Społeczeństwo i Edukacja
Society and Education

Wydawca / Publisher:
Instytut Studiów
Międzynarodowych
i Edukacji HUMANUM
www.humanum.org.pl

29 (2) 2018
ISSN 1898-0171

Leszek Porębski
Katedra Politologii i Historii Najnowszej
Wydział Humanistyczny AGH

Cyfrowy świat na nowo zdefiniowanego bezpieczeństwa. Prywatność jako ofiara rewolucji informacyjnej / *Digital world of redefined security. Privacy as the victim of the information revolution*

Abstract
Privacy has been one of the major democratic values since the origin of liberal democracy. The information revolution and rapid increase of accessible information resulted in the necessity of redefinition of the privacy concept. Privacy has lost its status of the guarantee of personal liberty and turned out to be the secondary value, often regarded as commodity. Various forms of privacy intrusion (watching, intercepting, reading, interpreting) are highly accepted as the cost of being the part the digital world. It implied also the emergence of the new model of personal security. We no longer need privacy to feel secure. Consumption-oriented identity within which everything is public and common seems to overshadow perception of self as autonomous – self-dependent and sometimes solitary – citizen.

Key words: privacy, security, liberal democracy, democratic values, information revolution, ICT, social media.

1. WPROWADZENIE

Chęć bycia bezpiecznym jest niezbędnym elementem funkcjonowania człowieka, niezależnie od czasu, okoliczności, reprezentowanego kręgu kulturowego czy zajmowanej pozycji społecznej. W najbardziej bodaj znanej we współczesnej psychologii teorii potrzeb ludzkich, autorstwa Abrahama Maslowa zespół potrzeb bezpieczeństwa ma charakter podstawowy, ujawniający się bezpośrednio po zaspokojeniu potrzeb fizjologicznych (Maslow 1954: 39-43)[1]. W tym sensie poczucie bezpieczeństwa stanowi warunek konieczny dla przynoszącej choćby elementarną satysfakcję ludzkiej egzystencji.

1 Por. też: Maslow (1986, 1990)

Sposób definiowania kategorii bezpieczeństwo nie ma jednak charakteru w pełni zobiektywizowanego i wykracza poza perspektywę stricte psychologiczną. Istotną rolę w odpowiedzi na pytanie co oznacza „bycie bezpiecznym" odgrywają dominujące w dyskursie publicznym wartości. Internalizując konkretną wizję, tego co ważne – zarówno w wymiarze indywidualnym, jak i społecznym – jednostki tworzą swoją własną hierarchię wartości, przypisując konkretnym kwestiom określoną rangę. W tradycji liberalnej demokracji wysoką pozycję w tak rozumianej hierarchii zajmowała zawsze ochrona prywatności. Kreowanie autonomii wobec państwa i instytucji publicznych stało się na tyle ważnym aspektem przemian demokratycznych zachodzących w XIX wieku, że zbudowane na tej podstawie prawo do prywatności okazało się jednym z podstawowych wymiarów obywatelskiego poczucia bezpieczeństwa. „Być bezpiecznym" zaczęło od tego momentu oznaczać w równym stopniu zapewnienie ochrony przed napastnikami czy agresorami dzięki aktywnej pomocy ze strony instytucji państwa, jak i prawo do wyłączenia znaczących sfer życia od ingerencji tych samych instytucji.

Znaczenie tak rozumianej sfery prywatności było oczywiście redefiniowane przez cały wiek XX. Wydaje się jednak, że impulsem najsilniej wymuszającym konieczność ponownej refleksji nad rolą odgrywaną przez prawo do prywatności, także w kontekście poczucia bezpieczeństwa, stała się rewolucja informacyjna. Poprzez rozwój technologii informacyjnych i komunikacyjnych (*information and communication technologies* – ICT) intensywnie zmieniła ona rzeczywistość społeczną, począwszy od ostatnich dekad ubiegłego stulecia. W tym kontekście podstawowe znaczenie miało przede wszystkim powstanie i rozpowszechnienie serwisów społecznościowych, związane z udostępnianiem przez ich użytkowników na masową skalę danych wcześniej uznawanych za prywatne. W połączeniu z nowymi narzędziami technicznymi pozwalającymi na świadome ingerowanie w prywatność, jakie rozwój ICT dał do ręki instytucjom państwa i firmom komercyjnym, stworzyło to zupełnie nowe wyzwania dla tradycyjnych wartości demokratycznych.

Podstawowym celem tego tekstu jest próba uchwycenia dynamiki przemian sposobu rozumienia prawa do prywatności i poczucia bezpieczeństwa w związku z rozwojem ICT. Czy prywatność przestała być wartością cenioną powszechnie? Na ile dyfuzja tradycyjnie rozumianego prawa do prywatności jest równoznaczna z osłabieniem indywidualnego bezpieczeństwa? Czy w świecie nowych technologii państwo jest zagrożeniem czy obrońcą indywidualnego bezpieczeństwa? Wszystkie te kwestie mają charakter wielowymiarowy i trudno je jednoznacznie rozstrzygnąć. Poświęcenie im chwili refleksji wydaje się jednak warunkiem koniecznym dla zrozumienia otaczającej nas i podlegającej gwałtownym przemianom społecznej rzeczywistości.

