Studia Socialia Cracoviensia 10 (2018) nr 2 (19), s. 67–82
http://dx.doi.org/10.15633/ssc.3334

Agata Dziekan-Łanucha
Uniwersytet Papieski Jana Pawła II w Krakowie

Strategia zaciemniania jako odpowiedź na cyfrową inwigilację

Abstract **The strategy of the obfuscation as the reaction to the digital surveillance**. Users, who take advantage of the digital media, gradually lose their privacy. Internet corporations and national governments use the new technology to track people. It is impossible to avoid the surveillance. Common users will not cope with the fight with Internet giants and state administrations. Helen Nissenbaum and Finn Brunton recommend the defense against the domination of the strong ones. They present the strategy of the obfuscation, i.e. such activity while using the digital media, which will not allow to collect true information about the user, because the information noise will be formed around him. The aim of this article is to show the examples of the digital surveillance, and to present the reaction to this surveillance, namely, the strategy of the obfuscation.

Strategia zaciemniania jako odpowiedź na cyfrową inwigilację. Użytkownicy korzystający z mediów cyfrowych stopniowo tracą swoją prywatność. Przedsiębiorstwa internetowe i rządy państw wykorzystują nowe technologie do śledzenia ludzi. Nie jest możliwe uchronienie się przed inwigilacją. Zwykli użytkownicy nie poradzą sobie w konfrontacji z gigantami internetowymi i państwami. Helen Nissenbaum i Finn Brunton proponują obronę przed dominacją silnych. Przedstawiają strategię zaciemniania, czyli taką aktywność podczas korzystania z mediów cyfrowych, która nie pozwoli na zebranie prawdziwych informacji o użytkowniku, ponieważ wokół niego zostanie stworzony szum informacyjny. Celem artykułu jest pokazanie przykładów cyfrowej inwigilacji i przedstawienie odpowiedzi na tę inwigilację, czyli strategii zaciemniania.

Keywords obfuscation, digital surveillance, information noise, privacy, asymmetries of power and information, search engine, social media

zaciemnianie, cyfrowa inwigilacja, szum informacyjny, prywatność, asymetria władzy i informacji, wyszukiwarka, media społecznościowe

Prywatność to selektywna kontrola jednostki nad dostępem do niej samej[1]. W innej definicji – nieco bardziej rozbudowanej – również pojawia się element kontrolowania, trzymania pieczy nad tym, co dotyczy bezpośrednio danej osoby. W tej definicji prywatność jawi się jako konstrukt mający trzy wymiary: informacyjny, dostępności, ekspresji. W pierwszym kontrola dotyczy informacji o jednostce (kto z zewnątrz może mieć do nich dostęp, kiedy, w jakim zakresie). W drugim chodzi o sprawowanie nadzoru nad fizycznym dostępem do chroniącej swą prywatność jednostki. Trzeci wymiar związany jest z decydowaniem, kontrolą nad tym, w jaki sposób osoba wyraża swoją tożsamość, osobowość (ten wymiar kojarzony jest z wolnością)[2].

O sprawowaniu kontroli w odniesieniu do wyjaśniania pojęcia prywatności mówi też definicja przedstawiająca prywatność jako integralność kontekstową informacji. O ochronie prywatności, kontroli nad tym, co prywatne, można mówić wtedy, gdy w danej sytuacji, kontekście nastąpiło ujawnienie, przekazanie tylu informacji prywatnych, na ile ten kontekst, sytuacja pozwalała. Człowiek bowiem funkcjonuje w różnych kontekstach i w każdym z nich kontrola nad ujawnianymi informacjami prywatnymi ma inny zakres (szerszy lub węższy). Co innego uznaje się za możliwe do ujawnienia w rozmowie z bliskim przyjacielem, co innego podczas wizyty u lekarza, a co innego w rozmowie z przełożonym w miejscu pracy[3].

Zachowanie prywatności, przywiązywanie coraz większej wagi do ochrony prywatności przynosi ludziom korzyści. Prywatność daje szanse na odpoczynek od napięć życia społecznego, odcięcie się od wymagań, jakie stawia społeczeństwo (pełnienia określonej roli). Odizolowanie się od innych to także sposobność do odkrycia własnej tożsamości, realizacji tych jej cech, które na zewnątrz nie zawsze są dobrze postrzegane (a co daje satysfakcję jednostce, poczucie integralności).

Prywatność oznacza nie tylko korzyści indywidualne, ale także takie, które warunkują rozwój społeczny. Prywatność bowiem daje jednostce – jej aktywność jest wtedy nieograniczona obserwacją i krytyką innych osób – możliwość pełniejszego zaangażowania się w kreatywne myślenie, rozwój idei, rozwiązywania problemów[4].

W świecie, w którym istniały tylko media analogowe (można nazwać go światem analogowym w odróżnieniu od obecnego, nazywanego światem cyfrowym), uzgodnienia dotyczące prawa do prywatności wystarczyły do jego ochrony. Na co dzień ludzie, jeśli nie żyli w państwie totalitarnym lub autorytarnym, nie musieli bać się o swoją prywatność. Zbieranie danych na potrzeby marketingowe, badania poziomu odbioru mediów, określenie różnych tendencji występujących w społeczeństwie – aby je uzyskać – wymagało zwykle otwartego, jawnego działania, badany miał zatem świadomość

[1] Ł. Kołodziejczyk, *Prywatność w Internecie*, Warszawa 2014, s. 16.

[2] Ł. Kołodziejczyk, *Prywatność w Internecie*, dz. cyt., s. 18.

[3] H. Nissenbaum, *Privacy as Contextual Integrity*, „Washington Law Review" 79 (2004), https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (10.05.2017).

[4] L. Kołodziejczyk, *Prywatność w Internecie*, dz. cyt., s. 16.

przekazywania danych o sobie. Oczywiście naruszenie prawa do prywatności było możliwe, mogło dojść do podsłuchiwania rozmów, przejęcia korespondencji listowej, zakładania podsłuchów w telefonie, wyłudzania danych osobowych. Jednakże tego rodzaju działania mogły mieć tylko ograniczony zasięg. Jeśli charakteryzowały się większym, wymagały ogromnych nakładów pracy, a więc były trudne do zrealizowania. Decydujące znaczenie miała tu specyfika mediów analogowych. Pojawienie się internetu i mediów cyfrowych zmieniło realia.

