

Prywatność jako przedmiot wymiany

1. Wstęp

Cyfryzacja życia umożliwia zbieranie i przetwarzanie danych o konsumentach w niespotykanej dotychczas skali. Powoduje to naruszanie prywatności konsumentów, zwłaszcza użytkowników Internetu. W wyniku automatycznego przetwarzania danych o konsumentach powstają ich profile, coraz bardziej dokładne, wykorzystywane w działaniach marketingowych firm. Dotychczas konsumenci w znakomitej większości bezpłatnie udostępniali swoje dane i dlatego nie byli stroną w procesie wymiany. Profile były przedmiotem wymiany między firmami tworzącymi i wykorzystującymi je. Wycena profili była pochodną możliwości ich wykorzystania w biznesie, szczególnie zwiększania efektywności działań biznesowych.

Zakres i skala zbieranych danych oraz ich wykorzystanie w profilowaniu działań marketingowych wpłynęły na zmianę regulacji prawnych. Ochronie będą podlegać nie tylko dane osobowe, ale szeroko pojęta prywatność. Prowadzenie profilowanych działań marketingowych będzie uwarunkowane świadomą zgodą konsumenta. Wprowadzane przez Unię Europejską nowe przepisy zmieniają warunki rynkowe w relacjach konsument–firma. Zmienia się zarówno przedmiot wymiany, jak i rola konsumenta. Konsumenci jako sprzedawcy prywatności staną przed wyzwaniem oszacowania wartości ekonomicznej swoich danych. Obecnie istnieją jedynie szczątkowe badania dotyczące tych kwestii (wybrane przytoczono w artykule). Celem artykułu jest analiza zmian w regulacjach prawnych dotyczących prywatności (jej definicji i ochrony) pod kątem zmian w relacjach konsument–firma w zakresie sprzedaży/kupna prywatności.

¹ Szkoła Główna Handlowa, Kolegium Analiz Ekonomicznych.

2. Prywatność – definicja, prawne uwarunkowania

Prywatność jest pojęciem nieprecyzyjnie i różnie definiowanym. Większość osób posługuje się intuicyjnym rozumieniem prywatności i jego synonimem – „życie prywatne/osobiste”. Trudności z definicją podkreśla się zarówno w polskiej, jak i anglojęzycznej literaturze². Nawet w prawie to pojęcie nie jest precyzyjnie zdefiniowane. Europejski Trybunał Praw Człowieka stwierdził, że „nie jest możliwe, ani konieczne formułowanie wyczerpującej definicji pojęcia «życie prywatne»”. Polski Sąd Najwyższy zaś zauważył, że wykładnia sfery życia prywatnego wymaga uwzględnienia indywidualnych okoliczności charakteryzujących określoną sytuację³. Problemy ze zdefiniowaniem pojęcia prywatności prowadzą niektórych autorów, na przykład M. Jagielskiego, do stwierdzeń, że ważniejsze jest znalezienie właściwych mechanizmów ochronnych, aniżeli zdefiniowanie pojęć⁴. Takiemu podejściu przeciwstawia się J. Rzucidło, który mimo że przyznaje, iż „choć pod pojęciem prywatności znajduje się tak wiele różnorodnych zjawisk, że niekiedy mają one ze sobą niewiele wspólnego”, to jednak bez tego pojęcia nie można się obejść⁵. J. Rzucidło definiuje prywatność w ujęciu wąskim i szerokim. W ujęciu wąskim prywatność to stan, w ramach którego jednostka decyduje o zakresie i zasięgu informacji udostępnianych i zakomunikowanych innym osobom. W szerokim zaś to stan, w którym jednostka podejmuje decyzje dotyczące jej osoby bez ingerencji osób trzecich⁶. M. Pryciak określa prywatność jako przestrzeń wolnego poruszania się, autonomicznej aktywności, wolnej od kontroli innych podmiotów⁷. Współczesne definicje prywatności obejmują wiele aspektów, przez co stają się mało precyzyjne. J. Kohler, jeden z pionierów w tej dziedzinie, zdefiniował w 1907 roku prywatność jako swobodę rozporządzania informacjami na swój temat. Choć J. Kohler odnosił to stwierdzenie

² A. Acquisti, C. Taylor, L. Wagman, *The Economics of Privacy*, „Journal of Economic Literature” 2016, vol. 54(2), s. 442–492, <http://dx.doi.org/10.1257/jel.54.2.442> (dostęp: 20.07.2017).

