Nierówności Społeczne a Wzrost Gospodarczy, nr 52 (4/2017)
DOI: 10.15584/nsawg.2017.4.21 **ISSN 1898-5084**

dr Jędrzej Wieczorkowski[1]
Instytut Informatyki i Gospodarki Cyfrowej, Kolegium Analiz Ekonomicznych
Szkoła Główna Handlowa w Warszawie

Akceptacja naruszenia prywatności w erze *Big Data*

Wstęp

Podejście do prywatności podlega w ostatnim czasie szybkiej ewolucji związanej z rozwojem technologii informatycznych i komunikacyjnych. Dawniej naruszenie prywatności związane było przede wszystkim z bezpośrednimi kontaktami międzyludzkimi w niewielkich społecznościach. Życie w większych społecznościach dawało zaś poczucie anonimowości i w konsekwencji zwiększenia poczucia prywatności. Współczesne możliwości technologiczne częściowo odwracają tę sytuację – z jednej strony dzięki znaczącemu ułatwieniu komunikacji wpływają na życie w ogromnym globalnym społeczeństwie. Z drugiej strony jednak łatwość komunikacji i przetwarzania danych wpływa na niebezpieczeństwo naruszania prywatności i inwigilacji jednostek.

W szczególności problem wynika z nowych możliwości przetwarzania masowych danych dotyczących poszczególnych osób. Wcześniejsze stadium rozwoju technologii pozwalało na wykorzystywanie zbiorów danych osobowych opierających się przede wszystkim na danych zagregowanych, które powstawały z pewnym opóźnieniem w stosunku do zdarzeń (zachowań konkretnych jednostek). Analiza w czasie rzeczywistym lub zbliżonym do rzeczywistego dużych wolumenów często nieustrukturyzowanych szczegółowych danych, typowa dla przetwarzania typu *Big Data*, znacząco zmienia dotychczasową sytuację. W przypadku masowego przetwarzania i analizy danych osobowych istnieje niebezpieczeństwo istotnego naruszania prywatności rozumianej w dotychczasowym sensie. Przetwarzanie prywatnych danych (w tym osobowych, czyli umożliwiających identyfikację osoby fizycznej) może być związane z różnymi potrzebami realizowanymi w szczególności przez osoby prywatne (kontekst społeczny) oraz podmioty gospodarcze i organy administracji publicznej (kontekst instytucjonalny).

[1] Adres korespondencyjny: Szkoła Główna Handlowa w Warszawie, Instytut Informatyki i Gospodarki Cyfrowej, ul. Madalińskiego 6/8, 02-513 Warszawa, tel. 22 5649280; e-mail: jedrzej.wieczorkowski@sgh.waw.pl

Autor prowadzi od około trzech lat badania dotyczące subiektywnego zrozumienia pojęcia prywatności w kontekście stosowania nowych możliwości przetwarzania danych masowych, poczucia jego zagrożenia oraz stosowania metod ochrony prywatności. W szczególności analizowany jest problem społecznego poziomu akceptacji przetwarzania danych prywatnych w różnych (biznesowych i publicznych) celach.

Celem artykułu jest scharakteryzowanie zjawiska zmiany podejścia do prywatności wynikającego z masowego przetwarzania przez różne instytucje danych prywatnych (w tym osobowych), a w szczególności dyskusja nad poziomem akceptacji naruszenia prywatności związanego z różnorodnymi potrzebami analizy takich danych. Celem jest więc także próba odpowiedzi na pytanie o zrozumienie potrzeby prywatności, szczególnie wśród osób świadomych możliwości nowoczesnych technologii i jednocześnie zagrożeń płynących z ich stosowania. W poszczególnych rozdziałach opisano zarys historycznego i współczesnego spojrzenia na problem prywatności w kontekście przetwarzania danych osobowych, a następnie przedstawiono metodykę i wyniki przeprowadzonego badania.

