Malwina Popiołek

Uniwersytet Jagielloński
Wydział Zarządzania i Komunikacji Społecznej
Katedra Zarządzania, Ekonomiki Mediów i Reklamy
e-mail: malwinapopiolek@gmail.com

Jędrzej Wieczorkowski

Szkoła Główna Handlowa w Warszawie
Instytut Informatyki i Gospodarki Cyfrowej
Kolegium Analiz Ekonomicznych
e-mail: jedrzej.wieczorkowski@sgh.waw.pl

Zarządzanie prywatnością w internecie – wybrane problemy metodologiczne

Kody JEL: B40, B49, D83, O33

Słowa kluczowe: prywatność, cyberbezpieczeństwo, technologie informacyjno-komunikacyjne

Streszczenie. W artykule podjęto próbę uchwycenia i opisania najważniejszych problemów metodologicznych związanych z badaniem zarządzania prywatnością w internecie. Ukazano różnorodność teoretycznych kontekstów zagadnienia prywatności online, a także możliwe podejścia badawcze w różnych naukach: informatyce i naukach technicznych, prawnych, społecznych. Pokazano możliwe sposoby pozyskiwania danych (metody ilościowe i jakościowe), a także rodzaje badań z podziałem ze względu na cel – eksploracja, opis, wyjaśnienie. Przedstawiono także nowe metody badania prywatności, np. netnografię.

Wprowadzenie

Problem prywatności w ostatnich latach staje się coraz częstszym tematem dyskusji zarówno w publikacjach naukowych, jak i w prasie popularnej. Wiąże się to przede wszystkim z rozwojem technologii informacyjno-komunikacyjnych (ICT) i zastosowaniem jej w codziennym życiu. Wykorzystywanie internetu skutkuje ciągłym pozostawianiem śladów swojej aktywności, które jako dość dobrze ustrukturyzowane dane, mogą być łatwo wykorzystywane do różnych celów. Są to dane prywatne, często oso-

bowe, w tym wrażliwe, różnorodne informacje o zainteresowaniach, kontaktach z innymi osobami, codziennej aktywności itp. Nad takimi danymi aktywny internauta nie ma pełnej kontroli.

Coraz częściej spotkać można się z opiniami, że przeciętny użytkownik technologii informacyjno-komunikacyjnych ma nierówne szanse i przegraną pozycję względem podmiotów działających w branży technologicznej. Często bowiem nie jest on nawet dostatecznie świadomy zagrożeń dla prywatności, towarzyszących korzystaniu z różnych usług online (Kuczyński, 2009). Przykładem może być chociażby popularny na całym świecie serwis społecznościowy Facebook, z którego korzystanie, z różnych względów, postrzegane jest jako konieczność, a jego polityka prywatności budzi liczne kontrowersje (zob. Papińska-Kacperek, Polańska, 2016; Giermak, Popiołek, 2014).

Rodzi się pytanie o zrozumienie zmieniającego się zakresu prywatności, o stopień akceptacji tej sytuacji oraz o pożądany poziom prywatności. Zagadnienie wydaje się szczególnie interesujące wśród młodych osób, często określanych mianem cyfrowych tubylców (Prensky, 2001) wychowanych w świecie wszechobecnej technologii informacyjno-komunikacyjnej. Niniejszy artykuł stanowi próbę uchwycenia najważniejszych problemów metodologicznych, z jakimi można się zetknąć podejmując próby badawcze w obszarze zarządzania prywatnością online. Za cel autorzy powzięli pokazanie różnorodności podejść do tego zagadnienia, przedstawienie możliwych sposobów badania prywatności w internecie, a dzięki temu także teoretyczne wprowadzenie do własnych badań. Dokonano przeglądu literatury odnoszącej się do zagadnienia prywatności online, wyróżniając możliwe warianty badawcze. Wyciągnięto także pierwsze wnioski z dotychczasowych, własnych badań nad zarządzaniem prywatnością w sieci.

