http://forsal.pl/artykuly/785494,system-wyceny-czlowieka-oto-jak-big-data-rzadzi-swiatem.html,2?fb_action_ids=777140545632304&fb_action_types=og.likes (dostęp: 18.03.2015 r.).

Fernback J., Papacharissi Z., *Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies*, „New Media & Society" 2007 nr 9(5), s. 715-734.

Fuchs C., *The Political Economy of Privacy on Facebook*, „Television & New Media" 2012 nr 13(2), s. 139-159.

Gajda A., *What if Samuel D. Warren hadn't Married a Senator's Daughter: Uncovering the Press Coverage That Led to the Right to Privacy*, „Michigan State Law Review" 2008 nr 07-06, s. 3-38.

Gajewski M., *Podłe sztuczki Twittera*, „SPIDER'SWEB" (brak daty opubl.), http://www.spidersweb.pl/2012/02/podle-sztuczki-twittera.html (dostęp: 17.03.2015 r.).

Garde-Perik E., Markopoulos P., Ruyter B., Eggen B., Ijsselsteijn W., *Investing Privacy Attitudes and Behavior in Relation to Personalization*, „Social Science Computer Review" 2008 nr 26(1), s. 20-43.

Gilliom J., Monahan T., *SuperVision: An Introduction to the Surveillance Society*, Chicago 2012.

Glancy D.J., *Invention of the Right to Privacy*, „Arizona Law Review" 1979 nr 21(1), s. 1-39.

Gorman S., *NSA Officers Spy on Love Interests*, „The Wall Street Journal" z 23.08.2013 r., http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests (dostęp: 17.03.2015 r.).

Ion I. Sachdeva N., Kumaraguru P., Čapkun S., *Home is safer than the cloud!: privacy concerns for consumer cloud storage*, „SOUPS '11 Proceedings of the Seventh Symposium on Usable Privacy and Security" New York 2011, s. 1-20.

Keen A., *Digital Vertigo: How Today's Online Social Revolution Is Dividing, Diminishing, and Disorienting Us*, New York 2012.

Krueger B.S., *Government Surveillance and Political Participation on the Internet*, „Social Science Computer Review" 2005 nr 23(4), s. 439-452.

Kuczyński G., *Ochrona prywatności w internecie*, „Marketing w praktyce" 2009 nr 3, s. 30-32.

Kusio P., *Prawo do prywatności w Internecie*, „SPIDER'SWEB" (brak daty opubl.), http://www.spidersweb.pl/2012/07/prawo-do-prywatnosci-w-internecie.html (dostęp: 17.03.2015 r.).

Lalik E., A *Ty ile prywatności w sieci jesteś w stanie poświęcić dla wygody?*, „SPIDER'SWEB" (brak daty opubl.), http://www.spidersweb.pl/2012/08/ty-ile-jestes-stanie-poswiecic-dla-wygody.html (dostęp: 17.03.2015 r.).

Lalik E., *Żyję bez ciasteczek, ale to nie ma znaczenia*, „SPIDER'SWEB" (brak daty opubl.), http://www.spidersweb.pl/2013/12/internet-bez-cookies.html (dostęp: 17.03.2015 r.).

Lanier J., *Who Owns the Future?*, New York 2013.

Lisiecki M., Sowiński M., *Targetowanie behawioralne – jak ominąć pułapki*, „Marketing w Praktyce" 2009 nr 8, s. 8-11.

Marwick A.E., Murgia-Diaz D., Palfrey Jr. J.G., *Youth, Privacy and Reputation (Literature Review)*, „Harvard Public Law Working Paper" 2010 nr 10, s. 10-29.

McWhertor M., *Report: FarmVille 'Breaks' Facebook Privacy Rules, Sends Personal Info To Ad Firms*, „Kotaku" z 18.10.2010 r., http://kotaku.com/5667215/report-farmville-breaks-facebook-privacy--rules-sends-personal-info-to-ad-firms (dostęp: 17.03.2015 r.).

Mesch G.S., *Is Online Trust and Trust in Social Institutions Associated with Online*

Disclosure of Identifiable Information Online?, „Computers in Human Behavior" 2012 nr 28(4), s. 1471-1477.