Pojęcie prywatności

Pojęcie prywatności znajduje się na pograniczu zainteresowań psychologii, socjologii, filozofii, prawa, a także – w ostatnim czasie – technologii informatycznych. W literaturze rozróżniane są pojęcia prywatności i prawa do prywatności. Pierwsze określa czym jest prywatność i jak należy ją oceniać, drugie określa stopień w którym prywatność powinna być chroniona [Solove i Schwartz, 2009]. Istotne jest, aby analizując prywatność nie ograniczać się wyłącznie do prawnego spojrzenia na nią, ponieważ prawo może być ułomne lub nienadążające za rzeczywistością.

Jako historycznie pierwszą dojrzałą koncepcję prywatności traktuje się teorię przedstawioną przez Warrena i Brandeisa [1890] określoną jako *right to be let alone*. Już wówczas zwrócono uwagę na znaczenie postępu, w szczególności metod komunikacji oraz fotografii, które mogły naruszać prywatność jednostek. Ważne w koncepcji jest wydzielenie obszarów życia prywatnego i publicznego. Niedopuszczalne jest ujawnianie życia prywatnego, jeśli nie wiąże się to z interesem publicznym. Problemem staje się więc poszukiwanie równowagi pomiędzy prywatnością (interesem osobistym) a interesem publicznym.

W późniejszych latach pojęcie prywatności było stopniowo rozszerzane i wyodrębniano w nim różne typy. Przykładowo Solove [2002] do powyższej koncepcji dodaje pięć kolejnych kategorii: ograniczenie dostępu do swojej osoby; prawo zatajenia wybranych kwestii wobec innych; kontrolę nad danymi osobowymi; ochronę osobowości, indywidualności i godności; ograniczony dostęp do intymnych relacji i aspektów życia. Dopierała [2013] wyróżnia trzy podstawowe meto-

dy rozumienia prywatności: relacyjny (iteracyjny) związany z kontrolą kontaktów społecznych; informacyjny związany z zasobem i charakterem przekazywanych informacji; przestrzenny (fizyczny) dotyczący fizycznej dostępności do osoby.

Wraz z rozwojem technologii informacyjnych niektóre aspekty prywatności stają się wyjątkowo ważne. Najczęściej poruszanym obecnie tematem badań związanych z prywatnością i nowoczesnymi technologiami jest zagrożenie prywatności w Internecie, w tym w portalach społecznościowych. Podstawowy model biznesowy serwisów społecznościowych zakłada udostępnienie społeczności platformy użytkowej w zamian za dostęp do spersonalizowanych strumieni informacji współtworzonych i współdzielonych przez społeczność [Polańska i Wassilew, 2015]. W szczególności prowadzone są badania w zakresie wykorzystywanych ustawień prywatności w serwisach społecznościowych. Temat ten dotyczy pogranicza relacyjnego i informacyjnego rozumienia prywatności. Wyniki są bardzo niejednoznaczne. Z jednej strony badania przeprowadzone przez Surmę [2013] wskazują, że aktywni użytkownicy Facebooka chętnie wykorzystują dostępne ustawienia prywatności, rozumiejąc omawiany problem, z drugiej strony badania Kołodziejczyka [2014] wskazują, że ogół użytkowników dość często nie potrafi korzystać z ustawień prywatności w portalach społecznościowych. Można przypuszczać, że stosunek do prywatności zależy od umiejętności dokonywania krytycznej oceny swoich działań w Internecie wynikającej z miękkich barier w zakresie nierówności cyfrowych społeczeństwa. Zaliczane są one do tzw. podziałów cyfrowych drugiego rzędu (podziały pierwszego rzędu obejmują twarde bariery o charakterze infrastrukturalnym) i w ich skład wchodzą m.in. bariery kompetencyjne, psychologiczne, związane z wiedzą i świadomością zagrożeń [Popiołek, 2016].

Interesujące jest wyróżnienie przez Kołodziejczyka [2014] dwóch kontekstów prywatności w Internecie: społecznego i instytucjonalnego. Kontekst społeczny odnosi się do zagrożeń związanych z indywidualnymi odbiorcami informacji – zazwyczaj znanymi osobiście (np. znajomi, rodzina). Kontekst instytucjonalny odnosi się natomiast do instytucji, jako potencjalnych odbiorców prywatnych informacji, w tym administracji publicznej, reklamodawców itp. Dla większości badanych w portalach społecznościowych istotniejszy jest społeczny kontekst związany np. z dostępem osoby znajomej, lecz niepowołanej, do prywatnych danych. Prawdopodobnie zagrożenia prywatności związane z kontekstem instytucjonalnym wydają się bardziej enigmatyczne i abstrakcyjne.