1. Prywatność w świecie cyfrowym

Erik Schmidt, człowiek tworzący te media, mówi o całkowitej otwartości w relacjach międzyludzkich[5]. Jego poglądy nazywane są radykalną transparencją. Mark Zuckerberg, również wpływający na kształt cyfrowego świata, używał słów, które sugerowały, że prywatność nie jest już normą społeczną[6]. Rozwój internetu i mediów działających na bazie światowej sieci oraz technologii cyfrowych to czas stopniowej utraty tego, co stanowi istotę ochrony prywatności, czyli podkreślanej wyżej owej kontroli nad ujawnianiem, przekazywaniem przez jednostkę wiedzy o niej samej. Ludzie coraz częściej nie mają kontroli nad tym, co inni o nich wiedzą, nie mogą ograniczyć ujawnianych o sobie informacji. Te czynniki powodują pojawienie się lęku, niepewności, nieufności wobec cyfrowego świata.

Internet w swej istocie zakłada swobodny przepływ informacji. Sama jego natura o tym decyduje. Treści, dane, które są przekazywane za pomocą tego medium, charakteryzuje łatwość kopiowania, zapisywania, archiwizowania, brak ograniczeń przestrzennych w dystrybucji. Nastąpiło ograniczenie do minimum kosztów realizacji tego rodzaju procesów. Internet, media cyfrowe „prowokują" do dzielenia się treściami, przesyłania dalej tego, czego użytkownikom udało się dowiedzieć, co zdołali wykryć, wyszukać. Trudno zachować kontrolę nad danymi, które zostały wprowadzone do środowiska sieciowego.

Środowisko cyfrowe powoduje większą skłonność do ujawniania lub przekazywania informacji także ze względu na uwarunkowania psychologiczne. Użytkownik, komunikując się z innymi, zwykle nie doświadcza bezpośredniej i równoczesnej obecności innych uczestników. Obcując z bezosobowym komputerem, odczuwa raczej izolację, co daje mu poczucie bezpieczeństwa[7]. Jest też skłonny do przekazywania danych, ponieważ nie potrafi jeszcze przewidzieć konsekwencji swoich działań. Zna świat realny, fizyczny. W nim umie zadbać o ochronę prywatności (zamyka osobiste listy w szufladzie, ścisza głos podczas intymnej rozmowy). Świat cyfrowy to miejsce, którego przeciętny użytkownik dopiero się uczy.

[5] *Google CEO Eric Schmidt dismisses the importance of privacy*, https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy (11.05.2017). Słowa te brzmiały: „If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place?".

[6] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, Tychy 2015, s. 91.

[7] Ł. Kołodziejczyk, *Prywatność w Internecie*, dz. cyt., s. 35.

Środowisko internetu to miejsce skłaniające do rozpowszechniania danych, dla którego właściwsze jest rozgłoszenie jakiejś wiadomości niż utrzymanie jej w tajemnicy. Jednakże do prawdziwego „wyłudzania" informacji zaczęło dochodzić wraz z wejściem internetu w drugą fazę rozwoju (Sieć 2.0). Pojawiły się wtedy media, dla których istotą działania było gromadzenie danych o użytkownikach. Ich przedsięwzięcia biznesowe zostały oparte tylko na tym, czego dostarczyli użytkownicy.

Problem zagrożeń dla prywatności w kontekście rozwoju internetu i nowych mediów został wyraźnie dostrzeżony w połowie poprzedniego dziesięciolecia. Jego źródłem nie były jeszcze wtedy portale społecznościowe (w tym czasie jako raczkujące inicjatywy nie zdążyły objąć swoim zasięgiem całego globu), ale wyszukiwarki internetowe. Obserwatorzy świata mediów dostrzegli ich niezwykłą moc. Wpisywane zapytania poszczególnych użytkowników tych platform są rejestrowane, archiwizowane przynajmniej przez pewien czas. Mając dostęp do tych rejestrów, śledząc, czego dotyczą zapytania, jakie słowa się w nich pojawiają, można określić, kto był autorem tych zapytań. Wyszukiwarki stały się więc narzędziem do identyfikowania ludzi.

Analizując pytania, sformułowania wpisywane w wyszukiwarki, można było wyciągnąć wnioski co do problemów, z którymi boryka się wpisująca je osoba, określić jej przybliżony wiek, zainteresowania, status społeczny, ustalić, gdzie mieszka. Takie dane wystarczyły, aby następnie wskazać konkretnego człowieka.

Wyszukiwarki tego rodzaju informacji nie ujawniają publicznie (co nie znaczy jednak, że należy ograniczyć swój niepokój), jednak w połowie ubiegłego dziesięciolecia niefrasobliwym przedsiębiorstwem medialnym okazał się AOL, który opublikował rejestr zapytań za okres trzech miesięcy wszystkich swoich użytkowników. Rejestr stał się ciekawym materiałem do analizy, a dziennikarze gazety „New York Times", pisząc artykuł na ten temat, sami zidentyfikowali jedną osobę i poprosili o komentarz[8]. Bohaterka artykułu – okazała się nią sześćdziesięcioparoletnia wdowa – została przeproszona przez AOL, który nauczony skandalem obiecał przeciwdziałać wyciekom.

Istotą zagrożeń dla prywatności w opisanym przypadku nie był jednak tylko wyciek informacji. Problemem jest samo tworzenie rejestrów i to, co przedsiębiorstwa internetowe dysponujące wyszukiwarkami robią z tymi rejestrami. Nagle okazało się, że właściciele Google'a, Yahoo czy Binga zyskują dostęp do ogromnych zasobów informacji o ludziach, każdy z użytkowników staje się możliwą do opisania, scharakteryzowania jednostką. Na podstawie zapytań wpisywanych w wyszukiwarkę Google lub inny podmiot tworzy obraz człowieka, poznając jego zainteresowania, stan zdrowia, stan majątkowy, wykształcenie. Podstawowym założeniem Google'a i wielu innych przedsiębiorstw internetowych jest zatem uzyskiwanie o użytkowniku jak największej ilości informacji, aby go sprofilować, przypisać do określonej kategorii, zbudować jego szczegółową charakterystykę. Użytkownik traci w ten sposób swoją prywatność, a Google wykorzystuje zgromadzone informacje w dwóch celach. Gigant internetowy, mając profile swoich użytkowników, wie, jakie reklamy im podsunąć – reklamodawcy chcący skorzystać z jego usług dostają jako odbiorców te osoby, które na pewno zainteresują

[8] M. Barbaro, T. Zeller, *A face is exposed for AOL searcher no. 4417749*, „New York Times" 09.08.2006, http://www.nytimes.com/2006/08/09/technology/09aol.html (10.05.2017).

się ich ofertą (skoro Google ma o nich szeroką wiedzę, łatwo wyciąga wnioski odnośnie do ich potrzeb).