³ Za: W. Walkowski, *Pojęcie prywatności i przesłanki jej naruszenia*, LexVin Kancelaria Radcy Prawnego Dariusz Kostyra, <http://lexvin.pl/prawo-lexvin/3380/Pojecie-prywatnosci-i-przeslanki-jej-naruszenia> (dostęp: 20.07.2017).

⁴ M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Wolters Kluwer Polska, Warszawa 2010, s. 28.

⁵ J. Rzucidło, *Prawo do prywatności i ochrona danych osobowych*, w: *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, M. Jabłoński (red.), Wrocław 2014, s. 154.

⁶ Ibidem, s. 153.

⁷ M. Pryciak, *Prawo do prywatności*, „Studia Erasmiana Wratislaviensia” 2010, 4, s. 212.

do zachowania tajemnicy korespondencji⁸, to można powiedzieć, że wskazał istotny aspekt tego zagadnienia. Jest on tożsamy z wąskim ujęciem prywatności według J. Rzucidła.

Próbie kategoryzacji różnych aspektów prywatności podjął także K. Motyka. K. Motyka po dokonaniu szczegółowego przeglądu literatury poświęconej prywatności (polskiej i światowej z okresu kilkudziesięciu lat), również podkreśla niemożność precyzyjnego zdefiniowania tego pojęcia i proponuje postrzegać prywatność w następujących aspektach:

1. prywatność fizyczną, odnoszącą się do integralności fizycznej jednostek;
2. prywatność decyzyjną, umożliwiającą podejmowanie decyzji osobistych bez ingerencji władzy czy osób trzecich;
3. prywatność komunikacyjną, związaną z wolnością wypowiedzi i stowarzyszania się;
4. prywatność terytorialną, chroniącą pewne miejsca, zwłaszcza będące własnością danej jednostki oraz
5. prywatność informacyjną, związaną z danymi osobowymi.

Kategorie te autor wyodrębnił na podstawie kwerendy literatury i dodał jeszcze jeden aspekt prywatności od siebie, który nazwał „prywatnością uwagi”, jej naruszeniem są typowe we współczesnych społeczeństwach uciążliwe praktyki marketingu⁹. W procesach rynkowych kluczowe jest wąskie rozumienie prywatności jako prawa do ochrony informacji danych osobowych (prywatność informacyjna) oraz prywatność uwagi. Te rodzaje prywatności są ze sobą powiązane, gdyż dostęp do informacji o osobie prowadzi do bardziej wyrafinowanych sposobów promocji, przede wszystkim wykorzystania profilowania. Zaś naruszanie tych prywatności może skutkować naruszeniem prywatności decyzyjnej, szczególnie w zakresie decyzji zakupowych.

Proces perswazji marketingowej zaczyna się od pozyskania danych osobowych, dlatego tak ważna jest ich ochrona. Regulacje prawne wprowadzane przez Unię Europejską zaostrzą konkurencję o dostęp do danych osobowych. 25 maja 2018 roku wejdzie w życie rozporządzenie o ochronie danych osobowych – tzw. RODO¹⁰, które zastąpi obecną ustawę o ochronie danych osobowych

⁸ Ibidem, s. 213.

⁹ K. Motyka, *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Administracja i Zarządzanie” 2010, vol. 85, s. 35.

¹⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

(UODO). W planach Unii Europejskiej jest, aby to tego dnia uchwalić kolejne rozporządzenie o e-privacy.

Obecnie stosowana w prawie Unii definicja danych osobowych jest bardzo szeroka. Dane osobowe są rozumiane jako „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej («osobie, której dane dotyczą»); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”¹¹.