1. Zagadnienie prywatności – różnorodność ujęć teoretycznych

Pojęcie prywatności jest oczywiście znacznie starsze od współczesnych technologii informacyjno-komunikacyjnych (ICT), lecz w porównaniu z innymi prawami człowieka jest stosunkowo młode (zob. Pryciak, 2010). Prywatność jest ściśle powiązana z poziomem oraz stylem życia. Inaczej postrzega się prywatność przykładowo w obecnej europejskiej kulturze dużych zamożnych miast, inaczej – w kulturach tradycyjnych ubogich wiejskich społeczności z wielopokoleniowymi rodzinami, jeszcze inaczej była postrzegana kilka wieków temu. I można postawić tezę, że w ostatnich kilku lat podejście do prywatności wśród osób z szerokim dostępem do technologii ICT także gwałtownie się zmienia. Widać jednak, że ewolucja prywatności jest rzeczą w pełni naturalną, a podejście zależy od kultury, zmienia się wraz z zamożnością społeczeństwa i postępem technicznym.

Koncepcję prywatności opracowaną przez Warrena i Brandeisa (1890), którą określono jako prawo do bycia pozostawionym w spokoju (*right to be let alone*), można traktować jako pierwszą dość dojrzałą jej teorię. Tak jak obecnie jako zagrożenie prywatności traktowane są technologie ICT, wówczas podchodzono tak do fotografii. Tym

niemniej jako element ponadczasowy tej teorii należy uznać wydzielenie obszarów życia – prywatnego i publicznego. Już wówczas uznano, że niedopuszczalne jest ujawnianie życia prywatnego, jeśli nie wiąże się to z interesem publicznym. W kolejnych latach podejście do prywatności ewoluowało, jej ochrona stawała się coraz silniejsza i stopniowo prywatność stała się istotnym elementem praw człowieka i godności ludzkiej.

Trudno o jednoznaczną definicję prywatności, ze względu na jej wieloaspektowy charakter: m.in. prawny, filozoficzny, socjologiczny, technologiczny. Przykładowo można wyróżnić trzy podstawowe metody traktowania prywatności: relacyjna (iteracyjny) związana z kontrolą kontaktów społecznych; informacyjna związana z zasobem i charakterem przekazywanych informacji oraz przestrzenna (fizyczna) dotyczący fizycznej dostępności do osoby (Dopierała, 2013). Z punktu widzenia zachowania prywatności w internecie istotne są dwa pierwsze podejścia. W tym kontekście można rozumieć prywatność jako kontrolę przepływu informacji prywatnej – sprawowanie kontroli nad informacjami dotyczącymi jednostki, a w szczególności nad tym, w jakim zakresie dana informacja jest udostępniana innym (Westin, 1967). Kontrolę dostępu do takich informacji należy rozpatrywać zawsze w określonym kontekście społecznym – które informacje, komu, kiedy i jakiej sytuacji mogą zostać przekazane (Nisseubbaum, 2004).

Zakładając że użytkownicy internetu mają potrzebę zachowania pewnego poziomu prywatności, zapewne podejmują jakieś działania z tym związane. Można więc mówić o praktykach zarządzania prywatnością. Przykładowo A. Westin (1996) wyróżnił postawy: fundamentalistyczną (najsilniejsza ochrona kosztem rezygnacji z korzyści), beztroska (najsłabsza ochrona), pragmatyczną (každorazowa ocena korzyści i kosztów udostępnienia prywatnych informacji). Należy jednak pamiętać, że np. serwisy społecznościowe są komercyjnymi przedsięwzięciami, a ich podstawowy model biznesowy zakłada udostępnienie platformy w zamian za dostęp do spersonalizowanych informacji współtworzonych przez społeczność (Polańska, Wassilew, 2015). Jednocześnie niejednokrotnie korzystanie z takich serwisów przestaje być wyborem, a staje się koniecznością ze względu na sytuację zawodową lub kontakty towarzyskie. Bardzo uciążliwe jest także wykorzystywanie internetu jako źródła informacji bez pozostawiania śladów w postaci danych prywatnych. Pytaniem więc pozostaje jakie postawy przyjmują obecnie młodzi ludzie wobec prywatności w internecie i jak badać te postawy?

