PRZEGLĄD SOCJOLOGICZNY
2021 70(2): 129–156
ISSN 0033-2356; e-ISSN 2450-9361
https://doi.org/10.26485/PS/2021/70.2/7

ANNA TURNER
Polska Akademia Nauk
MARCIN W. ZIELIŃSKI
Polska Akademia Nauk

ZAINTERESOWANIE OPINII PUBLICZNEJ TEMATYKĄ INWIGILACJI, PRYWATNOŚCI I OCHRONY DANYCH. GOOGLE BIG DATA W SOCJOLOGII PORÓWNAWCZEJ[1]

Streszczenie

W artykule zaprezentowano wyniki projektu badawczego, w którym zbadano wpływ czynników makrospołecznych na zainteresowanie opinii publicznej tematyką inwigilacji, ochrony danych i prywatności w Internecie w kontekście ujawnionych przez Edwarda Snowdena informacji o istnieniu globalnego programu masowej inwigilacji. Poziom zainteresowania opinii publicznej zbadano, ustalając liczbę wyszukiwań dla zapytań związanych z inwigilacją w wyszukiwarce Google w 116 krajach, w których następnie przeprowadzono analizy porównawcze. W artykule zostanie zweryfikowana hipoteza, że w krajach bardziej demokratycznych zainteresowanie opinii publicznej

Dr, Instytut Filozofii i Socjologii; e-mail: aturner@ifispan.edu.pl
https://orcid.org/0000-0003-3908-5075

Dr, Instytut Filozofii i Socjologii; e-mail: mzielinski@ifispan.edu.pl
https://orcid.org/0000-0002-9388-4348

[1] Artykuł ten powstał w ramach grantu Narodowego Centrum Nauki (Preludium, 2017/25/N/HS6/01169, grant Anny Turner) przy poparciu programu Cross-national Studies: Interdisciplinary Research and Training Program (CONSIRT, www.consirt.osu.edu), którego autorzy są członkami. CONSIRT jest programem Polskiej Akademii Nauk (PAN) i Ohio State University (OSU), z siedzibą w Instytucie Filozofii i Socjologii PAN i Departamencie Socjologii OSU.

sprawami inwigilacji jest większe niż w pozostałych krajach. Przedstawimy także sposób, w jaki zaadaptowaliśmy dane Google na potrzeby projektu.

Słowa kluczowe: Planer słów kluczowych Google, big data, Google Trends, dane internetowe, Edward Snowden, inwigilacja, prywatność, ochrona danych, badania opinii publicznej

WPROWADZENIE

Od ponad dwóch dekad jesteśmy świadkami gwałtownej ekspansji Internetu[2], której skutki odczuwalne są nie tylko we wszystkich sferach życia społecznego, lecz także w codziennym życiu zwykłych obywateli. Z jednej strony rewolucja technologiczna stworzyła ogromne szanse i możliwości, z drugiej, ze względu na ingerowanie w nasze dotychczasowe życie na niespotykaną dotąd skalę, przyniosła także zagrożenia, które dotykają wszystkich bez względu na wiek, klasę społeczną czy miejsce zamieszkania [Wimmer, Quandt 2006; Beck 2008; 2009; Szpunar 2012; Kowalczyk 2019].

Zagrożenia, którymi zajmiemy się w tym artykule, są specyficznej natury, ponieważ charakteryzuje je przyczynowo-skutkowa sekwencja zdarzeń reprezentowana w trzech etapach: udostępnianie, monitorowanie i profilowanie danych[3]. Pierwszy etap – udostępnianie danych – jest definiowany przez sposób funkcjonowania wirtualnej rzeczywistości. Ewolucja i rozwój interaktywnego Internetu Web 2.0 charakteryzuje się tym, że użytkownicy sami generują i udostępniają ogromne ilości informacji. W ciągu zaledwie jednej sekundy powstaje ponad 9 tysięcy wiadomości na Twitterze, ponad tysiąc zdjęć jest dodawanych na Instagramie, ponad 90 tysięcy słów jest wyszukiwanych w Google [https://www.internetlivestats.com/], ponadto liczba aktywnych użytkowników portalu Facebook pod koniec 2020 roku przekroczyła 2 miliardy 800 milionów[4], co czyni go największym serwisem społecznościowym na świecie. Wszystkie te połączenia są realizowane za pomocą tabletu, smartfona czy komputera, a więc

[2] W roku 1995 mniej niż 1% populacji miał dostęp do Internetu, w roku 2005 ponad miliard osób miało dostęp do Internetu, a w styczniu 2021 roku 4,66 miliarda, w tym ponad 92% poprzez urządzenia mobilne [https://www.internetlivestats.com/internet-users/, https://www.statista.com/statistics/617136/digital-population-worldwide/].

[3] W artykule zagrożenia te, jak i wynikające z nich konsekwencje omawiamy, koncentrując się na poziomie zbiorowości, chociaż można je także rozpatrywać na poziomie indywidualnym.