2. PRYWATNOŚĆ JAKO WARTOŚĆ W DEMOKRACJI

O ile wśród badaczy panuje względna zgoda co do faktu, że prawo do prywatności stanowi jedną z podstawowych wartości demokratycznych, o tyle znacznie trudniej o porozumienie w sprawie samej definicji terminu prywatność. Dzieje się tak zapewne dlatego, że pojęcie to: „jest używane do oznaczania szerokiego zakresu różnych potrzeb obejmujących kontrolę nad informacjami dotyczącymi siebie samego, autonomię w sferze reprodukcji, dostępu do miejsc i do ciała, zachowywania tajemnicy i osobistego rozwoju" (Kemp i Moore 2007: 58). Opisana sytuacja sprawia, że nie można wskazać jednego kryterium decydującego np. o granicach prywatności,

a w konsekwencji używając tego samego terminu różni ludzie odnoszą się do odrębnych aspektów rzeczywistości.

Dla uporządkowania funkcjonujących równolegle definicji prywatności zazwyczaj przypisuje się je do jednej z dwóch podstawowych koncepcji tego pojęcia. Są to teoria kontroli i teoria ograniczonego dostępu. W ramach tej pierwszej to osoba zainteresowana, poprzez swoje subiektywne decyzje nadzoruje i steruje zakresem, w jakim inni ludzie mają dostęp do jej sfery prywatnej. Oczywiście oznacza to w konsekwencji, że różni ludzie zakreślają obszar swej prywatności w odrębny sposób. Z kolei idea ograniczonego dostępu odwołuje się do norm i praw ograniczających wgląd innych w osobiste sprawy jednostki. Prywatność jest więc tu rodzajem moralnego zobowiązania. Ma ono charakter zobiektywizowany i dotyczy każdego człowieka, jako swego rodzaju regulator relacji interpersonalnych i społecznych (Fuchs 2011: 222-224).

Teoria ograniczonego dostępu jest częścią klasycznej tradycji liberalnej, a za osobę, która jako pierwsza sformułowała jej podstawy zazwyczaj uznaje się Johna Stuarta Milla. Już w połowie XIX wieku zarysował on istotę prywatności, rozumianej jako przestrzeń wolna od ingerencji innych. Jej istnienie jest nieuniknioną konsekwencją akceptacji godności jako podstawowego atrybutu osoby ludzkiej (Mill 1965, 1966).

Walka o prawo do prywatności była więc częścią batalii, jaką toczyli liberałowie przez całe XIX stulecie. Stawką było w niej stworzenie katalogu podstawowych praw jednostki, który miał gwarantować stan wcześniej zupełnie nieznany – indywidualną autonomię. Prywatność, ale także inne prawa – takie jak wolność wypowiedzi – wyznaczać miały granice ingerencji instytucji państwa, ale także innych ludzi w funkcjonowanie obywatela. Przestrzeń autonomii jednostki stała się więc podstawowym elementem indywidualnego poczucia bezpieczeństwa. Czuć się bezpiecznie w relacjach społecznych oznaczało od czasu budowy podstaw dziewiętnastowiecznej liberalnej demokracji nie tylko gwarancje bycia chronionym przez instytucje reprezentujące państwo przed fizyczną napaścią czy przestępstwem. Równie istotne było prawo do „pozostawienia w spokoju" przez innych (w tym te same instytucje państwowe) w sytuacjach i okolicznościach, opisanych przez normy prawne i poddanych interpretacji samej zainteresowanej osoby. Prywatność jako wartość ma więc w tradycji zachodniej wyraźnie zaznaczony aspekt prawny, ale jest zakorzeniona w podstawowych potrzebach egzystencjalnych i psychologicznych. Stanowi przestrzeń potrzebną do osobowego rozwoju. Demokracja jest zaś naturalnym środowiskiem dla ochrony prywatności, na tyle na ile ochrona praw i podmiotowości jednostki stanowi podstawowy aksjologiczny wymiar funkcjonowania systemu demokratycznego.

Ranga prawa do prywatności została więc podniesiona do roli jednego z filarów liberalnej demokracji w sposób niejako nieunikniony. W tradycji amerykańskiej uznano wręcz, że: „możemy myśleć o dążeniu do prywatności w taki sam sposób, w jaki myślimy o dążeniu do szczęścia" (Thierer 2013: 415). Jeśli pamiętać, że wspomniane dążenie do szczęścia pojawia się na początku amerykańskiej deklaracji niepodległości jako podstawowe prawo człowieka (obok prawa do życia i prawa do wolności), to trudno znaleźć silniejszą legitymację dla znaczącej pozycji prawa do prywatności w katalogu praw przysługujących jednostce.

Współcześnie częste jest także w amerykańskiej praktyce prawnej wywodzenie istoty prywatności z konstytucji, a bardziej precyzyjnie z poprawek, o które ją uzupełniono.