Dysponując taką wiedzą, Google może też zaoferować swoim użytkownikom wyszukiwanie spersonalizowane. Znając użytkowników, podsuwa im te wyniki wyszukiwania, które najbardziej będą odpowiadać oczekiwaniom[9]. Wyszukiwarka dąży do odgadnięcia intencji poszukującego informacji zapewniając jego satysfakcję z poszukiwań (znalazł to, co odpowiada jego potrzebom) oraz chęć zadawania kolejnych pytań (skoro wyszukiwarka – w mniemaniu użytkownika – jest skuteczna, będzie się starał znaleźć w niej odpowiedź na każde pytanie).

Warto w tym miejscu podkreślić fakt, że wyszukiwanie spersonalizowane nie jest usługą wprowadzaną tylko z myślą o wygodzie użytkownika. Rezultaty wyszukiwania dostosowane do potrzeb skłaniają go bowiem do jeszcze częstszego zadawania pytań, a zatem jeszcze większego ujawniania informacji o sobie. Więcej różnych zapytań użytkownika to następnie dokładniejszy profil opracowany przez algorytmy Google'a.

Google zatem w rzeczywistości swoimi zabiegami „prowokuje" do ujawniania jak największej ilości informacji o sobie. „Prowokowanie" do podawania danych, skłanianie i zachęcanie poprzez różne strategie, aby dużo o sobie ujawniać, jest jednak domeną portali społecznościowych na czele z Facebookiem. Jest to miejsca, gdzie użytkownik sam zakłada swój profil, sam zatem rozpoczyna gromadzenie informacji na swój temat. Nie ogranicza się w tym działaniu do własnej osoby. Tworzy listę znajomych, zaprasza osoby niekorzystające z serwisu do podobnej aktywności. Następuje więc szybko poszerzenie kręgu ludzi, którzy rozpoczynają prezentowanie siebie, podawanie informacji ze swojego życia. Elementy składowe każdego z profili są użytkownikom narzucone. Nie oni decydują, jaki jest jego układ. Mogą się dostosować i np. umieścić informacje o swoich zainteresowaniach, odwiedzanych miejscach, ulubionej muzyce. W momencie kiedy szeroko o tym informują, skłaniają swoich znajomych do podobnych poczynań (ci nie chcą być gorsi). Tego rodzaju struktura serwisu ma charakter samonapędzającego się mechanizmu, mówi się o występowaniu w serwisach społecznościowych efektu „śnieżnej kuli"[10].

Istotą funkcjonowania serwisu społecznościowego Facebook jest wzmacnianie owego mechanizmu samonapędzania się. Z tego też powodu serwis świadomie stosował słabe systemy kontroli dostępu do profili, objawiające się chociażby stosowaniem domyślnych ustawień prywatności dla tychże profili zakładających możliwość ich oglądania przez wszystkich użytkowników, chyba że ich właściciele sami wprowadzili ograniczenia. Chociaż trzeba zaznaczyć, że w ostatnich latach Facebook nieco zmienił swoją strategię. W odpowiedzi na rosnącą świadomość użytkowników chcących chronić swoją prywatność, portal wprowadził narzędzia dające większą kontrolę nad udostępnianymi danymi. Faktycznie jednak narzędzia te służą nie do zarządzania swoją prywatnością, ale do zarządzania widocznością danych o sobie. Użytkownicy bowiem ciągle nie wiedzą,

[9] S. Vaidhyanathan, *Googlization of everything (and why we should worry)*, Berkeley–Los Angeles 2011, s. 183.

[10] Ł. Kołodziejczyk, *Prywatność w Internecie*, dz. cyt., s. 34.

w jaki sposób informacje o nich są wykorzystywane przez samego Facebooka oraz firmy i dostawców usług, którzy z tym portalem współpracują[11].

Prowokowaniu do ujawniania kolejnych danych o sobie służy także odpowiedni sposób prezentowania nowo pojawiających się informacji dodawanych przez znajomych, nazwany News Feed. Wprowadzenie tego narzędzia całkowicie zmieniło sposób dostępu do informacji. News Feed (w polskiej wersji nazywany po prostu Aktualności) oznaczało, że dany użytkownik nie musiał odwiedzać profilu któregoś ze swoich znajomych, aby przeczytać lub obejrzeć najświeższe materiały[12]. Nowości jego znajomych były prezentowane na głównej stronie jego profilu. Nastąpiła więc agregacja na jego profil. Facebook zagwarantował tym sobie, że nic nie zostanie przeoczone, a pokazanie aktywności znajomych skłoni użytkownika do równie intensywnego dodawania informacji.

Internetowi giganci przejęli kontrolę nad siecią. Trudno jest używać tego medium bez korzystania z ich usług: poszukiwanie informacji w internecie utożsamiane jest z sięgnięciem po wyszukiwarkę Google, a kontaktowanie się w sprawach towarzyskich i zawodowych z logowaniem na Facebooku. Globalne firmy decydują o codziennym funkcjonowaniu miliardów ludzi, mają wpływ na to, co można znaleźć o tych ludziach w sieci, jak te informacje są gromadzone, do czego są wykorzystywane. Jednocześnie ich strategie jasno wskazują na odrzucenie ochrony prywatności i danych osobowych. Swobodny dostęp do informacji o ludziach pozwala bowiem realizować ich cele marketingowe.

2. Protesty przeciwko cyfrowemu śledzeniu

Na poczucie bezpieczeństwa, którego źródłem byłyby firmy internetowe, użytkownicy liczyć nie mogą. Zwykle wykorzystuje się więc drogę prawną, interwencje instytucji zajmujących się ochroną danych osobowych lub zbiorowe protesty ludzi niezgadzających się na nowe narzędzia lub zapisy w politykach prywatności serwisów.

Taka sytuacja zaistniała np. w 2010 roku, kiedy Facebook zliberalizował zapisy dotyczące polityki prywatności, doprowadzając do tego, że nagle profile użytkowników były widoczne nawet dla osób niezarejestrowanych w serwisie. W wyniku protestów nastąpiły zmiany poprawiające ochronę prywatności[13]. Facebook stał się jednak stałym tematem doniesień medialnych dotyczących różnych zabiegów i narzędzi, które pobierają dane zwykle nieświadomych tego użytkowników. Można było zatem dowiedzieć się, że wiele dostępnych na Facebooku aplikacji przesyła dane osób mających swoje profile przedsiębiorstwom zajmującym się reklamą w internecie, a Facebook śledzi swoich użytkowników (sprawdza, co robią w sieci, jakie odwiedzają strony) nawet kiedy wylogują się z serwisu. Portal był też oskarżany (zaprzeczał tym doniesieniom),

[11] K. Śliwowski, A. Obem, *Odzyskaj kontrolę w sieci. Odcinek III: ustawienia prywatności na Facebooku*, https://panoptykon.org/wiadomosc/odzyskaj-kontrole-w-sieci-odcinek-iii-ustawienia-prywatnosci-na-facebooku (02.05.2017).

