Jędrzej Wieczorkowski

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

Malwina Popiołek

Uniwersytet Jagielloński
Wydział Zarządzania i Komunikacji Społecznej
Katedra Zarządzania, Ekonomiki Mediów i Reklamy
m.popiolek@uj.edu.pl

Podejście do prywatności wśród studentów polskich uczelni – badanie porównawcze

Kody JEL: C89, L86, O33

Słowa kluczowe: prywatność, technologie informacyjno-komunikacyjne, *big data*

Streszczenie. Artykuł zawiera wyniki autorskich badań ankietowych nad postrzeganiem prywatności wśród polskich studentów w kontekście nowych metod masowego przetwarzania danych prywatnych, w tym osobowych. Jego celem jest stwierdzenie, czy występują różnice pomiędzy postawami studentów w zależności od różnych typów uczelni, także od wielkości ośrodka akademickiego. Przedstawiono postrzeganie poziomu naruszenia prywatności związanego ze wskazanymi współczesnymi zjawiskami oraz akceptacji naruszenia prywatności wynikającego z przetwarzania danych na różne publiczne i komercyjne potrzeby.

Wprowadzenie

Z uwagi na istotne zmiany w technologiach informatycznych szybko zmienia się podejście do prywatności. Od czasu pochodzącej jeszcze z XIX wieku teorii *right to be let alone*, wydzielającej obszary życia prywatnego i publicznego (Warren, Brandeis, 1890) bardzo zmieniło się postrzeganie prywatności. Obecnie w erze *big data* typowe jest określanie jako danetyzacja (*datafication*) zjawisko pasywnego zbierania różnorodnych danych (w szczególności osobowych i pozostałych danych prywatnych) przy oka-

zji przetwarzania innych danych, bez znajomości celu ich późniejszego wykorzystania (Mayer-Schonberger, Cukier, 2013). Obecnie należy więc prowadzić rozważania w kontekście możliwości masowego przetwarzania danych prywatnych. Kontrolę dostępu do takich danych powinno się rozpatrywać zawsze w określonym kontekście społecznym – które informacje, komu, kiedy i w jakiej sytuacji mogą zostać przekazane (Nisseubaum, 2004), a samą prywatność można rozumieć jako kontrolę przepływu informacji prywatnej, a w szczególności stopień, w jakim zakresie dana informacja jest udostępniana innym (Westin, 1967).

Typowym aktualnym tematem badawczym w obszarze prywatności są serwisy społecznościowe. Ich model biznesowy zakłada udostępnienie platformy użytkowej w zamian za dostęp do spersonalizowanych strumieni informacji współtworzonych i współdzielonych przez społeczność (Polańska, Wassilew, 2015). Stąd badania serwisów społecznościowych w kontekście wykorzystywania ustawień prywatności (Surma, 2013; Kołodziejczyk, 2014). Tematyka badań prowadzonych przez autorów niniejszego artykułu jest jednak szersza. Wpływ nowych technologii na prywatność wykracza poza internet i młodzi ludzie obcy z tymi technologiami coraz bardziej powinni zdawać sobie z tego sprawę. Prywatność może być naruszana zarówno przez podmioty komercyjne, jak i organy państwa. Temat jest medialnie głośny, m.in. ze względu na zmiany w systemie prawnym – w 2016 roku w Polsce zmodyfikowano prawo, w szczególności ustawę o policji, ułatwiając działania służb naruszające prywatność, a w najbliższym czasie wejdzie w życie ogólne Rozporządzenie Parlamentu Europejskiego i Rady (UE) o ochronie danych, co istotnie wpłynie na komercyjne przetwarzanie danych osobowych.

Celem artykułu jest przedstawienie postaw polskich studentów wobec prywatności w kontekście masowego przetwarzania danych – szczególnie w zakresie poczucia naruszenia prywatności oraz poziomu akceptacji tego naruszenia. Podstawowe postawione pytanie dotyczy ewentualnych różnic między postawami studentów różnych typów uczelni, także w zależności od wielkości ośrodka akademickiego. Wykorzystane metody badawcze to badania kwestionariuszowe.