W tym kontekście najistotniejsze znaczenie ma odnosząca się do bezpieczeństwa osobistego i zapewniająca pełną ochronę przed nieuzasadnionymi rewizjami i sekwestrami, poprawka czwarta[2] (Konstytucja Stanów Zjednoczonych 1990: 30). Co ciekawe, amerykańskim sądom zdarza się także bronić prawa do prywatności na podstawie pierwszej poprawki do konstytucji, dotyczącej wolności wypowiedzi i wolności prasy. Znane są orzeczenia mówiące o prawie do pozostania anonimowym i niezidentyfikowanym, wtedy gdy korzysta się z wolności słowa (Kemp i Moore 2007: 68). Dzieje się tak mimo, iż prawo do prywatności może pozostawać w konflikcie z wymienioną wprost w tej samej poprawce wolnością prasy. Sytuacja taka ma miejsce choćby przy okazji sporu czy dziennikarze mają prawo do informacji ich zdaniem publicznej, a według ich adwersarzy mających charakter prywatny i jako takie podlegających ochronie.

Przykład ten uświadamia kwestię oczywistą dla każdego bliżej zajmującego się teorią demokracji. Podstawowe wartości konstytuujące system demokratyczny są ze sobą uwikłane w skomplikowane zależności, często mające charakter antynomiczny. Więcej wolności często oznacza mniej równości, a wolność osoby A bywa realizowana kosztem wolności osoby B. Prawo do prywatności nie jest wyjątkiem od tej reguły, a kwestię tę komplikuje dodatkowo wspomniany wcześniej brak precyzyjnego uzgodnienia jak w istocie prywatność powinna być definiowana. Co więcej, ostatnie dekady przyniosły na tyle intensywny rozwój nowych technologii informacyjnych i komunikacyjnych, że do opisanych problemów z prywatnością doszły zupełnie nowe wyzwania.

3. REWOLUCJA INFORMACYJNA JAKO WYZWANIE DLA PRYWATNOŚCI

Współczesny etap rewolucji informacyjnej, związany przede wszystkim z rozwojem internetu i nowych narzędzi komunikowania, powitany został przez zdecydowaną większość uczestników tego procesu, ale także badaczy samego zjawiska, ze słabo skrywanym entuzjazmem. W typowy dla fazy emocjonalnego zauroczenia sposób akcentowano przede wszystkim atuty ICT i pozytywne konsekwencje ich rozpowszechnienia, widziane z perspektywy statystycznego użytkownika. Większości przytaczanych w tym kontekście atrybutów charakteryzujących nowe technologie nie sposób zresztą negować. Internet niewątpliwie lawinowo zwiększa dostępność informacji, obniża koszty procesu komunikowania i czyni sam proces zdecydowanie szybszym. Szczególnie istotna jest z tego punktu widzenia możliwość korzystania z urządzeń zapewniających komunikację bezprzewodową.

Przytoczone charakterystyki niewątpliwie sprawiają, że wszystkie aspekty komunikowania są znacznie bardziej przyjazne dla osoby, która nie jest specjalistą w zakresie technologii, ale stara się być aktywna w swym otoczeniu. Nie zmienia to jednak faktu, że istnieją także inne, równie oczywiste cechy ICT. Są one co najmniej nieobojętne z perspektywy przeciętnego użytkownika, zaś w kontekście ochrony prywatności tworzą podstawy dla kreowania zupełnie nowej rzeczywistości. Pierwszą z nich jest cyfrowy zapis informacji, a bardziej precyzyjnie – wynikająca z niego multimodalność. Oznacza to, że w takiej samej – cyfrowej – formie można utrwalić

2 Warto zwrócić uwagę, że także ten, pochodzący z roku 1791, zapis wiąże bezpośrednio obywatelskie prawo do prywatności ze sferą indywidualnego bezpieczeństwa.

każdy nieomal typ danych. Zarówno dźwięk, ruchomy i nieruchomy obraz, jak i dowolną formę tekstu. W konsekwencji wykorzystywania jednolitego zapisu nie ma technicznych przeszkód by wszystkie wspomniane informacje zostały połączone w jednolitą bazę danych. Można sobie więc wyobrazić powstanie swego rodzaju cyfrowej kopii rzeczywistości, zapisującej sekunda po sekundzie każdy zachód słońca widziany z konkretnego miejsca, wszystkie kolejne operacje wykonywane w kasie osiedlowego sklepu, każde słowo wypowiadane przez dowolną osobę przechodzącą w pobliżu miejskiego ratusza, itd.

Ta czysto hipotetyczna możliwość staje się bardziej realna jeśli wziąć pod uwagę drugą istotną charakterystykę ICT. Jest nią sieciowość, będąca w istocie kwintesencją funkcjonowania internetu. Oznacza ona możliwość wykorzystania systemu odnośników dla budowania metabazy informacyjnej, stworzonej dzięki łączności pomiędzy bazami niższego rzędu. Jednocześnie dochodzi także do multiplikacji zgromadzonych danych i ich powielenia w wielu miejscach. W efekcie informacje znajdują się „wszędzie i nigdzie", a to oznacza, że bardzo trudno je usunąć, wtedy gdy z jakichś powodów wydaje nam się to pożądane (Boehme-Neßler 2016: 223).