Inaczej jednak sytuacja się przedstawia przy badaniu zagrożenia naruszenia prywatności związanego z przetwarzaniem danych masowych. Badania przedstawione w niniejszym artykule dotyczą przede wszystkim kontekstu instytucjonalnego, gdyż to różnorodne instytucje (publiczne i komercyjne) dysponują odpowiednimi narzędziami i technikami umożliwiającymi przetwarzanie takich danych. W badaniu skupiono się w szczególności na informacyjnym rozumieniu prywatności. Autor nie ogranicza się do zagrożeń prywatności wyłącznie w Inter-

necie, biorąc pod uwagę także inne zagrożenia wynikające z przetwarzania danych prywatnych metodami *Big Data*.

Pojęcie *Big Data*, choć dopiero się kształtuje, obejmuje szeroki zakres znaczeniowy. Może być przykładowo za Gartner Group rozumiane jako zasoby informacyjne dużych rozmiarów, szybko zmieniające się i/lub charakteryzujące się dużą różnorodnością, które wymagają efektywnych kosztowo i innowacyjnych form przetwarzania, umożliwiając poprawę wglądu w dane, podejmowanie decyzji i automatyzację procesów.

Zdaniem autora możliwe jest wyróżnienie trzech podstawowych aspektów *Big Data*: technologicznego (obejmującego możliwości, które dają IT i metody analityczne), biznesowego (obejmującego różnorodne zastosowania przetwarzania danych masowych) i społecznego (obejmującego konsekwencje społeczne tych zastosowań) [Wieczorkowski i Polak, 2014]. Aspekt społeczny poszukuje odpowiedzi, jak (często mimowolni) użytkownicy rozwiązań IT oceniają poziom zagrożenia swojej prywatności, jakie są powody, dla których są skłonni ograniczyć swoją prywatność oraz jakie podejmują działania w celu zachowania prywatności.

Obawy dotyczące zagrożenia prywatności związane z zastosowaniem nowych technologii można podzielić za Nissenbaum [2009] na trzy podstawowe kategorie: monitorowanie i śledzenie; rozpowszechnianie i publikację; agregację i analizę. Praktycznie wszystkie te kategorie do pewnego stopnia związane są z wykorzystywaniem koncepcji *Big Data*. Przykładowo monitorowanie i śledzenie służy do pozyskiwania danych na potrzeby ich dalszego przetwarzania. Rozpowszechnianie i publikacja obejmują problem ułatwienia dostępu do danych, w tym gromadzenia danych historycznych, które również są podstawą do dalszych analiz. Szczególną uwagę należy jednak zwrócić na kategorię agregacji i analizy, do której należy zaliczyć przetwarzanie danych masowych, zarówno w celu uzyskania zbiorczych zagregowanych danych, jak i analizy danych indywidualnych, przykładowo w celu profilowania użytkowników na potrzeby reklam.

Z punktu widzenia niniejszej pracy prywatność należy rozumieć w szczególności jako kontrolę przepływu informacji prywatnej. Tak rozumiana jest prywatność w koncepcji przedstawionej przez Nisseubaum [2004], która podkreśla problem kontroli dostępu do własnych informacji prywatnych zawsze w określonym kontekście społecznym – które informacje, komu, kiedy i w jakiej sytuacji mogą zostać przekazane.

Metodyka i opis badań

Na potrzeby opisanego badania rozważano zastosowanie metody pogłębionych wywiadów bezpośrednich lub przeprowadzenie ankiety, w której wskazano by z góry różne działania związane ze zjawiskiem *Big Data*. Pierwsza metoda stosowana w zbliżonych badaniach (przykładowo wspomniane wcześniej prze-

prowadzone także na polskich studentach badanie Kołodziejczyka [2014]) nie wymaga podania z góry listy działań, które potencjalnie mogą zagrozić poczuciu prywatności i na które ankietowany wyraża zgodę. Brak takiej sugestii ze strony ankietującego jest jednak także wadą ze względu na szerokość i wieloaspektowość pojęcia *Big Data*. Zdecydowano się więc przygotować wcześniej taką listę i w konsekwencji zastosować metodę ankiety z zamkniętą listą pytań.