1. Opis badania

W celu wyjaśnienia powszechnego rozumienia problemu prywatności w kontekście nowych możliwości przetwarzania danych masowych, autorzy od 2014 roku prowadzą badania ankietowe wśród studentów, które początkowo miały charakter eksploracyjny i ich celem było dokonanie wstępnego rozeznania w nowej problematyce. Później przybrały charakter deskryptywny, a ich celem jest przeprowadzenie dokładniejszej charakterystyki przedmiotu w ujęciu ilościowym. Na potrzeby doboru stawianych ankietowanym pytań wcześniej dokonano analizy literatury przedmiotu oraz prasy popularnej w celu określenia szczegółowych problemów związanych z prywatnością, które mogą być istotne dla ankietowanych. Skupiono się na zagadnieniach związanych

z nowoczesnymi technologiami i nowymi możliwościami przetwarzania dużych wolumenów danych prywatnych, w tym osobowych. Szczególne znaczenie ma tutaj powszechne wykorzystanie sieci internet, lecz wzięto pod uwagę także zagadnienia masowego przetwarzania danych pochodzących spoza sieci.

Z jednej strony dokonano próby wyodrębnienia zagadnień mających istotny wpływ na indywidualne naruszenie prywatności jednostek. Ankietowani w skali od 1 do 5 (skala Likerta) wskazywali poziom poczucia naruszenia prywatności związany z 12 wskazanymi zagadnieniami, obejmującymi m.in. różnorodne zastosowania internetu, telefonii komórkowej, płatności kartami, uczestnictwa w programach lojalnościowych, a także monitoringu miejskiego. Z drugiej strony, zakładając że powyższe zjawiska w pewnym stopniu prowadzą do naruszeń prywatności, badano różne cele przetwarzania pod kątem stopnia akceptacji naruszenia prywatności. Uwzględniono potrzeby ogólnospołeczne, jak zapewnienie bezpieczeństwa publicznego i prawidłowego funkcjonowania państwa, a także cele komercyjne, w szczególności indywidualizację przekazu reklamowego. Ankietowanym zadawano także pytania o stosowanie różnorodnych metod, mających na celu zachowanie prywatności i anonimowości w kontekście analizowanych zjawisk.

Badana grupa powinna dość dobrze orientować się w potencjalnych zagrożeniach płynących z masowego przetwarzania danych oraz mieć do czynienia z technologią informatyczną i internetem, jako aktywni uczestnicy. Do badania wybrano studentów, czyli grupę dość dobrze spełniającą te warunki. Należy wziąć pod uwagę, że taki dobór nie jest oczywiście reprezentatywny dla całości społeczeństwa, lecz pozwala na realizację celów badań. Początkowo badania prowadzono wśród studentów Szkoły Głównej Handlowej w Warszawie (SGH). W roku akademickim 2016/2017 w celu zmniejszenia homogeniczności próby badania rozszerzono na studentów innych uczelni – z wydziałów humanistycznych i technicznych. Przebadano wówczas 373 studentów, w tym 144 z SGH, 123 z Politechniki Opolskiej (PO), 62 z Uniwersytetu Jagiellońskiego w Krakowie (UJ) z Wydziału Zarządzania i Komunikacji Społecznej i 44 z Uniwersytetu Opolskiego (UO) z Wydziału Nauk Społecznych. Można więc badanych podzielić na trzy podstawowe grupy: studentów uczelni ekonomicznej ($N = 144$), technicznej ($N = 123$) i uniwersyteckich wydziałów humanistycznych ($N = 106$). W niniejszym artykule dokonano porównania wyników dla powyższych grup sprawdzając tezę, czy typ uczelni lub kierunek studiów wpływa na postrzeganie naruszenia prywatności związanego ze stosowaniem nowoczesnych technologii. Część ankietowanych studiuje w bardzo dużych miastach i ośrodkach akademickich (Warszawa lub Kraków, $N = 206$), część w ośrodku średniej wielkości (Opole, $N = 167$). Porównano także wyniki dla tych dwóch grup. Ankieta jest anonimowa, w papierowej formie, dzięki czemu uzyskiwany jest prawie pełen zwrot, a bezpośredni kontakt z ankierem wpływa na poprawę wiarygodności jej wyników.