[12] Ł. Kołodziejczyk, *Prywatność w Internecie*, dz. cyt., s. 37.

[13] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, dz. cyt., s. 93.

iż dysponuje narzędziami pozwalającymi zebrać dane z wiadomości tekstowych (sms) w smarfonach z Androidem, w momencie kiedy właściciele tych telefonów instalowali na urządzeniach wersję mobilną Facebooka[14].

Facebook był pozywany w związku z wykorzystaniem w celach komercyjnych funkcji „Lubię to". Na profilach użytkowników zaczęły bowiem pojawiać się reklamy produktów ze wskazaniem, że produkty te polubili właśnie ich znajomi. Nastąpiło więc wykorzystanie informacji o tych znajomych (informacji dotyczących ich polubień) do rekomendacji produktów bez ich wiedzy na ten temat[15].

Serwis miał też do czynienia z europejskimi organami. Na starym kontynencie ze względu na istnienie precyzyjnie sformułowanych norm prawnych dotyczących ochrony danych osobowych (w odróżnieniu od sytuacji w Stanach Zjednoczonych) wystąpienia przeciwko Facebookowi przybierały formę bardziej oskarżycielskich i potępiających (co nie znaczy, że bardziej skutecznych). Serwis został poddany osądowi irlandzkiego rzecznika ochrony danych osobowych (w Irlandii ma bowiem swoją siedzibę europejski oddział Facebooka), co było efektem protestów zainicjowanych przez ówczesnego studenta prawa z Wiednia, Maksa Schremsa. Schrems założył też stronę internetową Europe versus Facebook, na której przedstawiał swoje zarzuty. To on podnosił problem domyślnych ustawień prywatności w serwisie, przewidujących publiczną dostępność informacji na profilu oraz akceptowanie przez użytkowników oferowanych im nowych usług i narzędzi (chodzi o stosowanie systemu opt-out, zamiast korzystniejszego dla użytkowników systemu opt-in)[16].

Facebookiem zajęły się także niemieckie instytucje. Hamburski pełnomocnik ds. ochrony danych rozpoczął batalię przeciwko serwisowi w 2010 roku, kiedy okazało się, że portal gromadzi dane osób, które nigdy nie miały swojego profilu na Facebooku (zarzut ten podnoszono nie tylko Niemczech, był on często formułowany wobec Facebooka, mówiono o tworzeniu „profili cieni"). Docierał do informacji o nich, korzystając z wiedzy ludzi działających w tym serwisie. Wykorzystywał do tego między innymi dane zawarte w książkach adresowych poczty elektronicznej. Osoby nieobecne na portalu dostawały następnie zaproszenie do założenia tu swojego profilu. Nastąpiło więc wykorzystanie danych osobowych bez zgody ich właścicieli[17].

Hamburski pełnomocnik ds. ochrony danych zajął się również narzędziem udostępnionym przez serwis w 2012 roku, umożliwiającym oznaczanie na fotografiach udostępnianych na profilach znajdujących się na nich osób. Została tu wykorzystana technologia rozpoznawania twarzy. To narzędzie służyło do podpowiadania użytkownikowi, kto jest na zdjęciu, jak się nazywa, i proponowało automatyczne podpisanie tej osoby imieniem i nazwiskiem (czyli oznaczenie). Aby mogło ono zadziałać, Facebook musiał wcześniej stworzyć ogromną bazę danych biometrycznych użytkowników. Tworzenie takiej bazy to gromadzenie danych osobowych. Pełnomocnik podnosił, że działanie to zostało dokonane niezgodnie z prawem, było nielegalne, ponieważ Facebook nie zwrócił się

[14] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, dz. cyt., s. 96.

[15] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, dz. cyt., s. 98.

[16] *Objectives of „europe-v-facebook.org"*, http://europe-v-facebook.org/EN/Objectives/objectives.html1 (2.05.2017).

[17] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, dz. cyt., s. 131.

do właścicieli tych danych o zgodę na ich zebranie, przetworzenie i wykorzystanie. Tego rodzaju normy tymczasem regulują korzystanie z danych osobowych. Efektem poczynań hamburskiego pełnomocnika była rezygnacja Facebooka w 2013 roku z prowadzenia bazy biometrycznej dla Europejczyków i tym samym możliwości korzystania z narzędzi rozpoznawania twarzy[18].

W kontekście zagrożeń dla prywatności uwagę przyciągała także aktywność innych mediów. W odniesieniu do Twittera pod koniec 2013 roku pojawiło się doniesienie o szerszym niż do tej pory wykorzystywaniu danych swoich użytkowników dla potrzeb reklamowych. Medium zdecydowało o udostępnianiu ich adresów mailowych wszystkim firmom reklamowym. Zgodnie ze strategią przyjmowaną w tego rodzaju wypadkach zgoda na udostępnienie maila miała być domyślna. Jeśli jego właściciel miał inne zdanie na ten temat, musiał podjąć aktywność i tę zgodę wycofać[19].

W tym samym czasie wprowadzenie nowego przedsięwzięcia reklamowego ogłosił także serwis społecznościowy Google+. W rekomendacjach reklamowych dla użytkowników miał wykorzystywać zdjęcia oraz nazwiska ich znajomych. Osoby rekomendujące miały jednak możliwość decydowania, do kogo te reklamy mają trafić[20].

Protesty i pozwy sądowe zmuszają firmy internetowe do modyfikowania i uwzględniania rozwiązań dobrych dla użytkowników. Trudno oczekiwać, aby wpłynęły one jednak na całościową zmianę ich strategii, wprowadzenie ograniczeń i bezpiecznych mechanizmów w momencie korzystania z danych osobowych. Zresztą cyfrowa inwigilacja nie odnosi się tylko do przedsięwzięć biznesowych. Pojawiają się głosy, że o wiele groźniejsza może być inwigilacja prowadzona przez państwo, chociaż w tym wypadku śledzenie obywateli również w przeważającym zakresie odbywa się przy użyciu danych zgromadzonych przez firmy internetowe lub poprzez narzędzia opracowane przez te firmy. Działalność państwa podejmowana w słusznym celu zapewnienia bezpieczeństwa obywateli zaczyna przybierać formę masowej inwigilacji, nieuzasadnionego sprawdzania każdej aktywności w internecie. Pokazuje to afera PRISM: okazało się, że amerykańska Agencja Bezpieczeństwa Narodowego (NSA), a także podobne instytucje z innych państw uzyskiwały dostęp do ogromnych zasobów danych o ludziach zgromadzonych przez firmy internetowe i telekomunikacyjne. Przy tej okazji dochodziło do ogromnych nadużyć. Fakty ujawnił w czerwcu 2013 roku pracownik NSA Edward Snowden[21]. Tego rodzaju nieograniczona możliwość inwigilacji wydaje się spełnieniem czarnych scenariuszy. Jeszcze bowiem osiem lat przed aferą z programem PRISM protest wywoływała nawet możliwość ujawnienia przez Google rejestru zapytań swoich użytkowników wpisywanych do wyszukiwarki, gdy takie żądanie wysunął Departament Sprawiedliwości USA[22].