Takie zdefiniowanie tego pojęcia pozwala w większym zakresie chronić dane wrażliwe. Wykorzystanie tych danych stanowi dużo większe zagrożenie prywatności niż w wypadku innych danych osobowych. Biorąc pod uwagę możliwości wnioskowania, jakie mają systemy automatycznego przetwarzania danych, są to praktycznie wszystkie ślady cyfrowe, jakie zostawia internauta. Możliwości tych systemów wskazują między innymi badania M. Kosińskiego. Wykazano, że cechy takie jak orientacja seksualna, rasa (biały, czarny) czy preferencje wyborcze (demokraci vs. konserwatyści) można trafnie wywnioskować ze śladów cyfrowych (bez konieczności uzyskania deklaracji) w ponad 80% przypadków (odpowiednio: orientacja seksualna – 88%, rasa – 95%, preferencje wyborcze – 85%)¹². W innych badaniach udowodniono, że wnioskowanie przez systemy komputerowe jest trafniejsze w ocenie cech osobowości, niż wnioskowanie ludzi¹³. Tego typu doniesienia uzasadniają szerokie definiowanie danych osobowych oraz pokazują, jakie możliwości profilowania (targetowania) mają firmy.

Przepisami RODO wprowadzono kilka istotnych rozwiązań, tj. prawo do bycia zapomnianym, wzmocnione prawo wglądu konsumenta w jego dane, ograniczenie profilowania (zgoda na zbieranie danych do profilowania, informowanie o profilowaniu oraz konieczność akceptacji braku zgody na ten proceder). Szczególnie ważne dla branży reklamowej może być rozszerzone prawo sprzeciwu wobec przetwarzania danych wykorzystywanych w marketingu bezpośrednim,

¹¹ Ibidem, art. 4.

¹² M. Kosinski, D. Stillwell, T. Graepel, *Private traits and attributes are predictable from digital records of human behaviour*, „PNAS” 2013, vol. 110(15), s. 5802–5805, <http://www.pnas.org/content/110/15/5802> (dostęp: 27.07.2017).

¹³ W. Youyou, M. Kosinski, D. Stillwell, *Computer-based personality judgments are more accurate than those made by humans*, „PNAS” 2015, vol. 112(4), s. 1036–1040, <http://www.pnas.org/content/112/4/1036> (dostęp: 27.07.2017).

w tym w profilowaniu (RODO, art. 21). A co najważniejsze – zdefiniowano samo profilowanie: „«Profilowanie» oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się” (RODO, art. 4). Tak zdefiniowane profilowanie i prawo sprzeciwu konsumenta wobec tego proceduru wymusi na firmach negocjowanie zakupu prywatności konsumenta. Do tej pory firmy zręcznie omijają problemy z ochroną prywatności przy procesach profilowania, wykorzystując anonimizację. Jednak jak zauważyła Grupa Robocza Art. 29¹⁴: „[...] trudne jest utworzenie prawdziwie anonimowego zbioru danych przy jednoczesnym zachowaniu tyłu podstawowych informacji, ile jest konieczne do realizacji zadania”¹⁵. Rozwój technologii informacyjno-komunikacyjnej (ICT), skala jej wykorzystania przez konsumentów powodują, że rzetelna anonimizacja w wypadku wykorzystania profili w działaniach marketingowych firm nie jest praktycznie możliwa. Dlatego kierunek zmian prawnych jest taki, aby dopuścić działania z wykorzystaniem profilowania, ale by konsument był w pełni świadomy tego proceduru. Będzie to trudne do realizacji ze względu na lukę cyfrową (umiejętności posługiwania się ICT). Zaledwie 56% polskich internautów deklaruje znajomość działania tzw. ciasteczek¹⁶, a jest to przecież jeden z najprostszych sposobów zbierania danych do profilowania. Naprzeciw tym wymaganiom wychodzi kolejne rozporządzenie Unii Europejskiej w sprawie e-prywatności¹⁷. Jest ono w fazie opracowywania i dyskusji, dlatego trudno powiedzieć, jak dokładnie wpłynie on na relację między konsumentem a firmą. Z kwestii istotnych podkreślanych przez analityków jest to, że dostawcy takich programów jak przeglądarki będą musieli dostarczyć przyjaznych rozwiązań

¹⁴ Zespół roboczy utworzony z przedstawicieli organów nadzorczych zajmujących się ochroną danych osobowych powołanych przez poszczególne państwa Unii Europejskiej.

¹⁵ *Opinia 5/2014 w sprawie technik anonimizacji* (WP 216), Grupa Robocza Art. 29, 10 kwietnia 2014 r., s. 3, <http://www.giodo.gov.pl/pl/1520203/7808> (dostęp: 30.07.2017).