Opisane właściwości procesów komunikowania realizowanych dzięki ICT nie wyczerpują wpływu rewolucji informacyjnej na sferę prywatności. Istotne znacznie ma także stały rozwój narzędzi i urządzeń wykorzystujących cyfrową formę zapisu danych, które w ramach licznych realizowanych funkcji posiadają także możliwość rejestrowania informacji. Telefon komórkowy – a współcześnie smartfon – nie został skonstruowany do rejestrowania koncertów muzycznych, ale nie zmienia to faktu, że zdecydowana większość fanów widzi potrzebę nagrania choćby części występu swych idoli. W tym samym czasie po ulicach jeżdżą tysiące samochodów wyposażonych w kamery filmujące wydarzenia na drodze, a studenci uznają fotografowanie slajdów wyświetlanych przez wykładowcę za nieomal domyślną formę robienia notatek.

Wykorzystywanie wszystkich opisanych urządzeń może pozostawać bez wpływu na sferę prywatności, ale może też całkowicie zmienić realia w tym zakresie. Jedno nie ulega wątpliwości. Rewolucja informacyjna sprawiła, że podaż dostępnych informacji uległa gwałtownej multiplikacji. Niezależnie od tego czy w intencji ich dysponentów mają one mieć charakter powszechnie dostępny czy zastrzeżony dla pewnego kręgu odbiorców, wszystkie one wchodzą do cyfrowej puli danych obecnych w cyberprzestrzeni i stają się potencjalnym źródłem informacji zarówno dla uprawnionych, jak i nieuprawnionych użytkowników.

Rewolucja informacyjna stworzyła więc co najmniej duży potencjał wpływania na sferę prywatności. Obejmuje on szeroki wachlarz działań, w których wykorzystywane są możliwości stwarzane przez ICT. Frank Bannister już kilkanaście lat temu wymieniał w tym kontekście cztery podstawowe rodzaje aktywności. Są nimi: obserwowanie, przechwytywanie, odczytywanie i interpretacja[3] (Bannister 2005: 67-70). Obserwowanie odbywa się przede wszystkim przez coraz bardziej wszechobecne systemy monitoringu, w ramach którego tysiące kamer przekazuje w czasie rzeczywistym obraz tego, co dzieje się zarówno w miejscach publicznych, instytucjach komercyjnych jak i w posiadłościach prywatnych[4].

3 *Watching, intercepting, reading, interpreting.*

4 Szeroko rozumiane obserwowanie obejmuje także działania polegające na śledzeniu sieciowej aktywności jednostki, poprzez odnotowywanie historii transakcji wykonywa-

Przechwytywanie elektronicznej komunikacji jest współczesną wersją sztuki podsłuchu czy sprawdzania korespondencji, stosowanej zarówno przez służby policyjne jak i zazdrosnych mężów od wieków. Obecnie odbywa się to choćby poprzez kontrolę treści wiadomości wysyłanych przez pocztę elektroniczną (oraz plików przesyłanych w formie załączników), albo informacji przekazywanych w trakcie korzystania z sieciowych komunikatorów.

Kolejna forma ingerowania w prywatność – odczytywanie – wychodzi poza kontrolę zachowania czy procesu komunikowania. Dotyczy ono zapoznawania się z treścią prywatnych danych zgromadzonych przez administrację publiczną (urząd skarbowy), instytucje prywatne (przychodnia lekarska), albo przechowywanych przez samą zainteresowaną osobę na należących do niego urządzeniach. O ile omówione wcześniej obserwowanie i przechwytywanie są – jak wspomniano – łatwiejszą i bardziej skuteczną formą działań znanych od kiedy istnieją służby śledcze, o tyle znaczenie odczytywania danych gwałtownie wzrosło w ostatnich dekadach. Jest to związane zarówno z rosnącą ilością informacji przechowywanych w formie elektronicznej, jak i relatywną łatwością dostępu do tak gromadzonych danych. Włamanie do gabinetu lekarskiego, by poznać medyczną historię konkretnego pacjenta, przechowywaną w wersji papierowej jest zadaniem znacznie trudniejszym – i prawnie ryzykownym – niż zrealizowanie tego samego celu przez doświadczonego hakera kopiującego odpowiednie pliki siedząc za biurkiem we własnym mieszkaniu.

Ostatni z typów ingerencji w prywatność, interpretacja, jest aktywnością, która może korzystać z każdego z omówionych wcześniej działań. Polega ona na integrowaniu wszystkich dostępnych danych w wielkie objętościowo bazy, które poddawane są wyrafinowanej analizie przy pomocy specjalnie stworzonych narzędzi algorytmicznych. Celem jest uzyskanie wiedzy, która nie jest „powierzchniowo" dostępna, wtedy gdy poszczególne zbiory danych przetwarzane są niezależnie od siebie. Ten rodzaj aktywności rozwija się bardzo dynamicznie w ostatnich latach i powszechnie jest określany jako analiza *big data*.