Mistewicz E., *Czy można jeszcze zaufać Google i Facebookowi?*, „Forbes" z 04.11.2013 r., http://www.forbes.pl/czy-mozna-jeszcze-zaufac-google-i--facebookowi-,artykuly,165870,1,1.html (dostęp: 17.03.2015 r.).

Morozov E., *The Net Delusion. The Dark Side of Internet Freedom*, New York 2011.

Musil S., *Google filing says Gmail users have no expectation of privacy*, „CNET" z 13.08.2013 r., http://www.cnet.com/news/google-filing-says-gmail-users-have-no-expectation-of-privacy (dostęp: 17.03.2015 r.).

O'Neil D., *Analysis of Internet Users' Level of Online Privacy Concerns*, „Social Science Computer Review" 2001 nr 19(1), s. 17-31.

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

Pariser E., *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, New York 2011.

Rogacka-Łukasik A., *Naruszenie dóbr osobistych w Internecie oraz ich ochrona na podstawie ustawy o świadczeniu usług drogą elektroniczną*, „Roczniki Administracji i Prawa" 2012 nr 12, s. 233-252.

Siuda P., *Kultury prosumpcji. O niemożności powstania globalnych i ponadpaństwowych społeczności fanów*, Warszawa 2012.

Siuda P., Stunża G.D. (red.), *Dzieci sieci – kompetencje komunikacyjne najmłodszych: Raport z badań*, Gdańsk 2012.

Siuda P., Stunża G.D., Dąbrowska A.J., Klimowicz M., Kulczycki E., Piotrowska R., Rozkosz E., Sieńko M., Stachura K., *Dzieci Sieci 2.0. Kompetencje komunikacyjne młodych*, Gdańsk 2013.

Solove D.J., *Conceptualizing Privacy*, „California Law Review" 2002 nr 90(4), s. 1087-1155.

Solove D.J., *I've Got Nothing to Hide and Other Misunderstandings of Privacy*, „San Diego Law Review" 2007 nr 45, s. 745-772.

Solove D.J., *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale 2007.

Toch E., Wang Y., Cranor L.F., *Personalization and Privacy: A Survey of Privacy Risks and Remedies in Personalization-Based Systems*, „User Modeling and User-Adapted Interaction" 2012 nr 22(102), s. 203-220.

Turow J., *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*, New Haven-London 2011.

Warren S.D., Brandeis L.D., *The Right to Privacy*, „Harvard Law Review" 1890, nr 4(5), s. 193-220.

Waszkiewicz P., *Wielki Brat Rok 2010: Systemy monitoringu wizyjnego – aspekty*
kryminalistyczne, kryminologiczne i prawne, Warszawa 2010.

Weber R.H., *Internet of Things – New security and privacy challenges*, „Computer Law & Security Review" 2010 nr 26(1), s. 23-30.

Wilusz D., *Zagrożenia dla prywatności w Internecie. Przyszłości i możliwości jej ochrony*, w: R. Naskręcki, G. Pawłowski, A. Zabor, J. Morawska (red.), *Kształcenie w zakresie Internetu rzeczy*, Poznań 2011, s. 84-103.

Woo J., *The right not to be identified: privacy and anonymity in the interactive media environment*, „New Media & Society" 2006 nr 8(6), s. 949-967.

O AUTORZE:

dr Piotr Siuda *– zainteresowany między innymi popkulturą i internetem. Adiunkt w Katedrze Socjologii na Wydziale Administracji i Nauk Społecznych UKW w Bydgoszczy, wykładowca na Humanistyce 2.0 tej uczelni. Koordynator szeregu projektów badawczych (Prosumpcjonizm pop-przemysłów, cykl Dzieci sieci) oraz autor książek Religia a Internet (2010), Kultury prosumpcji (2012) oraz Japonizacja (2014); publikował w wielu periodykach naukowych (między innymi w „European Journal of Cultural Studies", „Studia Socjologiczne", „Kultura i Społeczeństwo", „Kultura i Edukacja"). Jest szkoleniowcem Wydawnictwa Naukowego PWN; organizuje dla tej firmy seminaria naukowe. Członek Zarządu Oddziału Toruńskiego Polskiego Towarzystwa Socjologicznego oraz Członek Association of Internet Researchers. Prowadzi stronę WWW i blog: http://piotrsiuda.pl; można do niego napisać na adres: piotr.siuda@gmail.com.*