2. Badanie stopnia naruszenia prywatności w zależności od typu uczelni

W celu określenia stopnia indywidualnego poczucia naruszenia prywatności w zależności od zjawiska sformułowano 12 zagadnień przedstawionych szczegółowo w tabeli 1 wraz ze średnimi arytmetycznymi odpowiedzi w podziale na trzy typy uczelni.

Tabela 1. Poczucie naruszenia prywatności wg wskazanych zjawisk – pytania i średnie arytmetyczne w podziale na typy uczelni

Zagadnienie	Uniwersytet	Politechnika	Uczelnia ekonomiczna	Łącznie	Odchyl. stand.
1. Korzystanie z usług przechowywania prywatnych plików w chmurze	2,6	2,8	2,5	2,6	1,09
2. Możliwość dostępu nieuprawnionych osób/maszyn do prywatnych e-maili	3,7	3,6	3,7	3,6	1,19
3. Gromadzenie informacji o zachowaniach użytkowników w Internecie (np. odwiedzane strony)	3,9	3,6	3,9	3,8	1,09
4. Automatyczne śledzenie informacji o aktywności w portalach społecznościowych	4,0	3,7	4,1	3,9	1,03
5. Gromadzenie informacji o płatnościach dokonywanych np. kartami płatniczymi	3,9	3,7	3,8	3,8	1,15
6. Gromadzenie danych o zachowaniach konsumentów dzięki programom lojalnościowym	3,3	3,2	3,0	3,1	1,07
7. Gromadzenie w systemach IT danych o korzystaniu z usług służby zdrowia	3,0	2,9	2,6	2,8	1,17
8. Gromadzenie przez telekomunikację danych geolokalizacyjnych i bilingów telefonów komórkowych	3,7	3,6	3,7	3,7	1,15
9. Gromadzenie danych o sieciowym wykorzystaniu urządzeń, np. o logowaniach do Wi-Fi	3,6	3,3	3,1	3,3	1,13
10. Powszechny monitoring miejski i przemysłowy (kamery)	2,8	2,8	2,3	2,6	1,29
11. Masowe wykonywanie zdjęć: satelitarnych, lotniczych, typu <i>street view</i>	2,6	2,6	2,0	2,4	1,21
12. System identyfikacji pojazdów, np. w celu naliczania opłat za drogi płatne, wykrywania wykroczeń drogowych	2,6	2,8	2,4	2,6	1,17
Razem	3,3	3,2	3,1	3,2	

Zródło: opracowanie własne.

Analiza łącznych wyników (bez podziału na typy uczelni) dała podobne wyniki do wcześniejszych badań z lat 2014–2016 prowadzonych wyłącznie na SGH. Średni poziom naruszenia prywatności (przy możliwych odpowiedziach od 1 do 5) dla poszczególnych pytań jest zróżnicowany i mieści się w zakresie od 2,4 (pytanie 11) do 3,9 (pytanie 4). Odchylenia standardowe dla poszczególnych pytań zawierały się w przedziale od 1,03 (pytanie 4) do 1,29 (pytanie 10).

Trudno natomiast wskazać wyraźne różnice w wynikach dla poszczególnych typów uczelni. Wyniki dla poszczególnych typów uczelni niemal nie wykraczają poza granice $\pm 0,2$ od wyniku łącznego, wyjątkowo osiągając 0,3, a w jednym przypadku 0,4. Tym wyjątkiem są głównie pytania związane z monitoringiem miejskim i drogowym oraz zdjęciami lotniczymi. Tutaj wyższe wyniki zanotowano dla uczelni ekonomicznej, lecz prawdopodobnie jest to związane z tym, że uczelnią jest SGH z Warszawy, czyli największego miasta. Temat zostanie więc poruszony przy porównaniu wyników według wielkości ośrodka.

3. Badanie zgody na naruszenie prywatności w zależności od typu uczelni

W celu określenia stopnia indywidualnego stopnia akceptacji naruszenia prywatności w zależności od celu przetwarzania danych wskazano dziewięć takich potrzeb przedstawionych szczegółowo w tabeli 2 wraz ze średnimi arytmetycznymi odpowiedzi w podziale na typy uczelni.