Kolejnym problemem, przed którym stanął autor był dobór właściwej próby do przeprowadzenia badania. Jak zaznaczono, powinny to być osoby w miarę świadome zarówno możliwości nowoczesnych technologii, jak i zagrożeń płynących z ich stosowania. Jako badaną grupę, dość dobrze spełniającą takie wymagania, wybrano studentów poziomu licencjackiego uczelni ekonomicznej – Szkoły Głównej Handlowej w Warszawie. Nie jest to oczywiście grupa reprezentatywna dla ogółu społeczeństwa, lecz wymogiem w badaniu była ogólna orientacja w problematyce przetwarzania danych masowych i metod *Big Data*. Dobór ankietowanych, dzięki wystarczającemu zrozumieniu problemu, pozwalał na zadawanie dość szczegółowych pytań. Studenci uczelni o takim profilu powinni rozumieć możliwości zastosowań nowoczesnych technologii jako ich użytkownicy – zarówno prywatni, jak i przyszli użytkownicy biznesowi.

Pozostał problem doboru odpowiednich pytań, w szczególności wskazania działań, które mogą powodować poczucie zagrożenia prywatności. Wykorzystano tutaj wcześniejsze badania autora dotyczące powszechnego rozumienia pojęcia *Big Data* poprzez analizę treści artykułów prasowych [Wieczorkowski i Polak, 2014]. W konsekwencji na podstawie poruszanych w prasie problemów dotyczących społecznego aspektu *Big Data* na potrzeby niniejszego badania sformułowano listę 9 pytań związanych z przetwarzaniem danych masowych w sytuacjach, w których może dochodzić do subiektywnego poczucia naruszenia prywatności. Dobierając pytania autor starał się wskazać różne źródła danych i metody związane z przetwarzaniem danych: monitoring miejski i drogowy, analiza bilingów i danych geolokalizacyjnych, kontrola poczty elektronicznej i plików przechowywanych w chmurze, analiza ogólnodostępnych treści w Internecie, analiza danych transakcyjnych np. o zakupach, analiza danych medycznych, analiza zachowań użytkowników Internetu. Wskazano różne cele przetwarzania danych związane z szeroko rozumianym bezpieczeństwem publicznym i drogowym, finansami państwa, ochroną zdrowia oraz biznesowymi celami marketingowymi i handlowymi.

Badaniu podano 256 respondentów w trzech kolejnych semestrach. Ankieta była anonimowa, prowadzona w tradycyjnej formie papierowej, dzięki czemu uzyskiwany jest prawie pełen zwrot. Bezpośredni kontakt z ankieterem wpływa na poprawę wiarygodności jej wyników. Ostatecznie pierwsza część ankiety dotyczyła znajomości i rozumienia pojęcia *Big Data*, w celu przypisania ankietowanym ogólnego poziomu rozumienia pojęcia określanego dalej jako wskaźnik wiedzy. Dołączenie na początku ankiety tej części zmusiło także respondentów do

głębszego zastanowienia nad omawianym zjawiskiem. Druga część ankiety dotyczyła poczucia i akceptacji naruszenia prywatności związanego z różnorodnym przetwarzaniem masowych danych osobowych.

W niniejszym artykule autor skupia się na wybranych zagadnieniach akceptacji naruszeń prywatności, odnosząc się jedynie do ogólnych wyników pierwszej części ankiety. Wykorzystano klasyczną skalę Likerta. Respondenci w skali od 1 do 5 wskazywali poziom akceptacji naruszenia swojej prywatności w przypadku różnych celów przetwarzania danych. Poziom 1 oznaczał brak zgody na takie naruszenie prywatności, poziom 5 – całkowitą zgodę.