Opisane typy działań wskazują na bezprecedensowe możliwości, jakie rozwój ICT stworzył w zakresie tworzenia, gromadzenia i przetwarzania danych, które w dużej części wcześniej uznane byłyby za prywatne. W efekcie problem „rewolucja informacyjna jako zagrożenie dla prywatności" stał się w ostatnich latach jednym z najintensywniej eksplorowanych. Dotyczy to zarówno pragmatycznej oceny ryzyka naruszeń prywatności w różnych sferach (i oczywiście sposobów jego minimalizacji), jak i akademickiej refleksji nad powodowanymi przez rozwój nowych technologii przemianami hierarchii wartości demokratycznych[5]. Odpowiadając na podstawowe pytanie: w jakim sensie ICT stanowią wyzwanie dla tradycyjnie rozumianego prawa do prywatności? Trzeba jednak pamiętać, że mamy do czynienia z co najmniej dwoma różnymi problemami.

nych kartą płatniczą czy analizę historii odwiedzanych stron internetowych (Bannister 2005: 68).

5 Badacze poddali analizie chyba każdy możliwy aspekt uwikłania nowych technologii w sferę prywatności. Dotyczy to np. bezpieczeństwa danych medycznych (Fu i Blum 2013; Kruse et al. 2017), ochrony danych pracowników i studentów (Thumma 2017), ochrony danych na stronach internetowych kościołów (Hoy i Phelps 2003) czy wreszcie wyzwań dla prywatności w kontekście rozwoju internetu rzeczy (Rehman et al. 2016; Wang et al. 2017).

Po pierwsze, rewolucja informacyjna znacznie ułatwiła dokonywanie różnego rodzaju przestępstw, związanych z naruszeniem prywatności. Jest to efekt zarówno wspomnianego już skoncentrowania wielkiej liczby danych personalnych w relatywnie słabo zabezpieczonych miejscach w cyberprzestrzeni, jak i banalnych zaniedbań, związanych z nieprzestrzeganiem podstawowych zasad bezpieczeństwa. Ktoś komu skradziono informacje o przebytych chorobach dlatego, że na swym komputerze w pracy „na wszelki wypadek" umieścił w widocznym miejscu numer identyfikacyjny i hasło do logowania do sieci medycznej, której jest pacjentem, nie powinien winić za to rozwoju technologii. Nie zmienia to jednak faktu, że dokonanie tego rodzaju przestępstwa byłoby znacznie trudniejsze w przypadku tradycyjnej przychodni lekarskiej, konieczności okazania w rejestracji dokumentu tożsamości, złożenia zgodnego ze wzorem podpisu, itd.

Dostępność w sieci dużej liczby informacji na własny temat znacznie ułatwia też dokonywanie aktów z zakresu cyberprzemocy. Jeżeli większość kontaktów społecznych realizujemy w internecie przy pomocy ICT to łatwo możemy stać się ofiarą sieciowego zastraszania czy napastowania[6] ze strony znajomej lub nieznajomej osoby, z którą weszliśmy w jakikolwiek konflikt. Co więcej, jedynym sposobem na przerwanie kontaktów z tego typu agresorem byłoby zniknięcie z sieci, co jest trudne bo musiałby oznaczać całkowitą zmianę dotychczasowego sposobu życia.

Przykłady sytuacji w których permanentna obecność w sieci czyni nas transparentnymi, a przez to łatwo dostępnymi dla osób podejmujących różnego typu nielegalne działania, ingerujące w naszą prywatność można by mnożyć. Nie wszystkie jednak wyzwania dla tradycyjnie rozumianej prywatności związane są z poczynaniami przestępczymi. Coraz większą rolę odgrywa obecnie aktywność polegająca na wykorzystywaniu przez podmioty dostarczające różne usługi sieciowe legalnie uzyskanych danych swych użytkowników w celach komercyjnych. W kategoriach omawianych wcześniej czterech typów zagrożeń dla prywatności jest to najbliższe procedurze interpretacji, a dotyczy choćby firmy Facebook czy Google, które chętnie dzielą się – za odpowiednią opłatą – ze swymi klientami, informacjami posiadanymi na temat własnych użytkowników. W efekcie prywatni „abonenci" poczty elektronicznej uzyskują bezpłatną usługę wraz z wieloma dodatkowymi serwisami w zamian za zgodę na wyświetlanie informacji reklamowych kontekstowo związanych z treścią wysyłanych i otrzymywanych wiadomości. To reklamodawcy płacą więc w istocie dostawcy poczty za utrzymanie całego przedsięwzięcia.