[18] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, dz. cyt., s. 134.

[19] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, dz. cyt., s. 100.

[20] K. Łuszczek, *Wolność i kontrola w internecie drugiej fali*, dz. cyt., s. 101.

[21] *NSA Prism program taps in to user data of Apple, Google and others*, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (10.05.2017).

[22] *Trackmenot. Background*, https://cs.nyu.edu/trackmenot/#why (03.05.2017). W efekcie sprzeciwu firmy internetowej tłumaczącej, że ujawnienie zapytań naruszy zaufanie do Google ze strony użytkowników i wywoła efekt mrożący w ich aktywności, Federalny Sąd Okręgowy zrezygnował z żądań w tym zakresie. Firma musiała zrealizować żądanie podania danych, ale w innym obszarze, nie zapytań.

Obecnie dążenie do cyfrowej inwigilacji oraz wykorzystywania baz danych serwisów społecznościowych i innych platform do totalnego nadzoru wydaje się bardzo realne.

3. Asymetria władzy i informacji

Powyższe analizy rysują bardzo pesymistyczny obraz sytuacji, w jakiej znajduje się przeciętny użytkownik internetu i technologii cyfrowych. Stając naprzeciwko firm o zasięgu globalnym i rządów państw zainteresowanych śledzeniem jego każdego ruchu, nawet jeśli zjednoczy się z innymi, nie zmusi drugiej strony do uwzględnienia swoich interesów. Relacje między użytkownikami a podmiotami biznesowymi i państwowymi charakteryzuje nierówność, którą Helen Nissenbaum i Finn Brunton nazwali asymetrią władzy i asymetrią informacji. Badacze o tych pierwszych mówią jako o „słabych". Przedsiębiorstwa internetowe i rządy państw dysponujące narzędziami inwigilacji to „silni". Z tego układu wynika niepewność, strach, brak zaufania wobec świata cyfrowego: nie wiadomo, co zrobią giganci decydujący o jego kształcie, co czeka w nim przeciętnego użytkownika.

Przedstawiając problem inwigilacji, Brunton i Nissenbaum nie ograniczają się do opisu form prowadzonych za pośrednictwem portali społecznościowych i korzystających z ich usług agencji rządowych. Nie wystarczy porzucić korzystanie z Facebooka i Google'a, aby uchronić się przed śledzeniem. Ludzie doświadczają asymetrii władzy, ponieważ są niejako zmuszani do poddania się tej dysponującej różnymi środkami inwigilacji. Nie mogą zrezygnować z narzędzi, poprzez które są śledzeni. Inwigilacja odbywa się także wtedy, gdy ludzie przemierzają miasto (monitoring uliczny i w budynkach), dysponują kartami kredytowymi (można prześledzić ich historię zakupów, transakcji), następuje określenie ich dróg przemieszczania się poprzez wyznaczenie położenia ich telefonu. Inwigilacji dokonują nie tylko wielkie firmy internetowe, ale także sklepy internetowe, banki, firmy ubezpieczeniowe, które również śledzą poczynania swoich klientów w Sieci i opracowują ich profile. Można oczywiście wyobrazić sobie funkcjonowanie poza dużymi centrami, bez używania mediów, ale wtedy nie byłoby możliwe życie według pewnych ugruntowanych standardów z legalną pracą zarobkową (pensje otrzymuje się bowiem poprzez bezgotówkowe przelewy na konto internetowe, co już stanowi pewien ślad cyfrowy).

Poważniejsze konsekwencje dla użytkowników wiążą się jednak z asymetrią informacyjną (lub inaczej poznawczą). Przede wszystkim ludzie nie wiedzą, jakie dane o nich są gromadzone, kto je gromadzi i w jakim celu. Nawet jeśli mają na ten temat wiedzę, nie dysponują gwarancją bezpiecznego ich użycia w przyszłości. Bazy danych przecież nie znikną, a trudno przewidzieć, czy kiedyś nie nastąpi ich przejęcie przez inny podmiot (ponieważ np. pierwotny właściciel baz danych zbankrutował)[23].

[23] F. Brunton, H. Nissenbaum, *Zmyl trop. Na barykadach prywatności w Sieci. Przewodnik*, przekł. J. Konieczny, Warszawa 2016, s. 123.

Zbierane dane są poddawane analizie, tworzy się specjalistyczne oprogramowania do ich przetwarzania, analizowania, powstają algorytmy, dzięki którym na podstawie, wydawałoby się, mało znaczących informacji wyciąga się wnioski dotyczące cech osobowościowych, stanu zdrowia, statusu społecznego. Dane są przydatne w celach marketingowych. Na podstawie wyników tych analiz następuje przypisywanie ludzi do określonych kategorii. Decydująca jest tu kwestia ich przyszłych decyzji zakupowych, czy staną się klientami określonych usług lub produktów (i dlatego trzeba im podsunąć reklamy droższych, lepszych, ambitniejszych ofert), czy też są w tym zakresie mało wartościowi.

Asymetria informacyjna zaznacza się nie tylko w obszarze przetwarzania danych służących określeniu przyszłych decyzji konsumenckich. Przyszłe decyzje ludzi chce też określić państwo. W wypadku rządów chodzi o przewidywanie głównie działań przestępczych. W odniesieniu do tego zagadnienia pojawią się sformułowania „modelowanie predyktywne" czy „oprogramowanie predyktywne". Są opracowywane algorytmy, które z pozoru błahych informacji przewidują zachowania ludzi. „Systemy predyktywne korzystają z wielkich baz danych do tworzenia przewidywań na temat ludzkiej aktywności: przygotowują prognozy, trafne lub nietrafne, które są później wykorzystywane do podejmowania decyzji i tworzenia represyjnych rozwiązań, w wyniku czego ludzie są karani lub nagradzani za rzeczy, których jeszcze nie zrobili"[24]. Do zilustrowania niebezpieczeństwa może posłużyć raczej skrajny przypadek, kiedy ktoś zostaje zatrzymany na lotnisku, ponieważ oprogramowanie predyktywne podało, że może on dokonać zamachu.