Wyniki badań

Średnie wyniki odpowiedzi na poszczególne pytania dotyczące zgody na naruszenie prywatności kształtują się w przedziale od 2,2 do 4,0 (przy możliwych odpowiedziach w przedziale od 1 do 5). Pozwala to na stwierdzenie, że ocena akceptacji naruszeń prywatności dla różnych celów dość wyraźnie się różni. Ogólnie naruszenie prywatności jest wyraźnie zauważalne, gdyż średnia ocena to 3,1. Szczegółowe wyniki przedstawiono w tabeli 1.

Najwyższy sprzeciw wobec wykorzystywania danych osobowych związany jest z ostatnimi pytaniami – dotyczącymi indywidualnego przekazu handlowego i marketingowego. Zdecydowanie najniższa zgoda na naruszenie prywatności dotyczy pytania „8. indywidualizacja treści reklamowych (np. reklamy w Internecie wyświetlane w związku z aktywnością danego użytkownika, wykrytą jego lokalizacją)" – średni wynik 2,2. Także pozostałe pytania tej grupy uzyskały wyniki wyraźnie poniżej średniej z całego badania: „7. przygotowywanie zindywidualizowanej oferty handlowej (np. dla uczestników programów lojalnościowych z wykorzystaniem analizy wcześniejszych zakupów)" – wynik 2,6 oraz „9. indywidualne oferty usług służby zdrowia (z wykorzystaniem danych o zdrowiu pacjentów)" – wynik 2,7.

Także podobnie niską akceptację uzyskał cel „4. wykrywanie naruszeń podatkowych (np. wykrywanie szarej strefy i analiza majątku z wykorzystaniem śledzenia ogólnodostępnych treści w Internecie)" – wynik 2,7. Pytanie o „5. poprawę bezpieczeństwa transportu (np. wykorzystanie monitoringu drogowego, fotoradarów itp.)" uzyskało wynik 3,2 – zbliżony do średniego.

Najwyższa zgoda na naruszenie prywatności występuje w przypadku pytania „1. zapewnienie bezpieczeństwa publicznego (np. wykorzystanie monitoringu w miejscach publicznych)" – na poziomie 4,0. Wyniki wyraźnie powyżej średniej są także dla pozostałych pytań dotyczących ogólnego bezpieczeństwa publicznego: „2. wykrywania przestępstw (np. analiza bilingów telefonicznych i danych geolokalizacyjnych)" – wynik 3,7 oraz „3. przeciwdziałanie terroryzmowi (np. częściowa kontrola poczty elektronicznej, plików przechowywanych w chmurze)" – wynik 3,4.

Tabela 1. Łączne wyniki badania zgody na naruszenie prywatności związane z różnymi celami – średnia arytmetyczna i odchylenie standardowe

Nr	Do realizacji których z poniższych celów zgodziłbyś się na naruszenie swojej prywatności (w skali od 1 do 5)?	Średnia arytmetyczna
1	Zapewnienie bezpieczeństwa publicznego (np. wykorzystanie monitoringu w miejscach publicznych)	4,0
2	Wykrywanie przestępstw (np. analiza bilingów telefonicznych i danych geolokalizacyjnych)	3,7
3	Przeciwdziałanie terroryzmowi (np. częściowa kontrola poczty elektronicznej, plików przechowywanych w chmurze)	3,4
4	Wykrywanie naruszeń podatkowych (np. wykrywanie szarej strefy i analiza majątku z wykorzystaniem śledzenia ogólnodostępnych treści w Internecie)	2,7
5	Poprawa bezpieczeństwa transportu (np. wykorzystanie monitoringu drogowego, fotoradarów itp.)	3,2
6	Poprawa funkcjonowania służby zdrowia i przeciwdziałanie zagrożeniom epidemiologicznym przy anonimizacji danych o zdrowiu pacjentów (np. dostęp do historii leczenia)	3,6
7	Przygotowywanie zindywidualizowanej oferty handlowej (np. dla uczestników programów lojalnościowych z wykorzystaniem analizy wcześniejszych zakupów)	2,6
8	Indywidualizacja treści reklamowych (np. reklamy w Internecie wyświetlane z związku z aktywnością danego użytkownika, wykrytą jego lokalizacją)	2,2
9	Indywidualne oferty usług służby zdrowia (z wykorzystaniem danych o zdrowiu pacjentów)	2,7
	Średnia całkowita	3,1

Źródło: opracowanie własne.