Wymaga to oczywiście monitorowania treści elektronicznej korespondencji klientów, ale sam model biznesu, który można umownie nazwać „pozwól, że dokładnie przyjrzymy się kim jesteś, a w zamian za to dostaniesz od nas darmową usługę o najwyższej jakości" przyjął się bez zastrzeżeń. Kiedy firma Google, prekursor tego typu rozwiązań, udostępniała w roku 2004 swym użytkownikom pocztę elektroniczną (*Gmail*), wielu analityków i polityków oburzało oczywiste naruszanie zasad prywatności, kryjące się za opisanym sposobem funkcjonowania (Thierer 2013: 420). Ponieważ jednak nikt nie zmuszał potencjalnych klientów do korzystania z usługi zaproponowanej przez Google ostatecznym sprawdzianem poziomu ich wrażliwości na ochronę własnej prywatności mógł stać się tylko popyt na tak sformułowaną

6 Na temat istoty sieciowego zastraszania (cyber-bullying) i sieciowego napastowania (cyber-harassment), a także relacji pomiędzy tymi zjawiskami, zob. np. Porębski (2014: 302-304).

ofertę. Liczby mówią same za siebie. W roku 2012 liczba osób korzystających z *Gmail* sięgnęła 425 milionów, w roku 2015 było to już 900 milionów, a w 2016 1 miliard. Jak się ocenia obecnie (marzec 2018) *Gmail* ma ok. 1,2 miliarda użytkowników na całym świecie, co jest równe 20% udziału w globalnym rynku poczty elektronicznej[7].

Oznacza to, że w zamian za wysoki standard usług (np. wyjątkowo dużą pojemność konta pocztowego) klienci są w stanie pogodzić się ze świadomością, że ich różne dane ujawniane w trakcie sieciowej aktywności będą przez firmę wykorzystywane w celach komercyjnych. Prywatność, przynajmniej w pewnym zakresie, stała się więc towarem. Ta właśnie przemiana wydaje się najciekawsza z perspektywy przeobrażeń współczesnej demokracji. Jest ona też silnie związana z relacją między prawem do prywatności a poczuciem bezpieczeństwa.

4. REDEFINICJA POCZUCIA BEZPIECZEŃSTWA

Możliwość azylu w sferze prywatnej, do której dostęp regulujemy my sami, już od końca XIX wieku była ważnym elementem poczucia bezpieczeństwa obywatela w państwie demokratycznym. Istnienie obszaru autonomii, wyłączonego z arbitralnej ingerencji innych osób i państwa, różnicowało demokrację od autokratycznego systemu politycznego i współtworzyło podmiotowość jednostki. Wszystko to nie oznacza jednak, że samo pojęcie prywatności, a zwłaszcza jej zakres, nie spotykały się z krytyką już od momentu jej pojawienia się wśród podstawowych wartości liberalnej demokracji[8]. Co więcej, jedną z głównych płaszczyzn tego typu kontrowersji była właśnie relacja pomiędzy prywatnością, a bezpieczeństwem, rozumianym jednak w kategoriach kolektywnych.

Im szerszy zakres danych i informacji traktowanych jako prywatne nie jest dostępny dla instytucji państwa, tym trudniej organom tym realizować swoje zadania, związane np. z zapobieganiem czy ściganiem przestępczości. Dotyczy to choćby tajemnicy bankowej dzięki której można unikać płacenia podatków, ale także nielegalnie finansować pospolite przestępstwa kryminalne. To, co z perspektywy jednostki jest gwarancją ważnego aspektu jej wolności, tworząc tym samym jej indywidualne poczucie bezpieczeństwa, z punktu widzenia społecznego może być uznawane za zagrożenie bezpieczeństwa publicznego. Istnieje więc naturalne napięcie pomiędzy prywatnością, a bezpieczeństwem, sfera w ramach której wartości te mogą wydawać się wręcz antynomiczne.

Ostatnie dekady przyniosły nie tylko – opisany wcześniej – gwałtowny wzrost ilości krążących informacji, związany z rewolucja informacyjną, ale jednocześnie intensyfikację zagrożeń o charakterze terrorystycznym. W oczywisty sposób zwiększyło to skłonność władz publicznych, także w krajach demokratycznych, do maksymalizacji kontroli wszelkich dostępnych danych. Ponieważ prawo do prywatności radykalnie ogranicza dostępność informacji z punktu widzenia policji czy służb specjalnych, konflikt między obrońcami prywatności, a zwolennikami pełnej przejrzystości w imię bezpieczeństwa wybuchł z wyjątkową mocą. Wynik tego rodzaju konfrontacji

7 Dane za lata 2014-2016 za: https://www.statista.com/statistics/432390/active-gmail-users/ (4.05.2018), dane z roku 2018 za: https://expandedramblings.com/index.php/gmail-statistics/ (4.05.2018).

8 Na temat głównych aspektów krytyki pojęcia prywatności zob. np. Kemp i Moore (2007: 73-74), Fuchs (2017: 187-188).

można było bez trudu przewidzieć. Wszechobecne w mediach (i często nieadekwatnie wyolbrzymiane) sceny krwawych skutków zamachów terrorystycznych są zdecydowanie bardziej sugestywne niż abstrakcyjne i trudne do zdefiniowania prawo do prywatności. W rezultacie na całym świecie zaczęto przyjmować akty prawne, radykalnie zwiększające możliwości inwigilacji przez władze wszelkich – ale zwłaszcza realizowanych poprzez ICT – form komunikowania. Opisane wcześniej: obserwowanie, przechwytywanie, odczytywanie i interpretacja stały się w pełni legalnymi działaniami, podejmowanymi dla dobra obywateli. Mimo, iż niewątpliwie: „istnieje taki hipotetyczny punkt, w którym 'wystarczający poziom bezpieczeństwa' może zostać zrównoważone przez 'wystarczający poziom prywatności' " (Bird 2013: 669), wahadło wyraźnie wychyliło się w jedną stronę. Do pewnego stopnia prywatność została zredukowana do wartości drugiego rzędu.