¹⁶ *Prywatność w sieci (2016/2017)*, IAB, 7.03.2017, <https://iab.org.pl/badania-i-publikacje/raport-prywatnosc-w-sieci-20162017/>, s. 6 (dostęp: 27.07.2017).

¹⁷ *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, Komisja Europejska, Bruksela 10.1.2017, <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications> (dostęp: 27.07.2017).

pozwalających na požądane przez internautę ustawienie prywatności¹⁸. Biorąc pod uwagę lukę cyfrową, będzie to zadanie trudne do wykonania. W projekcie rozporządzenia nie wspomina się o programach blokujących reklamy, co może oznaczać, że w tym zakresie sytuacja nie ulegnie zmianie (programy nie zostaną zakazane, jakby chciały tego agencje reklamowe i reklamodawcy). Tym samym ochrona prywatności uwagi będzie nadal w rękach użytkownika. W tym zakresie emancypacja internautów zaszła daleko. Od kilku lat nasila się blokowanie reklam przez internautów. W USA 1/3 internautów używa programów blokujących reklamy (30,1% – stan na luty 2017)¹⁹, zaś polscy internauci są liderami światowymi w tym zakresie. Szacuje się, 46% odsłon stron w Polsce jest zablokowanych, a straty wydawców reklamy na świecie są rzędu 42 mld dolarów (wartość rynku ok. 100 mld USD)²⁰. Branża reklamowa próbuje zachęcać internautów do odblokowywania reklam, na ogół blokując dostęp do treści merytorycznych. Kończy się to przeważnie (w 74% przypadków) opuszczeniem serwisu²¹. Wprowadzenie w Unii Europejskiej wspomnianych regulacji może spowodować podobną sytuację w stosunku do wszelkich działań profilowanych. Reklamodawcy i branża reklamowa muszą podjąć bardziej zniuansowane działania wykorzystujące rozwijającą się ekonomikę prywatności.

3. Ekonomika prywatności

Pojęcie prywatności przez lata było przedmiotem rozważań prawników, psychologów czy socjologów. Dopiero pod koniec lat 70. zainteresowali się nimi ekonomiści²². Nadal jest to dziedzina mało znana. Google Trends nie jest w stanie pokazać żadnych statystyk w stosunku do frazy „ekonomika prywatności” jak

¹⁸ E. Todd, *The new ePrivacy Regulation: how will it impact your business?*, CMS, Londyn, <http://datonomy.eu/2017/01/16/the-new-eprivacy-regulation-how-will-it-impact-your-business/> (dostęp: 20.07.2017).

¹⁹ *As Ad Blocker Use Grows, Publishers Face New Challenges*, „eMarketer”, <https://www.emarketer.com/Article/Ad-Blocker-Use-Grows-Publishers-Face-New-Challenges/1016076> (dostęp: 2.08.2017).

²⁰ *Ad blocking in the Internet, Report 2017*, OnAudience.com, www.onaudience.com/files/adblock_report.pdf (dostęp: 2.08.2017).

²¹ *The state of the blocked web. 2017 Global Adblock Report*, PageFair, <https://pagefair.com/blog/2017/adblockreport/> (dostęp: 2.08.2017).

²² R.A. Posner, *The Economics of Privacy*, „The American Economic Review” 1981, vol. 71(2), s. 405–409.

i *economics of privacy*. Zapytanie kierowane do Google o wyszukanie frazy „ekonomika prywatności” nie daje żadnych rezultatów. To samo zapytanie kierowane w języku angielskim wyświetla kilka stron wartościowych rezultatów, głównie pozycje napisane przez A. Acquisti, który od kilku lat propaguje ten temat. Jednak jak popatrzymy na liczbę cytowań jego pozycji (poniżej 200), jak i klasycznej pozycji R.A. Posnera (niewiele ponad 300 w ciągu ponad 30 lat), to widać, że jest nowa dziedzina, która nie cieszyła się zainteresowaniem ekonomistów.