2. Badanie prywatności w internecie – perspektywy badawcze i podejścia metodologiczne

Zainteresowanie problematyką zarządzania prywatnością w internecie systematycznie wzrasta. Można przypuszczać, że wraz z rozwojem i upowszechnieniem dostępu do ICT trend ten będzie się utrzymywał. Wśród publikacji naukowych polskich autorów poświęconych temu zagadnieniu pojawiają się głównie prace eksploracyjne (zob. Surma, 2013; Koło-

dzieczyk, 2014; Wieczorkowski, Pawełoszek, 2016); rzadko znaleźć można monografie, w których autorzy opisywaliby zagadnienie kompleksowo (zob. Dopierała, 2013).

Zagadnienie zarządzania prywatnością w internecie jest dość problematycznym obszarem refleksji naukowo-badawczej. Wynika to przede wszystkim z dużej transdyscyplinarności. Wiele problemów badawczych, które mieszczą się w ramach szeroko rozumianej refleksji nad społeczeństwem informacyjnym ma charakter inter- lub transdyscyplinarny, co może być postrzegane jako pewnego rodzaju bariera metodologiczna (zob. Sienkiewicz, 2016). Refleksja nad zarządzaniem prywatnością online rozwija się równolegle w ramach wielu dyscyplin, w tym przede wszystkim:

1. W naukach informatycznych i technicznych – pojęcie prywatności wiąże się głównie z metodami ochrony danych w przestrzeni cyfrowej, a więc zagadnieniem bezpieczeństwa teleinformatycznego, rozumianego jako ochrona systemów teleinformatycznych przed włamaniami, kradzieżą czy też nieuprawnionym wykorzystaniem danych (Klimek, 2015, s. 96; Malko, Lis, 2016, s. 182–185).
2. W naukach prawnych – dotyczy prawnych aspektów związanych z ochroną i udostępnianiem informacji online. W tym ujęciu uwaga skupia się zwykle na analizowaniu praktyk podmiotów oferujących swoje usługi w sieci i ich ocenie pod kątem zgodności z obowiązującym stanem prawnym. Szeroko analizowana jest także kwestia zasadności wykorzystywania prywatnych danych pozyskanych online przez różne organy państwowe, np. dla potrzeb zapewnienia szeroko rozumianego bezpieczeństwa (Świeboda, 2013).
3. W naukach społecznych – bada się szerokie spektrum przyczyn i konsekwencji związanych z przemianami w obszarze prywatności, a także wpływem internetu i ICT na rodzaj i charakter tych przemian. Samo zarządzanie prywatnością rozumiane jest najczęściej jako jedna z e-umiejętności czy e-kompetencji i analizowane z perspektywy użytkowników internetu. Dominują tu przede wszystkim badania socjologiczne (Mazurek, Zając, Rakocy, 2007), psychologiczne (Sanecka, 2014), pedagogiczne (Czopek, 2015), politologiczne (Lakomy, 2013), a także medioznawcze.

Mamy zatem do czynienia z dużą różnorodnością perspektyw badawczych, jak również wielorakim definiowaniem pojęcia prywatności online i sytuowaniem jej raz w obszarze cyberbezpieczeństwa¹, innym zaś razem w obszarze e-kompetencji cyfrowych.