Asymetria informacyjna polega tu nie tylko na braku wiedzy ludzi na temat danych, które są wykorzystywane przez władze do modelowania ich zachowań. Gdy już predyktywne modelowanie zakończy się jakimś postanowieniem wobec danego człowieka, skomplikowanie tych procedur matematycznych i informatycznych nie pozwoli na określenie, dlaczego trzeba zrealizować właśnie takie postępowania (co faktycznie zdecydowało, że ktoś został uznany za terrorystę). Człowiek zostanie poddany woli zautomatyzowanego systemu, którego decyzje nie są możliwe do wyjaśnienia w kategoriach ludzkiego rozumowania.

Wywody Bruntona i Nissenbaum można uzupełnić o rozważania Katarzyny Szymielewicz, która wskazuje, że w Europie, inaczej niż w Stanach Zjednoczonych, istnieje system prawny pozwalający walczyć o zachowanie prywatności. Użytkownik musi jednak być świadomy takich możliwości oraz charakteryzować się wytrwałością. To jedna droga zmagania się z gigantami decydującymi o kształcie cyfrowego świata. Druga droga to nauczenie się korzystania z bezpiecznego Internetu. Wcale bowiem nie trzeba korzystać z usług przedsiębiorstw, kiedy chce się wysłać maila lub opublikować jakąś informację. Można np. szyfrować maile, zainstalować wtyczki do przeglądarek blokujące reklamy i śledzące nas „ciasteczka" czy skorzystać z Wirtualnych Sieci Prywatnych (VPN). Nie jest więc tak, że użytkownik jest pozostawiony na pastę wielkich korporacji i rządów. Jeśli tylko czuje taką potrzebę, już teraz może się przed nimi bronić[25].

[24] F. Brunton, H. Nissenbaum, *Zmyl trop*, dz. cyt., s. 127.

[25] K. Szymielewicz, *Słowo wstępne. Jeszcze możemy odzyskać kontrolę*, w: F. Burton, H. Nissenbaum, *Zmyl trop*, dz. cyt., s. 17.

4. Strategia zaciemniania

Koncepcja Bruntona i Nissenbaum jest jednak czymś więcej niż tylko prostą strategią obrony przed inwigilacją. Zaciemnianie, które proponują w reakcji na wystąpienie asymetrycznych relacji między użytkownikiem a biznesowymi i państwowymi gigantami, ma pozwolić ochronić prywatność, ale ma także wyrazić protest przeciwko nierówności, zaznaczyć bunt, wywołać szkody, uczynić gromadzone dane bezużytecznymi. W tej strategii chodzi o pokazanie siły mimo słabości i niezgodę na obecny kształt cyfrowego świata.

Zaciemnianie dokonywane przez użytkowników to zatem normalne korzystanie z usług mediów cyfrowych przy równoczesnym wytwarzaniu szumu informacyjnego, wprowadzeniu przez tych użytkowników w obszar ich aktywności internetowej pewnych elementów, informacji (nieprawdziwych, mylących, dezorientujących), które spowodują, że gromadzone dane będą mniej wiarygodne, zagmatwane, na ich podstawie nie będzie możliwe wytworzenie prawdziwego obrazu/profilu tychże użytkowników. Autorzy tej koncepcji wybrali termin „zaciemnianie" (ang. *obfuscation*), ponieważ kojarzy im się z niejasnością, nieczytelnością i odróżniają go od metod mających wywołać zniknięcie, wymazanie ze świata cyfrowego[26].

Przykładem zastosowania powyższej strategii jest używanie programu TrackMeNot. Narzędzie będące rozszerzeniem przeglądarki służy do zafałszowania obrazu użytkownika zbudowanego na podstawie jego zapytań wpisywanych w wyszukiwarkę. Użytkownik może oczywiście swobodnie zadawać pytania wyszukiwarce Google lub innej. W tym samym czasie zainstalowane narzędzie będzie na własną rękę generować inne zapytania (zwykle jednak takie, które ze sporym prawdopodobieństwem mógłby zadać używający TrackMeNot). Do rejestru wyszukiwarki trafią więc zarówno rzeczywiste pytania użytkownika, jak i te wygenerowane tylko po to, żeby „zaciemnić" obraz tego, co faktycznie go interesuje. (W długiej liście zapytań trudno będzie określić, co jest autentyczne, a co podsunęło oprogramowanie)[27].

Cyfrowa inwigilacja jest w dużej mierze prowadzona po to, aby uzyskać informacje o preferencjach zakupowych użytkownika. Następuje śledzenie jego aktywności, aby sprawdzić, jakie strony odwiedza, w które klika reklamy. Te działania czyni bezużytecznymi przeglądarkowy dodatek AdNauseam wraz z nakładką Adblock Plus. Kiedy użytkownik serfuje po sieci, oprogramowanie klika we wszystkie napotkane reklamy. Gdy on sam zainteresuje się jakąś reklamą i ją otworzy, ten fakt zginie wśród ogromnej liczby innych oznaczających klikanie w reklamy sygnałów[28].

W wyniku gromadzenia o użytkownikach informacji, tworzenia ich profili i na tej podstawie podsuwania wyników w wyszukiwarce i dostosowywania reklam następuje personalizacja internetu. Każdy użytkownik, sięgając po zasoby sieciowe, otrzymuje inny zestaw informacji, widzi inne bannery reklamowe. Zjawisko to określane jest

[26] F. Brunton, H. Nissenbaum, *Zmyl trop*, dz. cyt., s. 116.
[27] *Trackmenot*, https://cs.nyu.edu/trackmenot/ (11.05.2017).
[28] F. Brunton, H. Nissenbaum, *Zmyl trop*, dz. cyt., s. 216.

jako zamykanie internautów w filtrowych bańkach. Finn Brunton i Helen Nissenbaum proponują rozwiązanie, które pozwoli wyzwolić się ze swojej spersonalizowanej bańki, zaburzyć proces profilowania. Ma ono postać gry komputerowej Vortex[29].

W tym, że ludziom można przypisać określoną internetową tożsamość, mają swój udział „ciasteczka" zostawiane na urządzeniach każdego z użytkowników w momencie odwiedzania poszczególnych stron internetowych. „Ciasteczka" zbierają informacje o preferencjach użytkowników. Istotą wieloosobowej gry Vortex jest wymienianie się „ciasteczkami" z innymi. Uzyskanie „ciasteczek" innego gracza powoduje, że sieć identyfikuje daną osobę jako właśnie tego innego gracza. Gra pozwala więc wymieniać się *de facto* internetowymi tożsamościami. Można uzyskiwać dostęp do wielu takich internetowych tożsamości. Oznacza to w praktyce szerszy dostęp do internetowych zasobów (nie tylko tych przewidzianych dla profilu danej osoby).