A. Acquisti dostrzega trzy nurty w publicznej debacie poświęconej prywatności w kontekście ekonomii²³:

1. Ochrona prywatności nie ma sensu ekonomicznego – rynek zapewni optymalną równowagę między ochroną informacji i dzieleniem się.
2. Utrata prywatności to cena za postęp technologiczny i korzyści wynikające z big data. Wprowadzając regulację, można stworzyć nieprawidłowości w funkcjonowaniu rynku tam, gdzie obecnie ich nie ma.
3. Udostępnianie danych osobowych jest ekonomicznie korzystne dla obu stron. Na przykład w przypadku reklam profilowanych klienci widzą reklamy produktów, którymi mogą być zainteresowani, dlatego reklamodawcy mają większą szansę sprzedaży, a wartość reklamy jest zwiększona, co też przynosi korzyści wydawcy publikującemu reklamy.

Podjęcie pierwsze i drugie zostało odrzucone w Unii Europejskiej, o czym świadczą wprowadzane regulacje prawne. Pod tym względem podjęcie w Europie i USA mocno się różni.

Podjęcie trzecie jest forsowane przez reklamodawców i branżę reklamową. Profilowanie niewątpliwie przyczynia się do obniżania kosztów dopasowania (poszukiwania informacji przez konsumenta i kosztów promocji po stronie firmy). Ten aspekt był wielokrotnie dostrzegany²⁴ i jest podstawą działania takich pośredników, jak Google czy Facebook. Zagrożenia płynące z takiego postępowania punktuje E. Pariser²⁵, który uważa, że internauci mają dzięki temu mniejszy kontakt z opiniami/informacjami odmiennymi, co powoduje, że żyją w swego rodzaju „silosach informacyjnych”.

²³ A. Acquisti, *The Economics of Privacy*, London School of Economics and Political Science, <http://blogs.lse.ac.uk/mediapolicyproject/2016/07/27/the-economics-of-privacy/> (dostęp: 2.08.2017).

²⁴ Zob. H.R. Varian, *Economic Aspects of Personal Privacy*, UC Berkeley, <http://people.ischool.berkeley.edu/~hal/Papers/privacy/> (dostęp: 27.07.2017) czy M. Sawhney, Ph. Kotler, *Marketing in the Age of Information Democracy*, w: *Kellogg on Marketing*, D. Iacobucci (red.), John Wiley, New York, Chichester, Weinheim, Brisbane, Singapore, Toronto 2001, s. 386.

²⁵ E. Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Penguin Books, New York 2011.

Profilowanie do tej pory odbywało się na podstawie danych prywatnych pozyskiwanych praktycznie za darmo. Badania Eurobarometru pokazują, że nasila się tendencja do kontroli swoich danych i zachowania prywatności informacyjnej u internautów w Europie (ponad 90% widzi potrzebę kontroli nad tym, kto ma dostęp do ich danych)²⁶. Pojawia się pytanie, czy internauci są zainteresowani profilowanymi treściami i czy w zamian są gotowi udostępnić swoje dane. Większość polskich internautów nie oczekuje profilowanych treści. Treści profilowanych (dopasowanych do zainteresowań internauty), tj. artykuły, filmy itp., oczekuje 39% badanych, zaś profilowanych reklam – 30%²⁷. Niekorzystnie też wyglądają deklaracje odnośnie do „sprzedaży” swoich danych. W badaniach Deloitte 43% ankietowanych twierdzi, że „zdecydowanie nie” lub „raczej nie udostępni” swoje dane, nawet gdy w zamian oferowana jest im jakaś nagroda, na przykład bon, rabat lub inna korzyść. Podobna grupa (38%) gotowa jest wymienić swoje dane w zamian za jakieś korzyści (20% nie ma jednoznacznego zdania w tej kwestii). Na rozkład odpowiedzi wpływa zapewne przeświadczenie respondentów (51% deklaracji), że firmy potrzebują danych osobowych przede wszystkim po to, by informować o promocjach. Mniej niż połowa (45%) uważa, że zbieranie danych służy dostosowaniu oferty do klienta. Taki sam odsetek osób uważa, że firmy zbierają dane w celu ich odsprzedaży, a 39% dostrzega w tym chęć monitorowania zachowania klientów. Zrozumienie charakterystyki klientów wskazywało 24%, a polepszenie jakości obsługi 15% respondentów²⁸. Wyniki te świadczą o tym, że konsumenci widzą firmy jako głównych beneficjentów zbierania i przetwarzania danych. Badania wskazują, że tak nie musi być. A. Acquisti i H.R. Varian analizowali korzyści płynące ze zróżnicowania cen możliwe dzięki przetwarzaniu informacji o konsumencie przez firmy. Z ich badań wynika, że więcej korzyści odnosi firma, ale konsument również na tym korzysta (przede wszystkim obniżanie kosztów, tym ważniejsze, im częstszy jest zakup)²⁹.