Z metodologicznego punktu widzenia należałoby wyodrębnić dwa główne podejścia do badania prywatności online – podejście ilościowe i jakościowe. Pierwsze ma przede wszystkim na celu stwierdzenie czy jakieś zjawiska występują lub nie,

¹ Pojęcie cyberbezpieczeństwa najczęściej kojarzone jest z tzw. bezpieczeństwem teleinformatycznym. W anglojęzycznym nazewnictwie występują dwa terminy: *computer security* i *cyber security*, przy czym pierwsze dotyczy głównie systemów informatycznych, drugie odnosi się do bezpieczeństwa w cyberprzestrzeni w sensie bardziej ogólnym.

a także określenie skali ich występowania (często na poziomie makro). Dominować będą w nim badania kwestionariuszowe w formie ankiet przeprowadzane na dużych reprezentatywnych próbach populacji. Przykładem mogą być analizy zrobione na zlecenie różnych instytucji, np. Generalnego Inspektoratu Ochrony Danych Osobowych (*Raport z badań...*).

W badaniach jakościowych nie analizuje się skali zjawisk, a ich złożoność, przyczyny i ewentualne konsekwencje (zob. Flick, 2012; Silverman, 2012). Wybór metod jest tu dość szeroki, poczynwszy od obserwacji i metod etnograficznych, poprzez indywidualne wywiady pogłębione, aż do zogniskowanych wywiadów grupowych. W tego typu badaniach dobór próby ma często charakter celowy lub arbitralny, a jej struktura nie musi być reprezentatywna (Babbie, 2008, s. 212).

Z względu na cel prowadzonych badań można mówić o trzech głównych przyczynach poznawczych badania prywatności w internecie (Babbie, 2008, s. 107–110):

1. Badania eksploracyjne – ich celem jest dokonanie wstępnego rozeznania w określonym obszarze refleksji. Podejście eksploracyjne jest częste, zwłaszcza wówczas, gdy przedmiot badań jest nowym zjawiskiem. Zagadnienie zarządzania prywatnością online niewątpliwie takim zjawiskiem jest, toteż w literaturze dominują właśnie prace o charakterze eksploracyjnym (np. prezentujące wyniki badań pilotażowych. Badania te mogą wprawdzie zawierać zarówno elementy opisu, jak i wyjaśnienia zjawisk, stanowią one jednak wstęp do dalszych pogłębionych badań, a nie próbę uzyskania ostatecznych odpowiedzi (Babbie, 2008, s. 107). Praktyka badawcza pokazuje, że w przypadku eksploracji poszczególnych zagadnień stosowane są różne warianty metod, zarówno ilościowe, jak i jakościowe, przy czym w obydwu przypadkach wyniki raczej nie dają się ekstrapolować na ogół populacji.
2. Badania deskryptywne (opisowe) – ich celem jest dokonanie szczegółowej charakterystyki badanego przedmiotu. Szuka się zatem odpowiedzi na pytania: co, ile, kiedy, gdzie? Dominuje podejście ilościowe. Aby dokonać opisu tego jak zmieniają się preferencje w zakresie ustawień prywatności, np. ze względu na wiek, płeć, czy wykształcenie badanej populacji, sięgamy właśnie po badania ilościowe.
3. Badania eksplanacyjne (wyjaśniające) – ich celem jest udzielenie odpowiedzi na pytania dotyczące przyczyn zjawisk, a także próba zrozumienia ich złożoności. Dominować będzie w nich podejście jakościowe, a więc np. obserwacja, badania terenowe, wywiady, czy podejście etnograficzne (np. netnografia). Wywiady stanowią bogate źródło informacji na temat motywów jakimi kierują się użytkownicy usług online udostępniający swoje prywatne dane w różnych sytuacjach. Przede wszystkim jednak wywiady indywidualne czy zogniskowane wywiady grupowe pozwalają zorientować się na ile prywatność jest dla badanych istotna, jaka jest ich świadomość w zakresie zagrożeń związanych z korzystaniem z usług online, a także czy postrzegają oni prze-

strzeń wirtualną jako przestrzeń prywatną czy publiczną. W badaniu prywatności ciekawym sposobem gromadzenia danych może być także nowa metoda jaką jest netnografia (zob. Kozintes, 2012).