Także wynik znacznie powyżej średniej zanotowano w przypadku pytania „6. poprawa funkcjonowania służby zdrowia i przeciwdziałanie zagrożeniom epidemiologicznym przy anonimizacji danych o zdrowiu pacjentów (np. dostęp do historii leczenia) – wynik 3,6. To ostatnie pytanie wyraźnie odnosiło się do danych zanonimizowanych, co przy założeniu prawidłowej anonimizacji oznacza brak dostępu do danych indywidualnych, i to prawdopodobnie wpływa na tak wysoki wynik.

Odpowiedzi pokazują znacznie wyższą akceptację dla naruszeń prywatności związanych z interesem publicznym – bezpieczeństwem i dobrem ogólnym (lecz z wyjątkiem kwestii naruszeń podatkowych), niż indywidualnym przekazem w celach handlowych. Interesujące jest natomiast specyficzne podejście do podatków. Może to być specyfika polskiej kultury, w której istnieje prawdopodobnie dość wysoka akceptacja (znacznie wyższa niż w krajach Europy zachodniej i północnej) dla unikania podatków. W konsekwencji wykorzystywanie nawet ogólnodostępnych danych pochodzących z Internetu do wykrywania nadużyć podatkowych nie cieszy się wysoką akceptacją.

Należy też zwrócić uwagę na pytanie dotyczące danych wrażliwych – stanu zdrowia (pyt. 9). Dotyczyło ono zindywidualizowanego przekazu handlowego (oferta służby zdrowia), czyli zagadnień ogólnie cieszących się niską akceptacją, lecz co ciekawe wśród tych pytań (pyt. 7–9) uzyskało wynik najwyższy. Może się to wydawać dziwne, należy tutaj jednak zauważyć, że ankietowani byli ludzie młodzi, mający zazwyczaj niewielkie problemy zdrowotne. Z tego powodu mogą częściowo ignorować problemy przetwarzania danych wrażliwych o zdrowiu. Jednocześnie jednak akceptacja przetwarzania zanonimizowanych danych medycznych na potrzeby ogólnospołeczne (pyt. 6) była jednak wyraźnie wyższa.

Odchylenia standardowe dla poszczególnych pytań mieściły się w zakresie od 1,0 do 1,28. Zróżnicowanie odpowiedzi jest więc umiarkowane, ankietowani unikali zazwyczaj odpowiedzi skrajnych. Warto zwrócić uwagę na pytania z najwyższym odchyleniem standardowym odpowiedzi, gdyż wyższe zróżnicowanie odpowiedzi świadczyć może o kontrowersjach wokół danego zagadnienia. Najwyższe odchylenie standardowe dotyczyło właśnie pytania o wykorzystanie indywidualnych danych wrażliwych o zdrowiu (pyt. 9) – odchylenie 1,28. Problem ten jest więc odbierany bardzo niejednoznacznie. Także stosunkowo wysokie odchylenie standardowe 1,26 było w przypadku pytania o naruszenie prywatności w związku z przeciwdziałaniem terroryzmowi (pyt. 3). Pytanie to ponadto w porównaniu z innymi dotyczącymi dobra ogólnego otrzymało dość niski średni wynik. Jest to więc także temat dość kontrowersyjny, związany prawdopodobnie z obawami przez nadużywaniem prawa do kontroli prywatnych treści elektronicznych, dodatkowo aktualnie podsycanymi dyskusją o zmianach prawnych.

Okres badania nie był dotychczas długi, gdyż obejmował kolejne trzy semestry. Porównano jednak wyniki na przestrzeni czasu. Nie można jednak zaobserwować jednoznacznego trendu w poziomie akceptacji naruszania prywatności. Warto zaznaczyć, że w tym czasie odnotowano jednocześnie zauważalny stały wzrost znajomości zagadnienia *Big Data* (wskaźnik wiedzy). W praktyce można przypuszczać, że na zmiany poziomu akceptacji w czasie mogą mieć wpływ zjawiska, takie jak pojawiające się okresowo w prasie poruszane tematy dotyczące prywatności związane ze zmianami prawnymi lub z falami terroryzmu.