Proces ten, w jakiejś mierze nieunikniony w kontekście gwałtownej utraty stabilności systemu stosunków międzynarodowych, nie jest jednak jedynym aspektem redefiniowania poczucia bezpieczeństwa i prawa do prywatności. Równolegle mają miejsce zmiany stymulowane przez pojawienie się serwisów społecznościowych i zdominowanie przez nie społecznego wymiaru funkcjonowania zdecydowanej większości ludzi. Realny wybór, jaki ma współcześnie jednostka (przynajmniej w swym subiektywnym odczuciu) sprowadza się do stosunkowo prostej alternatywy. Po jednej stronie jest aktywne funkcjonowanie we własnym środowisku, a to oznacza konieczność obecności w mediach społecznościowych – na niepodlegających negocjacjom warunkach narzucanych przez prowadzące je firmy. Oznacza to między innymi daleko idące ograniczenie prywatności poprzez realną utratę kontroli nad dostępnymi w sieci danymi i informacjami na swój temat. Po drugiej stronie w grę wchodzi trwanie przy tradycyjnie rozumianej ochronie własnej prywatności, ale kosztem absencji w serwisach społecznościowych, a więc swoistej społecznej marginalizacji.

Doświadczenia kolejnych pokoleń, obcujących od kołyski ze smartfonem i innymi nowymi technologiami sprawiły, że wraz z upływem lat opisana alternatywa staje się coraz bardziej iluzoryczna. W kwietniu 2018 roku najpopularniejszy serwis społecznościowy, Facebook miał 2, 234 miliarda aktywnych użytkowników[9]. Oznacza to, że z Facebooka korzysta prawie 30% mieszkańców Ziemi i ponad połowa (53,7%) wszystkich użytkowników internetu na świecie[10]. Mowa zaś o największym, ale wyłącznie jednym z wielu dostępnych dla każdego mediów społecznościowych. Poczucie, że nieobecność na Facebooku, WhatsApp czy Instagramie jest równoznaczna ze swoistym społecznym wykluczeniem (czymś w rodzaju współczesnego odpowiednika analfabetyzmu) stało się powszechne. W konsekwencji równie domyślne co samo korzystanie z serwisów społecznościowych jest obecnie podejście do ochrony informacji na swój temat. Warto zaakceptować komercyjne korzystanie z moich danych przez firmy dostarczające mi usługi sieciowe, jeżeli w zamian za to dostaję możliwość nieograniczonego funkcjonowania w cyberprzestrzeni, a profilowane na podstawie moich zachowań (i bez mojej wiedzy) reklamy mogą przecież przynieść mi, jako konsumentowi sporo korzyści i oszczędności.

9 Zob. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (6.05.2018). Według tych samych danych każdy spośród dziewięciu najpopularniejszych serwisów społecznościowych na świecie miał w tym czasie ponad pól miliarda użytkowników.

10 Liczba internautów na świecie była na koniec grudnia 2017 roku szacowana na 4,156 mld. Zob. https://www.internetworldstats.com/stats.htm (6.05.2018).

Czy oznacza to, że wszyscy akceptujący taki tok rozumowania nie mają świadomości zagrożenia własnej prywatności i w konsekwencji poczucia bezpieczeństwa? Zapewne nie, ale dominujące nastawienie to postrzeganie zagrożeń jako co najwyżej potencjalnych, a korzyści jako całkowicie realnych – „tu i teraz". Jest to zapewne efekt przemian społecznych o znacznie głębszym charakterze. W coraz większym stopniu tożsamość jednostki budowana jest wokół roli konsumenta, kosztem schodzenia na dalszy plan roli obywatela. W czasie, gdy ten pierwszy stara się maksymalizować doraźne profity, związane zarówno z darmowymi usługami zapewnianymi przez *Gmail*, jak i szeroką siecią znajomych na Facebooku, ten drugi mógłby zauważyć, że jest manipulowany przez dostawców reklam i traktowany przedmiotowo – jako towar. Ponieważ jednak całe otoczenie kulturowe oraz kierunek przemian gospodarczych stymulują wyraźnie postawy konsumenckie, głos w obronie tradycyjnie rozumianych prywatności i bezpieczeństwa wydaje się dochodzić coraz ciszej.

Co więcej, także w kategoriach psychologicznych poczucie bezpieczeństwa budowane jest obecnie znacznie bardziej na wspólnotowości niż na zakładającej pewien dystans wobec otoczenia autonomii. Setki znajomych w serwisach społecznościowych i bycie częścią wielomilionowej wspólnoty daje silniejsze poczucie akceptacji i bezpieczeństwa niż związana z umiejętnością wyznaczania granic dostępu do siebie świadomość autonomii wobec własnego środowiska i pełnej kontroli nad swym losem.