Średnie wyniki (bez podziału na typ uczelni) odpowiedzi na poszczególne pytania dotyczące zgody na naruszenie prywatności kształtują się w granicach od 2,3 (pytanie 8) do 4,0 (pytanie 1). Odchylenia standardowe dla poszczególnych pytań zawierały się w przedziale od 1,03 (pytanie 1) do 1,32 (pytanie 3). Zauważalna jest wyższa akceptacja naruszeń prywatności związanych z interesem publicznym – bezpieczeństwem i dobrem ogólnym (pytania 1–6 – średni wynik 3,4) niż indywidualnym przekazem w celach handlowych (pytania 7–9 – średni wynik 2,5). Także te wyniki są podobne do wyników wcześniejszych badań z lat 2014–2016 prowadzonych wyłącznie w SGH.

W tej części ankiety także trudno wskazać wyraźne różnice w wynikach dla poszczególnych typów uczelni. Wyniki dla poszczególnych typów niemal nie wykraczają poza granicę $\pm 0,2$ w porównaniu z wynikami łącznymi, tylko w dwóch przypadkach osiągając 0,3. Ponieważ znowu częściowo te różnice można wyjaśnić wielkością ośrodka, zostaną poruszone w dalszej części.

Ankietowanym zadano także pytania o stosowanie w internecie metod zachowania prywatności lub anonimowości. Ze wskazanych metod zdecydowanie najczęściej we wszystkich typach uczelni stosowane jest ograniczanie udostępnienia prywatnych danych w serwisach społecznościowych – poza ustawienia domyślne (dominująca odpowiedź „stosuję często”). Podobnie typ uczelni nie wpływa na częstość wykorzystywania trybu prywatnego (incognito) w przeglądarce internetowej (dominująca odpowiedź „stosuję czasami”). Odmierna sytuacja jest w przypadku stosowania metod wymagających większych umiejętności technicznych, takich jak wykorzystanie mechanizmów VPN (wirtualne sieci prywatne), np. w celu utrudnienia geolokalizacji oraz sieci TOR w celu zapewnienia anonimowości w internecie. Te ogólnie zdecydowanie rzadziej stosowane rozwiązania, wyraźnie częściej, co zrozumiałe, są stosowane przez studen-

tów uczelni technicznych. Szersze omówienie metod zachowania prywatności w internecie wykracza jednak poza ramy niniejszego artykułu.

Tabela 2. Zgoda na naruszenie prywatności związana z różnymi celami przetwarzania danych – pytania i średnie arytmetyczne w podziale na typy uczelni

Cel przetwarzania danych	Uniwersytet	Politechnika	Uczelnia ekonomiczna	Łącznie	Odczyn. stand.
1. Zapewnienie bezpieczeństwa publicznego (np. wykorzystanie monitoringu w miejscach publicznych)	4,0	4,0	4,1	4,0	1,03
2. Wykrywanie przestępstw (np. analiza bilingów telefonicznych i danych geolokalizacyjnych)	3,7	3,4	3,5	3,5	1,16
3. Przeciwdziałanie terroryzmowi (np. częściowa kontrola poczty elektronicznej, plików przechowywanych w chmurze)	3,2	2,9	3,2	3,1	1,32
4. Wykrywanie naruszeń podatkowych (np. wykrywanie szarej strefy i analiza majątku z wykorzystaniem śledzenia ogólnodostępnych treści w internecie)	3,0	2,7	2,9	2,8	1,23
5. Poprawa bezpieczeństwa transportu (np. wykorzystanie monitoringu drogowego, fotoradarów itp.)	3,5	3,0	3,5	3,3	1,26
6. Poprawa funkcjonowania służby zdrowia i przeciwdziałanie zagrożeniom epidemiologicznym przy anonimizacji danych o zdrowiu pacjentów (np. dostęp do historii leczenia)	3,5	3,7	3,7	3,6	1,20
7. Przygotowywanie zindywidualizowanej oferty handlowej (np. dla uczestników programów lojalnościowych z wykorzystaniem analizy wcześniejszych zakupów)	2,8	2,8	2,7	2,8	1,24
8. Indywidualizacja treści reklamowych (np. reklamy w internecie wyświetlane z związku z aktywnością danego użytkownika, wykrytą jego lokalizacją)	2,5	2,0	2,3	2,3	1,19
9. Indywidualne oferty usług służby zdrowia (z wykorzystaniem danych o zdrowiu pacjentów)	2,6	2,5	2,6	2,6	1,27
Razem	3,2	3,0	3,2	3,1	

Źródło: opracowanie własne.