3. Netnografia w badaniu prywatności online

Netnografia, jak pisze D. Jemielniak (2013), to metoda badań wirtualnych oparta na bezpośrednim zastosowaniu zespołu technik i metod stosowanych w repertuarze antropologicznym. Początkowo miała charakter pomocniczy i polegała na uzupełnianiu danych służących triangulacji, np. przez wzbogacenie informacji z wywiadów o kontekst stron internetowych dla danej zbiorowości. Współcześnie etnografie wirtualne dotyczą przede wszystkim samodzielnych badań społeczności internetowych, choć naturalnie nadal mogą mieć zastosowanie także wtedy, gdy po prostu internet jest jednym z wielu narzędzi badawczych, a także gdy analizuje się zjawiska zachodzące zarówno online, jak i offline.

Stosując netnografię możemy np. badać zachowania użytkowników serwisów społecznościowych, forów przez analizę materiałów przez nich udostępnianych. Można wówczas dokonać jakościowej oceny zdjęć i innych materiałów upublicznianych przez internautów, oceniając przy tym stopień autoujawnienia (inaczej samoujawnienia – *self-disclosure*) i stopnia zachowania prywatności w określonych sytuacjach online.

Wydaje się, że w przypadku badań nad prywatnością w internecie dla uzyskania najbardziej miarodajnych efektów korzystne jest zwiększanie rzetelności badań poprzez tzw. triangulację metod (zob. Denzin, 2006), a więc łączenie różnych sposobów pozyskiwania danych. Takie podejście zastosował np. Ł. Kołodziejczyk (2014), przeprowadzając najpierw badanie kwestionariuszowe, a następnie badanie jakościowe w postaci wywiadów pogłębionych, dzięki czemu udało mu się uzyskać lepszy wgląd w badane zagadnienie, zwłaszcza w kwestii definiowani pojęcia prywatności przez badanych, a także określenia jej istotności.

Projektując badanie nad prywatnością online, prócz wspomnianej już świeżości zagadnienia, należy wziąć pod uwagę także dużą dynamikę zachodzących procesów. Warto zatem w badaniach przyjmować podejście indukcyjne (Babbie, 2008, s. 67–70). Należałoby wówczas przeprowadzić badania jakościowe, które pozwolą na sformułowanie wstępnych kategorii badawczych, pól konceptualnych, a także ewentualnych hipotez, które będzie można następnie weryfikować dalszymi badaniami. Stosując podejście dedukcyjne, można bowiem wpaść w pułapkę przyjmowania niewłaściwych założeń i testowania błędnie postawionych hipotez. Dla przykładu – często badając sposoby zarządzania informacją prywatną, zakładamy *a priori*, że badani przez nas użytkownicy usług online cenią sobie prywatność i uważają ją za istotną wartość, tymczasem niekoniecznie musi tak być. Częstym problemem jest też odwoływanie się do teorii innych badaczy, które straciły na aktualności. Przestrzeń internetowa dynamicznie się zmienia, zatem twierdzenia sprzed kilku czy nawet kilkunastu lat, mogą współcześnie mało przystawać do rzeczywistości. Podejście indukcyjne pozwala na uniknięcie tego typu pułapek.

4. Podsumowanie i kierunki dalszych badań

W celu rozpoznania problematyki postaw wobec prywatności w internecie autorzy prowadzą obecnie eksploracyjne badanie kwestionariuszowe, którego celem jest określenie subiektywnego poziomu zagrożenia prywatności respondentów związanego z przetwarzaniem wskazanych danych prywatnych, w szczególności tych pochodzących z internetu. Badany jest także poziom akceptacji ankietowanych dla naruszenia prywatności, związanego z różnorodnymi podanymi celami przetwarzania, w tym biznesowymi i ogólnospołecznymi, a także ewentualnie stosowane metody służące zachowaniu prywatności lub anonimowości. Szczegółowe omówienie dotychczasowych wyników wykracza poza cele niniejszego artykułu, lecz warto wskazać wybrane problemy już widoczne przy realizacji badania.