5. PODSUMOWANIE

Trudno uznać, na ile opisane tendencje mają charakter trwały. Badacze przemian społecznych mogą mieć jednak poczucie, że historia zatoczyła koło. Chęć potwierdzania swej samooceny przez grupę do której się należy i budowanie poczucia bezpieczeństwa na identyfikacji z otoczeniem współcześnie są niewątpliwie wzmacniane przez rozwój ICT. Same te tendencje nie są jednak niczym nowym dla wnikliwych obserwatorów. David Riesman (1996) opisując samotny tłum czy Jose Ortega y Gasset (1997) w kontekście buntu mas, mieli na ten temat sporo do powiedzenia już w pierwszej połowie ubiegłego wieku.

Na początku XXI stulecia sytuacja jest jednak o tyle nowa, że nigdy wcześniej w realiach demokratycznych nikt nie deklarował otwarcie, że: „wiek prywatności już się skończył" (Boehme-Neßler 2016: 224). Te słowa, wypowiedziane przez Marka Zuckerberga w roku 2010 miały być zapewne zobiektywizowanym opisem rzeczywistości (a na poziomie nieświadomym stały się projekcją pragnień biznesmena zarabiającego krocie na udostępnianiu danych o innych ludziach). Jeśli pamiętać jednak, że wypowiedział je człowiek kontrolujący narzędzie z którego korzysta i uważa je za podstawowy element swej codzienności prawie co trzeci mieszkaniec Ziemi, to brzmią one jak groźne memento. Świat społeczny bez realnej gwarancji prywatności i egzystencja ludzka bez subiektywnej potrzeby prywatności są tuż za progiem. Jeśli próg ten zostanie przekroczony czeka nas zapewne sporo nowych i ekscytujących doznań. To czy uda się ich doświadczyć chroniąc poczucie własnego bezpieczeństwa stoi pod dużym znakiem zapytania.

BIBLIOGRAFIA

- Bannister F., 2005, The Panoptic State: Privacy, Surveillance and the Balance of Risk, Information Polity, vol. 10, s. 65-78.
- Bird S., 2013, Security and Privacy: Why Privacy Matters, Science and Engineering Ethics, vol. 19, issue 3, s. 669-671.
- Boehme-Neßler V., 2016, Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection, International Data Privacy Law, vol. 6, no. 3, s. 222-229.
- Fu K., Blum J., 2013, Inside Risks: Controlling for Cybersecurity Risks of Medical Device Software, Communication of the ACM, vol. 56, no. 10, s. 35-37.
- Fuchs Ch., 2011, Towards An Alternative Concept of Privacy, Journal of Information, Communication & Ethics in Society, vol. 9, no. 4, s. 220-237.
- Fuchs Ch., 2017, Social Media: A Critical Introduction, London: Sage.
- Hoy M. G., Phelps J., 2003, Consumer Privacy and Security Protection on Church Websites: Reasons for Concern, Journal of Public Policy and Marketing, vol. 22, issue 1, s. 58-70.
- Kemp R., Moore A., 2007, Privacy, Library Hi Tech, vol. 25, no. 1, s. 58-78.
- Konstytucja Stanów Zjednoczonych, 1990, Kraków: Oficyna Filmowa Galicja.
- Kruse C., Frederick B., Jacobson T., Monticone K., 2017, Cybersecurity in Healthcare: A Systematic Review of Modern Thereats and Trends, Technology and Healthcare, vol. 25, s. 1-10.
- Maslow A., 1954, Motivation and Personality, New York: Harper & Row
- Maslow A., 1986, W stronę psychologii istnienia, Warszawa: Wydawnictwo PAX.
- Maslow A., 1990, Motywacja i osobowość, Warszawa: Wydawnictwo Pax.
- Mill J. S., 1965, Zasady ekonomii politycznej i niektóre jej zastosowania do filozofii społecznej. T. 1, Warszawa: PWN.
- Mill J. S., 1966, Zasady ekonomii politycznej i niektóre jej zastosowania do filozofii społecznej. T. 2, Warszawa: PWN.
- Ortega y Gasset J., 1997, Bunt mas, Warszawa: Wydawnictwo Literackie Muza.
- Porębski L., 2014, Gorzki smak technologii. Nowe formy przemocy jako konsekwencja rewolucji informacyjnej, Ethos, nr 106, s. 299-313.
- Rehman A., Rehman S., Khan I., Moiz M., Hasan S., 2016, Security and Privacy Issues in IoT, Internationa Journal of Communication Networks and Information Security, vol. 8, no. 3, s. 147-157.
- Riesman D., 1996, Samotny tłum, Warszawa: Wydawnictwo Literackie Muza.
- Thierer A., 2013, The Pursuit of Privacy in A World Where Information Control is Falling, Harvard Journal of Law and Public Policy, vol. 36, no. 2, s. 409-455.
- Thumma S., 2017, When You Can Not "Just Say No": Protecting the Online Privacy of Employees and Students, South Carolina Law Review, vol. 69, no. 1, s. 1-79.
- Wang L., Lu Z., Sun H., Hou Y., Huang M., 2017, Security and Privacy in Internet of Things with Crowd-Sensing, Journal of Electrical and Computer Engineering, vol. 2017, s. 1-2.