4. Analiza danych w zależności od wielkości ośrodka akademickiego

Analizie podano także dane według wielkości miasta akademickiego. Do jednej grupy zaliczono uczelnie z miast bardzo dużych, czyli Warszawy (SGH) i Krakowa (UJ), do drugiej – z miast średniego, czyli z Opola (PO, UO). Pierwsza grupa liczy 206 ankietowanych, druga 167.

W tabeli 3 przedstawiono wyniki części ankiety dotyczącej naruszenia prywatności według wskazanych zjawisk. Średnie dla wszystkich pytań łącznie są niemal iden-

tyczne, zauważa się jednak różnice w przypadku poszczególnych pytań. Wyraźne różnice dotyczą wcześniej wspomnianych pytań o monitoring miejski i drogowy oraz o zdjęcia satelitarne i lotnicze (pyt. 10–12). Wyższe poczucie naruszenia prywatności dla tych zagadnień zauważa się w przypadku ośrodka średniego, czyli Opola (średnie arytmetyczne od 2,7 do 2,8) niż w ośrodkach bardzo dużych, czyli Warszawy i Krakowa (od 2,2 do 2,4). Jest to zapewne związane z życiem w większym mieście i przyzwyczajeniem do części tych zjawisk. Odwrotna sytuacja występuje w przypadku naruszenia prywatności, wynikającego z aktywności internetowej, w szczególności gromadzenia informacji o zachowaniach użytkowników w internecie (np. odwiedzane strony) oraz automatycznego śledzenia informacji o aktywności w portalach społecznościowych (pyt. 3 i 4). Dla dużych miast są to wartości od 3,9 do 4,1, zaś dla Opola – od 3,6 do 3,7. Autorzy nie są jednak w stanie wyjaśnić przyczyn tej zależności.

Tabela 3. Poczucie naruszenia prywatności według wskazanych zjawisk – średnie arytmetyczne w podziale na wielkość ośrodka akademickiego

Pytanie	1	2	3	4	5	6	7	8	9	10	11	12	Razem
Ośrodki bardzo duże	2,6	3,7	3,9	4,1	3,9	3,1	2,8	3,7	3,3	2,4	2,2	2,4	3,17
Ośrodki średnie	2,7	3,5	3,6	3,7	3,7	3,2	2,8	3,6	3,3	2,8	2,7	2,8	3,20

Zródło: opracowanie własne.

W tabeli 4 przedstawiono wyniki części ankiety dotyczącej zgody na naruszenie prywatności związanej z różnymi celami przetwarzania danych. Podobnie jak w przypadku poprzedniej części nie ma wyraźnej różnicy w średniej dla wszystkich pytań łącznie, lecz zauważa się różnice dla poszczególnych pytań. W szczególności wśród studentów z dużych miast zauważa się wyższą akceptację naruszenia prywatności w celach związanych z interesem publicznym, nie ma takiej zależności w celach komercyjnych. Najwyższa różnica (3,5/3,1) występuje przy pytaniu o cel poprawy bezpieczeństwa transportu (pyt. 5), co związane jest prawdopodobnie ze wspomnianą powyżej specyfiką życia w dużych miastach.

Tabela 4. Zgoda na naruszenie prywatności związana z różnymi celami przetwarzania danych – średnie arytmetyczne w podziale na wielkość ośrodka akademickiego

Pytanie	1	2	3	4	5	6	7	8	9	Razem
Ośrodki bardzo duże	4,1	3,6	3,3	2,9	3,5	3,6	2,7	2,3	2,5	3,17
Ośrodki średnie	3,9	3,4	2,9	2,7	3,1	3,7	2,8	2,2	2,6	3,06

Zródło: opracowanie własne.