Ponieważ w badaniu ankietowym bardzo istotne są dobór, precyzja i jednoznaczność pytań, a także ustandaryzowanie odpowiedzi, posłużono się zamkniętymi pytaniami z odpowiedziami w klasycznej 5-stopniowej skali Likerta. Przykładowo, w pierwszej części kwestionariusza z góry podano listę metod i rodzaj przetwarzanych danych, np. poziom poczucia zagrożenia związany z gromadzeniem informacji o zachowaniach użytkowników w internecie, w tym informacji o odwiedzanych stronach. Przy konstruowaniu pytań dokonano uprzednio analizy literatury przedmiotu oraz prasy popularnej (a więc, jak wcześniej zaznaczono, źródeł, które szybko mogą ulec dezaktualizacji). Wątpliwość może zatem budzić to, na ile postawione pytania odpowiadają rzeczywistości tym problemom naruszania prywatności w internecie, które są ważne dla respondentów w momencie przeprowadzania badania. I przede wszystkim, jak ankietowani w ogóle tę prywatność rozumieją, czy jest to dla nich istotna wartość. W praktyce przyjęto więc założenie, że tak – prywatność jest wartością. Analizując odpowiedzi respondentów, niewątpliwie dużo można dowiedzieć się o ich postawach. Możliwe jest tworzenie różnych statystyk, np. korelacji pomiędzy poszczególnymi elementami. Przy próbie odpowiedniej wielkości można też grupować ankietowanych według różnych cech demograficznych (np. płci). Mimo zalet powyższego ilościowego podejścia eksploracyjnego, należy zdawać sobie sprawę z jego ograniczeń, np. takich, że badanie nie pozwala w pełni zrozumieć przyczynowości zjawiska oraz poznać motywacji respondentów.

Biorąc pod uwagę charakterystykę poszczególnych podejść metodologicznych przy badaniu prywatności w sieci, należy rozważyć pracę w interdyscyplinarnych zespołach badawczych. Możliwe jest łączenie metod stosowanych w różnych dziedzinach, takich jak socjologia i demografia. W szczególności wskazane jest umiejętne łączenie metod ilościowych i jakościowych. Podejście takie pozwala bowiem spojrzeć na badane zagadnienie w sposób szeroki, uwzględniając szerokie spektrum istotnych czynników. W tym kierunku autorzy zamierzają prowadzić swoje dalsze badania.