Aby pomieszać szyki systemom inwigilującym ludzi, nie zawsze konieczne jest użycie oprogramowania. Wystarczy odpowiednia strategia postępowania. Autorzy koncepcji zaciemniania podają przykład programisty Kevina Ludlowa, który chcąc zaprotestować przeciwko postępowaniu Facebooka skłaniającego ludzi do ujawniania większej liczby informacji, niż wynika to z ich zwyczajów, sam wprowadził do swojego profilu ogromną ich liczbę. Dane te były nieprawdziwe (Ludlow pisał o swoich ślubach, rozwodach, narodzinach dzieci, chorobach i podróżach, a wszystko to miało wydarzyć się w ciągu kilku miesięcy), co dla każdego czytającego było łatwe do odgadnięcia. Nie od odgadnięcia jednak jest to dla algorytmów śledzących aktywność użytkowników. Ich praca, w przypadku Ludlowa, poszła więc na marne[30].

Inny sposób na uniemożliwienie Facebookowi dostępu do informacji o użytkowniku to zastosowanie wtyczki FaceCloak. Gdy w momencie tworzenia profilu i wprowadzania informacji o sobie używa się FaceCloak, wtyczka, jeśli dane zostaną opatrzone statusem prywatne, spowoduje zablokowanie ich wysłania na serwery Facebooka, a zamiast tego wyśle je na całkiem inny serwer. Gdy znajomi osoby rejestrującej się w ten sposób będą chciały obejrzeć jej profil, dane zostaną pobrane z tego serwera i wyświetlone na profilu. Tego rodzaju działanie będzie nie do wykrycia dla Facebooka, gdyż z jego punktu widzenia profil nie zostanie pusty. FaceCloak wypełnia pola profilu sfabrykowanymi informacjami[31].

Realizując strategię zaciemniania, można także podjąć działania o szerszym zasięgu. Taką opcję oferuje system informatyczny umożliwiający tworzenie sklonowanej tożsamości danego użytkownika. Usługa klonowania pozwala zaciemniać jego obraz nie tylko w określonych miejscach cyfrowego świata (czyli nie tylko na Facebooku czy podczas korzystania z Google), ale w odniesieniu do całościowej jego aktywności.

System informatyczny najpierw określa zakres zainteresowań osoby, której klon ma zostać stworzony, bada rodzaj działań w internecie, tworzy cyfrowy profil. Klon użytkownika musi bowiem przejąć przynajmniej część informacji o rzeczywistej osobie,

[29] F. Brunton, H. Nissenbaum, *Zmyl trop*, dz. cyt., s. 99.
[30] F. Brunton, H. Nissenbaum, *Zmyl trop*, dz. cyt., s. 102.
[31] F. Brunton, H. Nissenbaum, *Zmyl trop*, dz. cyt., s. 104.

naśladować jej zwyczaj w cyfrowym świecie. Tylko wtedy sklonowana tożsamość będzie wiarygodna.

Do tworzonej tożsamości dodaje się też dużo nieprawdziwych informacji, tworzy się internetowe konto bankowe, konto mailowe. Następnie stworzony klon podejmuje własną aktywność (zwykle ta aktywność znajduje swoje uzasadnienie we wcześniejszych poczynaniach rzeczywistego użytkownika, w jakiś sposób wynika z tych poczynań), np. śledzi na Twitterze konto jakiejś instytucji czy osoby, odwiedza strony internetowe, zapisuje się na listy mailingowe. W miarę upływu czasu ta aktywność może jednak zacząć odbiegać od tego, co ewentualnie mógłby zrobić rzeczywisty użytkownik. Klon zaczyna żyć własnym życiem.

5. Prawo chroniące e-prywatność

Brunton i Nissenbaum proponują strategię zaciemniania, ponieważ nie widzą innego sposobu na ochronę przed inwigilacją. W Europie istnieje dążenie do wprowadzenia prawa, które ochroni przed tym śledzeniem. Czy ochroni w sposób skuteczny? Pytanie pozostaje otwarte ze względu na fakt, że nowe prawo dopiero się kształtuje. Projekt wywołuje co rusz wątpliwości w kręgach ekspertów zainteresowanych przeciwstawieniem się inwigilacji. Swój wpływ na formowanie prawa zaznaczają bowiem także przedsiębiorstwa internetowe chcące mieć cały czas dostęp do informacji o swoich użytkownikach.

W 2002 roku Unia Europejska wprowadziła dyrektywę o prywatności i łączności elektronicznej[32], regulującą kwestię ochrony prywatności w internecie. Zmiany, które od tego czasu zaszły w obrębie komunikacji internetowej, potrzebują nowej regulacji. Dyrektywę ma zastąpić rozporządzenie w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej. Projekt rozporządzenia w styczniu 2017 roku przestawiła Komisja Europejska.

Założenia nowej regulacji mówią o objęciu nowymi przepisami wszystkich form komunikacji elektronicznej. Jeśli jakaś usługa oferuje możliwość komunikowania się, nawet gdy nie jest to jej główne zadanie, powinna podlegać rozporządzeniu o e-prywatności. Chodzi tu między innymi o gry lub inne aplikacje, w których komunikowanie się ma znaczenie drugorzędne, ale jednak jest możliwe[33].

Rozporządzenie ma chronić nie tylko treści, które użytkownicy rozpowszechniają za pomocą sieci internetowej. Obecny rozwój technologiczny umożliwia pobieranie danych o użytkownikach, o których oni sami często nie wiedzą, że są możliwe do pobrania. Chodzi tu np. o dane dotyczące lokalizacji urządzenia, którym się posługują. Tego rodzaju informacje to metadane. W założeniach nowego prawa jest mowa o tym,

[32] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności).

[33] *Uwagi Fundacji Panoptykon dotyczące projektu rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej*, https://panoptykon.org/sites/default/files/publikacje/panoptykon_uwagi_eprywatnosc_17.01.2017.pdf (12.05.2017).

że regulacje będą zapewniać ochronę dla metadanych na równi z ochroną dla treści, które użytkownicy świadomie i aktywnie umieszczają w sieci.