Interesujące wydaje się zbadanie korelacji pomiędzy rozumieniem problematyki *Big Data* i zgody na naruszanie prywatności. Zależność taka jest trudna do przewidzenia. Z jednej strony większa wiedza o *Big Data* to większa świadomość różnych zagrożeń, z drugiej zaś lepsze zrozumienie problematyki może przekładać się na mniejsze obawy. Do badania związku wykorzystano wskaźnik znajomości problematyki *Big Data* opracowany dla każdego respondenta na podstawie pierwszej części ankiety (wskaźnik wiedzy) i badano jego korelację z poszczególnymi pytaniami. Ogólnie korelacja jest niewielka (dla wszystkich pytań łącznie +0.09), dla poszczególnych pytań w większości przyjmuje wartości bliskie zera (od –0.04 do +0.12). Najsilniejsza korelacja (+0,12) występuje w przypadku pytania „6. poprawa funkcjonowania służby zdrowia i przeciwdziałanie zagrożeniom

epidemiologicznym przy anonimizacji danych o zdrowiu pacjentów (np. dostęp do historii leczenia)". W tym przypadku chodzi prawdopodobnie o prawidłowe zrozumienie zagadnień anonimizacji i agregacji danych.

Podsumowanie i wnioski

Pojęcie prywatności ewoluuje wraz z rozwojem technologii informacyjnych. Zmienia się także świadomość dotycząca zagrożenia prywatności wynikającego z masowego przetwarzania danych prywatnych, w tym osobowych. Zaprezentowane badanie miało na celu ocenę poziomu akceptacji naruszenia prywatności wynikającego przede wszystkim z przetwarzania takich danych metodami *Big Data*. Znacząco wyższa akceptacja dla naruszenia prywatności występuje w przypadku pytań dotyczących potrzeb ogólnospołecznych – szeroko rozumianego interesu publicznego. Wyraźnie niższy poziom akceptacji jest dla pytań o wykorzystanie danych na potrzeby handlowe i reklamowe. Mimo że zależność ta nie jest wyraźnie skorelowana ze zrozumieniem metod *Big Data*, respondenci zapewne rozumieją współczesne zagrożenia takie jak terroryzm i inne przestępstwa i zdają sobie sprawę ze skuteczności przeciwdziałania im z wykorzystaniem metod masowego przetwarzania danych osobowych.

W kontekście wyników badania można stwierdzić, że respondenci mają dość wysokie zaufanie do instytucji państwa (wyższy poziom zgody na naruszenie prywatności w celach ogólnospołecznych). Istotna więc wydaje się dbałość o jego zachowanie poprzez budowanie zaufania do systemu prawnego i praktyki jego przestrzegania. Jednocześnie, ze względu na niższy poziom zgody na naruszenie prywatności w celach komercyjnych, prawo powinno zapewniać wystarczającą ochronę prywatności w odniesieniu do takich celów. Problemem współczesnego świata jest fakt, że ogromna zcentralizowana wiedza o obywatelach znajduje się w rękach kilku firm komercyjnych, dla których celem działalności nie są korzyści społeczne, lecz wypracowanie zysku.

Bibliografia

Dopierała R., 2013, *Prywatność w perspektywie zmiany społecznej*, Zakład Wydawniczy Nomos, Kraków.

Gartner Group, http://www.gartner.com/it-glossary/big-data/ (dostęp: 17.03.2017 r.).

Kołodziejczyk Ł., 2014. *Prywatność w Internecie: postawy i zachowania dotyczące ujawniania danych prywatnych w mediach społecznych*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa.

Nissenbaum H., 2004, *Privacy as Contextual Integrity,* „Washington Law Review", 79, s. 101–139.

Nissenbaum H., 2009, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Polańska K., Wassilew A, 2015, *Analizy Big Data w serwisach społecznościowych,* „Nierówności Społeczne a Wzrost Gospodarczy", 4/2015 cz. 2, red. nauk. M.G. Woźniak, wyd. UR, Rzeszów, s. 117–128, https://dx.doi.org/10.15584/nsawg.2015.4.2.11.