Bibliografia

- Babbie, E. (2008). *Podstawy badań społecznych*. Warszawa: Wydawnictwo Naukowe PWN.
- Czopek, J. (2016). Bezpieczeństwo i ochrona prywatności młodzieży w internecie w kontekście edukacji medialnej. *Zeszyty Naukowe Wyższej Szkoły Humanitas. Pedagogika*, 12, 67–74.
- Denzin, N. (2006). *Sociological Methods: A Sourcebook*. Aldine Transaction.
- Dopierała, R. (2013). *Prywatność w perspektywie zmiany społecznej*. Kraków: Zakład Wydawniczy Nomos.
- Flick, U. (2012). *Projektowanie badania jakościowego*. Warszawa: Wydawnictwo Naukowe PWN.
- Giermak, M., Popiołek, M. (2014). Media społecznościowe a prawo do informacji publicznej. W: W. Opiola, M. Popiołek (red.), *Media społecznościowe. Nowe formy ekspresji politycznej*. Toruń: Wydawnictwo Adam Marszałek.
- Jemielniak, D. (2013). Netnografia czyli etnografia wirtualna. *Prakseologia*, 152, 97–116.
- Klimek, M. (2015). Bezpieczeństwo teleinformatyczne i bezpieczeństwo informacji w przedsiębiorstwach budownictwa inżynierskiego. *Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach*, 105, 95–102.
- Kołodziejczyk, Ł. (2014). *Prywatność w internecie*. Warszawa: Wydawnictwo SPB.
- Kozintes, R.V. (2012). *Netnografia. Badania etnograficzne online*. Warszawa: Wydawnictwo Naukowe PWN.
- Kuczyński, G. (2009). Ochrona prywatności w internecie. *Marketing w Praktyce*, 3, 30–32.
- Lakomy, M. (2013). Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii. *E-politikon*, 6, 100–141.
- Malko, J., Lis, R. (2016). Cyberbezpieczeństwo systemów zabezpieczeń i sterowania. *Przegląd Elektrotechniczny*, 1, 182–185.
- Mazurek, P., Zając, J., Rakocy, K. (2007). Między inwigilacją a uwiedzeniem: Użytkownicy internetu wobec praktyk gromadzenia i przetwarzania danych. *Studia Socjologiczne*, 3 (186).
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79, 101–139.
- Papińska-Kacperek, J., Polańska, K. (2016). Publiczne zasoby informacyjne w mediach społecznościowych. *Ekonomiczne Problemy Usług*, 122, 93–102.
- Polańska, K., Wassilew, A. (2015). Analizy big data w serwisach społecznościowych. *Nierówności Społeczne a Wzrost Gospodarczy*, 4 (2), 117–128.
- Prensky, M. (2001). Digital Natives, Digital Immigrants: Do They Really Think Differently? *On the Horizon*, 9 (6), 1–6.
- Pryciak, M. (2010). Prawo do prywatności. *Studia Erasmiana Wratislaviensia*, 4.
- Raport z badań na zlecenie GIODO: Postrzeganie zagadnień związanych z ochroną danych i prywatności przez dzieci i młodzież. Pobrano z: http://www.giodo.gov.pl/1520124/id_art/6914/j/pl.
- Sanecka, E. (2014). Samoujawnianie online. Przegląd teorii i wyników wcześniejszych badań. W: K. Tucholska, M. Wysocka-Pleczyk (red.), *Człowiek zalogowany*. Kraków: Biblioteka Jagiellońska.

- Sienkiewicz, P. (2016). Metodologiczne aspekty badań nad rozwojem społeczeństwa informacyjnego. *Ekonomiczne Problemy Usług*, 123, 311–319.
- Silverman, D. (2012). *Prowadzenie badań jakościowych*. Warszawa: Wydawnictwo Naukowe PWN.
- Surma, J. (2013). *The Privacy Problem in Big Data Applications: An Empirical Study on Facebook*. ASE/IEEE International Conference on Social Computing.
- Świeboda, H. (2013). Problem prywatności w społeczeństwie informacyjnym. *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług*, 105/2, 93–106.
- Warren, S.D., Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, 5 (5).
- Westin, A. (1967). *Privacy and freedom*. New York: Athenaeum.
- Westin, A. (1996). Privacy in the Workplace: How Well Does American Law Reflect American Values? *Chicago-Kent Law Review*, 72 (271), 271–283.
- Wieczorkowski, J., Pawełoszek, I. (2016). Big data privacy concerns in the light of survey results. *IADIS International Journal on WWW/Internet*, 14 (1), 70–85. Pobrano z: <http://www.iadisportal.org/ijwi/papers/2016141106.pdf>.

ONLINE PRIVACY MANAGEMENT – SELECTED METHODOLOGICAL ISSUES

Keywords: privacy, cyber security, online privacy management

Summary. The article describes major methodological problems associated with the study of online privacy management. It deals with the problem of theoretical contexts of the subject, as well as the possible research approaches in different fields of science, e.g.: computer and engineering sciences, legal sciences and social sciences. The paper describes possible ways of empirical data collecting (quantitative and qualitative methods), as well as the types of research in this area divided by purpose: exploration, description, explanation. It describes also new ways of research which are possible to study privacy management on the net, e.g. netnography.

Translated by Malwina Popiołek and Jędrzej Wieczorkowski

Cytowanie

Popiołek, M., Wieczorkowski, J. (2017). Zarządzanie prywatnością w internecie – wybrane problemy metodologiczne. *Ekonomiczne Problemy Usług*, 1 (126/2), 231–239. DOI: 10.18276/epu.2017.126/2-23.