5. Podsumowanie i kierunki dalszych badań

Badania ankietowe o charakterze ilościowym pomagają zrozumieć postrzeganie problemu prywatności. W szczególności pozwalają, jak w niniejszym artykule, porównywać między sobą poziom naruszenia prywatności związany z różnymi zjawiskami wynikającymi z nowoczesnych technologii informatycznych, w tym przetwarzania danych masowych z użyciem metod *big data*, a także określić poziom akceptacji naruszenia prywatności związany z różnymi celami przetwarzania danych. Takie badania pozwalają jednocześnie na wydzielenie z populacji grup (kohort), zależnych przykładowo od kierunku studiów lub wielkości ośrodka akademickiego.

Celem niniejszego artykułu było porównanie ww. grup studentów. Za wyjątkiem częstości stosowania zaawansowanych technik ochrony prywatności (VPN i TOR – chętniej wykorzystywane przez studentów uczelni technicznych) nie dało się wykazać zależnych od typu uczelni lub ogólnego profilu studiów statystycznie istotnych różnic w postawach. Należy jednak wziąć pod uwagę to, że przykładowo studenci jednego typu uczelni nie są grupą jednorodną i przy większej skali badania być może udałoby się znaleźć zależności w podejściu do prywatności na poziomie poszczególnych kierunków studiów. Przeprowadzone badanie pozwoliło natomiast znaleźć różnice w podejściu do prywatności, zależne od wielkości ośrodka akademickiego, co przedstawione w artykule. Przy większej skali badania być może udałoby się odnaleźć także szczegółowe zależności regionalne, w tym – od miejsca pochodzenia poszczególnych studentów. Wykracza to jednak poza dotychczasowy zakres przeprowadzonego badania.

Należy jednak zdawać sobie sprawę, że takie ilościowe podejście badawcze nie pozwala w pełni zrozumieć przyczynowości zjawiska oraz poznać motywacji respondentów. Autorzy zamierzają dlatego kontynuować badania, w tym z wykorzystaniem podejścia jakościowego, w szczególności opartego na wywiadach. Tym niemniej na podstawie dotychczasowych badań można mówić o zróżnicowaniu postaw wobec prywatności, biorąc pod uwagę różne zjawiska wynikające z postępu w metodach przetwarzania danych, a także różne cele przetwarzania prywatnych danych, w szczególności danych osobowych.

Praca finansowana ze środków na badania naukowe lub prace rozwojowe
oraz zadania z nimi związane służące rozwojowi młodych naukowców
oraz uczestników studiów doktoranckich

Bibliografia

- Kołodziejczyk, Ł. (2014). *Prywatność w internecie*. Warszawa: Wydawnictwo SPB.
- Mayer-Schonberger, V., Cukier, K. (2013). *Big data – A revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79, 101–139.

- Polańska, K., Wassilew, A. (2015). Analizy big data w serwisach społecznościowych. *Nierówności Społeczne a Wzrost Gospodarczy*, 4/2, 117–128.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.
- Surma, J. (2013). The Privacy Problem in Big Data Applications: An Empirical Study on Facebook, W: *ASE/IEEE International Conference on Social Computing* (s. 955–958).
- Ustawa o Policji z 6.04.1990 r., z późniejszymi zmianami, Dz.U. 1990, nr 30, poz. 179.
- Warren, S.D., Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, IV (5).
- Westin, A. (1967). *Privacy and freedom*. New York: Athenaeum.

INTERNET PRIVACY PERCEPTION AMONG POLISH STUDENTS – A COMPARATIVE STUDY

Keywords: privacy, ICT, big data

Summary. The paper contains the results of author's survey study. The aim of the study was to find out what are the students' perception and attitudes towards privacy (especially in the context of new methods of private and personal data processing). The article presents the differences between students from different types of universities, also depending on the size of the academic center. The article shows how students perceive different levels of privacy violation connected with indicated modern occurrences and what is the level of possible acceptance of privacy breach in the context of data processing for various public and commercial purposes.

Translated by Jędrzej Wieczorkowski and Malwina Popiołek

Cytowanie

Wieczorkowski, J., Popiołek M. (2018). Podejście do prywatności wśród studentów polskich uczelni – badanie porównawcze. *Ekonomiczne Problemy Usług*, 2 (131/2), 311–319. DOI: 10.18276/epu.2018.131/2-30.