Popiołek M., 2016, *Nierówności cyfrowe i podziały cyfrowe drugiego rzędu jako wyzwanie dla gospodarki opartej na wiedzy,* „Ekonomiczne Problemy Usług", 122, s. 115–123, https://dx.doi.org/10.18276/epu.2016.122-10.

Solove D.J., 2002, *Conceptualizing Privacy*, „California Law Review", Vol. 90, Issue 4, pp. 1087–1155, http://dx.doi.org/10.2307/3481326.

Solove D.J., Schwartz P.M., 2009, *Information Privacy Law*, Aspen Publishers.

Surma J., 2013, *The Privacy Problem in Big Data Applications: An Empirical Study on Facebook* [w:] *ASE/IEEE International Conference on Social Computing*, pp. 955–958.

Warren S.D., Brandeis L.D., 1890, *The Right to Privacy,* „Harvard Law Review", Vol. IV, No. 5, http://dx.doi.org/10.2307/1321160.

Wieczorkowski J., Polak P., 2014, *Big Data: Three-aspect approach,* „Online Journal of Applied Knowledge Management", Vol. 2, Issue 2, International Institute for Applied Knowledge Management, pp. 182–196, http://www.iiakm.org/ojakm/articles/2014/volume2_2/OJAKM_Volume2_2pp182-196.pdf (dostęp: 12.07.2016 r.).

Streszczenie

Rozwój technologii informacyjnych dający nowe możliwości – biznesowe oraz związane z życiem prywatnym – powoduje także różnorodne zagrożenia wynikające z przetwarzania masowych danych prywatnych, w szczególności danych osobowych. Współczesne społeczeństwo informacyjne mierzy się więc z problemem znalezienia równowagi pomiędzy wykorzystywaniem nowych możliwości w gospodarce i życiu codziennym a ograniczaniem ich negatywnych konsekwencji w obszarze naruszenia prywatności jednostki.

Społeczny aspekt zjawiska *Big Data*, a w szczególności zagadnienia związane z prywatnością, jest przedmiotem badań autora. W ich ramach poszukuje się odpowiedzi, jak użytkownicy rozwiązań IT opierających się na przetwarzaniu danych masowych oceniają poziom zagrożenia swojej prywatności i jakie są powody, dla których są skłonni ograniczyć swoją prywatność. W artykule przedstawiono wyniki takich badań, stawiając za cel opis zmiany podejścia do prywatności w kontekście instytucjonalnym w zakresie akceptacji naruszenia prywatności.

Zaobserwowano, że znacząco wyższa akceptacja występuje w przypadku potrzeb ogólnospołecznych, w szczególności bezpieczeństwa publicznego, niż w przypadku wykorzystywania prywatnych danych na potrzeby indywidualnego przekazu reklamowego. Badania mają pomóc w zrozumieniu szerokiego problemu prywatności w świecie, w którym automatyczne masowe przetwarzanie danych prywatnych, w tym osobowych staje się codziennością.

Słowa kluczowe: prywatność, *Big Data*, dane osobowe, inwigilacja

The acceptance of privacy violations in the era of *Big Data*

Summary

The development of information technology gives new business and private opportunities. It also causes a variety of threats resulting from the processing of big private data, particularly personal

data. The modern information e-society have the problem of finding a balance between exploiting new opportunities (in the economy and everyday life) and reducing the negative consequences of individual privacy violations. The social aspect of the big date phenomenon and in particular privacy issues is the subject of authors research. What is IT and *Big Data* users attitude to threat to their privacy? What are the reasons that they agree to limit their privacy?

The article presents the results of this research. The goal of the paper is to describe a change in approach to privacy and the acceptance of privacy violations. It has been observed that significantly higher acceptance occurs in the case of social needs, especially public safety, than in the case of using private data for individual advertising. Research will help to understand the issue of privacy in a world with automatic mass-processing of personal and private data.

Keywords: privacy, *Big Data*, personal data, surveillance

JEL: O33, L86, D80, D83, K24