Prawdopodobnie to firmy odnoszą większe korzyści z profilowania, ale wykorzystywanie danych osobowych prowadzi też do możliwości manipulacji

²⁶ *Flash Eurobarometer 443 – July 2016, “e-Privacy” Report*, European Union, <https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy> (dostęp: 27.07.2017).

²⁷ *Prywatność w sieci*, s. 9.

²⁸ *Rok do RODO – ochrona danych osobowych oczami polskich konsumentów*, Raport Deloitte, https://www2.deloitte.com/pl_ochrona_danych_osobowych_oczami_polskich_konumentow_Raport_Deloitte_Maj_Final1.pdf (dostęp: 2.08.2017).

²⁹ A. Acquisti, H.R. Varian, *Conditioning Prices on Purchase History*, „Marketing Science” 2005, vol. 24(3), s. 367–381.

przez użytkownika. A. Acquisti i Ch. Fong przeanalizowali wpływ informacji dostępnych w mediach społecznościowych na decyzje dotyczące zatrudnienia przez firmy amerykańskie. Okazało się, że odpowiednio kształtując profil w serwisach społecznościowych (LinkedIn, Facebook), kandydat może zwiększyć szanse na zatrudnienie, eksponując informacje, których ze względu na ograniczenia prawne nie zamieszcza się/nie wymaga się w CV, na przykład kwestie stosunku do religii³⁰.

Podsumowanie i kierunki dalszych badań

Ekonomika prywatności to dyscyplina, która jeszcze w Polsce nie istnieje, ale ze względu na rozwój technologii ICT oraz regulacje prawne będzie musiała powstać. Do tej pory kwestiami prywatności zajmowali się przede wszystkim prawnicy. Nadszedł czas na ekonomistów, gdyż pozyskiwanie i przetwarzanie danych osobowych będzie istotnym elementem budowania pozycji firm na rynku. Obecnie wycena danych osobowych odbywa się głównie w relacjach B2B. Firmy kupują bazy danych, płacą różne ceny za działania promocyjne w zależności, czy są one profilowana czy też nie. W najbliższych latach firmy będą musiały negocjować z konsumentami zakup ich danych osobowych. Skłonność do sprzedaży swojej prywatności będzie wynikiem korzyści zaoferowanych przez firmę, ale też cech osobowości konsumenta. W tym zakresie otwiera się pole do interdyscyplinarnych badań psychologów i ekonomistów.

Bibliografia

- Acquisti A., Varian H.R., *Conditioning Prices on Purchase History*, „Marketing Science” 2005, vol. 24(3), s. 367–381.
- Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Wolters Kluwer Polska, Warszawa 2010, s. 28.
- Motyka K., *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Administracja i Zarządzanie” 2010, vol. 85, s. 35.

³⁰ A. Acquisti, Ch. Fong, *An Experiment in Hiring Discrimination via Online Social Networks*, <http://dx.doi.org/10.2139/ssrn.2031979> (dostęp: 2.08.2017).

- Pariser E., *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Penguin Books, 2012.
- Posner R.A., *The Economics of Privacy*, „The American Economic Review” 1981, vol. 71(2), s. 405–409.
- Pryciak M., *Prawo do prywatności*, „Studia Erasmiiana Wratislaviensia” 2010, 4, s. 212.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
- Rzucidło J., *Prawo do prywatności i ochrona danych osobowych*, w: *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, M. Jabłoński (red.), Wrocław 2014, s. 154.
- Sawhney M., Kotler Ph., *Marketing in the Age of Information Democracy*, w: *Kellogg on Marketing*, D. Iacobucci (red.), John Wiley, New York, Chichester, Weinheim, Brisbane, Singapore, Toronto 2001, s. 386.