Aby nowe prawo spełniło swoje funkcje, musi zawierać regulacje skutecznie zapewniające poufność i ochronę przed bezprawnym przechwyceniem dla wszystkich treści i danych, które tej poufności potrzebują. Oczywiście analiza danych użytkowników będzie możliwa, ale tylko w sytuacji, kiedy przewiduje to prawo, kiedy ich właściciel wyraża zgodę lub kiedy występuje uzasadniony interes administratora danych.

Istotne założenie nowego prawa wskazuje, że ochronę dla treści trzeba zapewniać na poziomie urządzeń i usług, które służą do tworzenia i rozpowszechniania tych treści[34]. Oznacza to, że każde urządzenie lub usługa powinno w swoich ustawieniach domyślnych dotyczących prywatności mieć opcję uniemożliwiającą pobieranie poufnych danych. To użytkownik mógłby dopiero zdecydować, że chce udostępniać swoje dane lub treści. Musiałby wtedy dokonać zmian w ustawieniach prywatności. To on zatem podejmowałby świadomą decyzję, np. że chce, aby Google pobierało jego historię zapytań i na tej podstawie w odpowiedziach na kolejne zapytania podsuwało wyniki najbardziej mu odpowiadające.

Trudno jednak przewidzieć, jak obszar ochrony e-prywatności zostanie uregulowany w szczegółach. Swoje uwagi przedstawili eksperci, którzy analizowali projekt rozporządzenia na zlecenie Parlamentu Europejskiego. Zwrócili uwagę na fakt, iż proponowane przepisy nie chronią przed ustalaniem lokalizacji, dróg przemieszczania się użytkowników posługujących się urządzeniami wykorzystującymi WiFi lub Bluetooth. Takie śledzenie może być przeprowadzane przez firmy lub instytucje, np. w centrach handlowych lub lotniskach.

Śledzeniu w internecie będzie można przeciwdziałać poprzez wprowadzenie odpowiednich ustawień w przeglądarkach internetowych. O te ustawienia będzie musiał jednak zadbać każdy z użytkowników. Rozwiązanie to nie sprzyja ochronie prywatności i zostało skrytykowane przez ekspertów. Przeglądarki w swoich domyślnych ustawieniach powinny mieć opcję niepozwalającą na jakiekolwiek śledzenie. Użytkownik mógłby ewentualnie sam zmodyfikować ustawienia. Eksperci zwrócili uwagę, że nastąpiło w tym miejscu złamanie założeń, które przyświecały reformie prawa dotyczącego e-prywatności zawierającej się w sformułowaniu „privacy by design"[35].

Zdaniem ekspertów należałoby ograniczyć zjawisko „cookie walls", czyli blokowania dostępu do stron internetowych, jeśli użytkownik nie zaakceptuje wcześniej śledzących go „ciasteczek"[36]. „Cookie walls" nie mogłyby stosować strony, które zajmują się ważnymi i publicznymi tematami, np. zdrowiem, oraz monopoliści typu Facebook.

---

[34] K. Szymielewicz, *Poznaliśmy projekt unijnego rozporządzenia o e-prywatności. Co ma się zmienić?*, https://panoptykon.org/wiadomosc/poznalismy-projekt-unijnego-rozporzadzenia-o-e-prywatnosci-co-ma-sie-zmienic (12.05.2017).

[35] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *An assessment of the commission's proposal on privacy and electronic communications*, s. 93, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf (12.05.2017).

[36] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *An assessment of the commission's proposal on privacy and electronic communications*, dz. cyt., s. 87.

Przepisy rozporządzenia powinny także zakazać sytuacji, w których, aby skorzystać z usług firmy internetowej (np. skorzystać z portalu Facebook) trzeba się bezwzględnie zgodzić na pobieranie i analizę treści, które użytkownik wytworzy dzięki tej usłudze[37].

Literatura

Barbaro M., Zeller T., *A face is exposed for AOL searcher no. 4417749*, „New York Times" 09.08.2006, http://www.nytimes.com/2006/08/09/technology/09aol.html (10.05.2017).

Brunton F., Nissenbaum H., *Zmyl trop. Na barykadach prywatności w Sieci. Przewodnik*, przekł. J. Konieczny, Warszawa 2016.

Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *An assessment of the commission's proposal on privacy and electronic communications*, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf (12.05.2017).

Google CEO Eric Schmidt dismisses the importance of privacy, https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy (11.05.2017).

Kołodziejczyk Ł., *Prywatność w Internecie*, Warszawa 2014.

Łuszczek K., *Wolność i kontrola w internecie drugiej fali*, Tychy 2015.

Niklas J., *Unijny projekt ochrony prywatności w Internecie potrzebuje wzmocnienia?*, https://panoptykon.org/wiadomosc/unijny-projekt-ochrony-prywatnosci-w-internecie-potrzebuje-wzmocnienia (12.05.2017).

Nissenbaum H., *Privacy as Contextual Integrity*, „Washington Law Review" 79 (2004), s. 101–139, https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (10.05.2017).

NSA Prism program taps in to user data of Apple, Google and others, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (10.05.2017).

Objectives of „europe-v-facebook.org", http://europe-v-facebook.org/EN/Objectives/objectives.html (2.05.2017)

Szymielewicz K., *Poznaliśmy projekt unijnego rozporządzenia o e-prywatności. Co ma się zmienić?*, https://panoptykon.org/wiadomosc/poznalismy-projekt-unijnego-rozporzadzenia-o-e-prywatnosci-co-ma-sie-zmienic (12.05.2017)

Szymielewicz K., *Słowo wstępne. Jeszcze możemy odzyskać kontrolę*, w: F. Burton, H. Nissenbaum, *Zmyl trop. Na barykadach prywatności w Sieci. Przewodnik*, przekł. J. Konieczny, Warszawa 2016.

Śliwowski K, Obem A., *Odzyskaj kontrolę w sieci. Odcinek III: ustawienia prywatności na Facebooku,* https://panoptykon.org/wiadomosc/odzyskaj-kontrole-w-sieci-odcinek-iii-ustawienia-prywatnosci-na-facebooku (2.05.2017).

Trackmenot. Background, https://cs.nyu.edu/trackmenot/#why (3.05.2017).

[37] J. Niklas, *Unijny projekt ochrony prywatności w Internecie potrzebuje wzmocnienia?*, https://panoptykon.org/wiadomosc/unijny-projekt-ochrony-prywatnosci-w-internecie-potrzebuje-wzmocnienia (12.05.2017).

Uwagi Fundacji Panoptykon dotyczące projektu rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej, https://panoptykon.org/sites/default/files/publikacje/panoptykon_uwagi_eprywatnosc_17.01.2017.pdf (12.05.2017).

Vaidhyanathan S., *Googlization of everything (and why we should worry)*, Berkeley–Los Angeles 2011.