Źródła sieciowe

- Acquisti A., Fong Ch., *An Experiment in Hiring Discrimination via Online Social Networks*, <http://dx.doi.org/10.2139/ssrn.2031979> (dostęp: 2.08.2017).
- Acquisti A., *The Economics of Privacy*, London School of Economics and Political Science, 27.07.2016, <http://blogs.lse.ac.uk/mediapolicyproject/2016/07/27/the-economics-of-privacy/> (dostęp: 2.08.2017).
- Acquisti A., Taylor C., Wagman L., *The Economics of Privacy*, „Journal of Economic Literature” 2016, vol. 54(2), s. 442–492, <http://dx.doi.org/10.1257/jel.54.2.442> (dostęp: 20.07.2017).
- Ad blocking in the Internet, Report 2017*, OnAudience.com, www.onaudience.com/files/adbblock_report.pdf (dostęp: 2.08.2017).
- As Ad Blocker Use Grows, Publishers Face New Challenges*, eMarketer, 26.06.2017, <https://www.emarketer.com/Article/Ad-Blocker-Use-Grows-Publishers-Face-New-Challenges/1016076> (dostęp: 2.08.2017).
- Flash Eurobarometer 443 – July 2016, “e-Privacy” Report*, European Union, <https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy> (dostęp: 27.07.2017).
- Kosinski M., Stillwell D., Graepel T., *Private traits and attributes are predictable from digital records of human behaviour*, „PNAS” 2013, vol. 110(15), s. 5802–5805, <http://www.pnas.org/content/110/15/5802> (dostęp: 27.07.2017).
- Opinia 5/2014 w sprawie technik anonimizacji* (WP 216), Grupa Robocza Art. 29, 10 kwietnia 2014 r., s. 3, <http://www.giodo.gov.pl/pl/1520203/7808> (dostęp: 30.07.2017).

- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, Komisja Europejska, Bruksela 10.1.2017, <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications> (dostęp: 27.07.2017).
- Prywatność w sieci (2016/2017)*, IAB, 7.03.2017, <https://iab.org.pl/badania-i-publikacje/raport-prywatnosc-w-sieci-20162017/>, s. 6 (dostęp: 27.07.2017).
- Rok do RODO – ochrona danych osobowych oczami polskich konsumentów*, Raport Deloitte, 5.05. 2017, https://www2.deloitte.com/pl_ochrona_danych_osobowych_oczami_polskich_konumentow_Raport_Deloitte_Maj_Final1.pdf (dostęp: 2.08.2017).
- The state of the blocked web. 2017 Global Adblock Report*, PageFair, <https://pagefair.com/blog/2017/adblockreport/> (dostęp: 2.08.2017).
- Todd E., *The new ePrivacy Regulation: how will it impact your business?* CMS, Londyn 16.01.2017, <http://datonomy.eu/2017/01/16/the-new-eprivacy-regulation-how-will-it-impact-your-business/> (dostęp: 20.07.2017).
- Varian H.R., *Economic Aspects of Personal Privacy*, UC Berkeley, 6.12.1996 <http://people.ischool.berkeley.edu/~hal/Papers/privacy/> (dostęp: 27.07.2017).
- Walkowski W., *Pojęcie prywatności i przesłanki jej naruszenia*, LexVin Kancelaria Radcy Prawnego Dariusz Kostyra, 26.10.2011, <http://lexvin.pl/prawo-lexvin/3380/Pojecie-prywatnosc-i-przeslanki-jej-naruszenia> (dostęp: 20.07.2017).
- Youyou W., Kosinski M., Stillwell D., *Computer-based personality judgments are more accurate than those made by humans*, PNAS 2015, vol. 112(4), s.1036–1040, <http://www.pnas.org/content/112/4/1036> (dostęp: 27.07.2017).

* * *

Privacy as an Object of Exchange

Summary

The article presents the analysis of privacy as the object of exchange from the perspective the latest EU regulations. The latter aim at empowering consumers, particularly in the process of marketing communications. Companies will have to change their strategies in acquiring personal data for profiling. Data acquired for free before 2018 will become the object of market exchange. The research on how consumers value their data is still missing. Hence, new possibilities arise for interdisciplinary research in the economics of privacy.

Keywords: RODO, privacy, profiling.