[4] Aktywny użytkownik to taki, który zalogował się na swoje konto w przeciągu ostatnich 30 dni. Dane z https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

urządzeń uznawanych za osobiste, które z definicji powinny zapewniać użytkownikom poczucie prywatności i anonimowości (jak się przekonamy, jest to odczucie iluzoryczne).

Drugi etap to monitorowanie danych, za którymi kryją się zachowania, zainteresowania i opinie miliardów użytkowników Internetu, którzy (często nieświadomie) dzielą się nimi każdego dnia. Prywatne firmy i instytucje rządowe, dostrzegając rosnącą siłę informacji, zaczęły wykorzystywać ogromny potencjał tych zasobów [Beniger 1986; Castells 2011; Krzysztofek 2012; Zuboff 2015; Juza 2019; Mau 2019]. Największym wyzwaniem, któremu próbują sprostać, jest to, jak za pomocą algorytmów sztucznej inteligencji i metod profilowania przekształcić zebrane dane w wartościowe informacje – ten etap jest szczególnie niepokojący, ponieważ odbywa się bez wiedzy osób, których dane zebrano. Nawet jeśli niektórym użytkownikom wydaje się, że nie pozostawiają po sobie dużego cyfrowego śladu, firmy internetowe takie jak Amazon, Facebook czy Alphabet posiadają dane tak wielu osób, że z pomocą modelowania statystycznego mogą stworzyć profil na podstawie udostępnianych informacji. Kazimierz Krzysztofek wyjaśnia: „Pozostawianie śladów cyfrowych w sieciach komputerowych przez ich użytkowników pozwala na coraz doskonalszą socjometrię. Inwestuje się olbrzymie środki finansowe w tworzenie i wdrażanie nowych generacji oprogramowania w biznesie znane pod nazwą Business Intelligence, Customer Relationship Management, Data Mining, hurtownie danych, «fermy wiedzy» i inne, które oddają w «ręce maszyn» władzę analityczną dotychczas przynależną człowiekowi. Dzięki technologiom cyfrowym rejestruje się coraz więcej ludzkiej codzienności, a w niej właśnie te trendy kiełkują i zataczają coraz szersze kręgi. Oto dlaczego wielu badaczy chce tę wiedzę analityczną posiąść" [Krzysztofek 2012].

Początkowo algorytmy służące do profilowania zostały opracowane na potrzeby reklam, których celem było przekształcenia pasywnego użytkownika w aktywnego konsumenta poprzez przypisanie go do określonych grup, którym oferowano spersonalizowane usługi i korzyści. Przełom nastąpił po atakach terrorystycznych 11 września 2001 roku, kiedy zautomatyzowane techniki monitorowania i profilowania zostały usankcjonowane przez władze jako niezbędne do zapewnienia bezpieczeństwa obywateli. 26 października 2001 roku prezydent Stanów Zjednoczonych George W. Bush w ramach „wojny z terroryzmem" podpisał ustawę Patriot Act[5], na mocy której między innymi zwiększono nadzór

[5] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

nad środkami komunikacji, co umożliwiło przejęcie kontroli nad wszystkimi połączeniami (a nie tylko osób podejrzanych o terroryzm) wykonywanymi za pośrednictwem amerykańskich operatorów. Wiele osób uwierzyło, że należy poświęcić swoją prywatność, obywatele na całym świecie godzili się być skanowani, fotografowani, przeszukiwani i wypytywani „dla własnego bezpieczeństwa". Kiedy w czerwcu 2013 roku Edward Snowden ujawnił dokumenty dotyczące ściśle tajnego globalnego programu szpiegowskiego PRISM, stworzonego i kierowanego przez amerykańską Agencję Bezpieczeństwa Krajowego (NSA), okazało się, że między innymi Google, Facebook, Microsoft czy Apple od 2007 roku udostępniały NSA bez wiedzy i zgody swoich użytkowników wszystkie ich dane, takie jak: adresy IP, loginy, hasła, treści wysyłanych wiadomości, zdjęcia, posty czy video. Rewelacje Snowdena, szeroko komentowane w mediach, także społecznościowych, wywołały debatę o globalnym zasięgu, w której wzięli udział politycy, dziennikarze, naukowcy, a także zwykli internauci.

Od momentu ujawnienia informacji przez Snowdena można odnieść wrażenie, że literacka fikcja Orwellowskiego *Roku 1984* zmieniła się w rzeczywistość – żyjemy w „kulturze inwigilacji" [Lyon 2017, 2018]. Doniesienia te potwierdziły także, że mamy dosyć złudne poczucie kontroli nad naszymi danymi oraz że nie mają nad nimi kontroli także ci, którym je w dobrej wierze powierzamy. Wszechobecne technologie – za cenę korzystania z nich, wymuszają na nas dzielenie się danymi, a korporacje i rządy wielu państw chętnie to wykorzystują, obiecując w zamian różnorakie korzyści lub tłumacząc się względami bezpieczeństwa. Zbyt często mamy do czynienia z sytuacją, w której demokratycznie wybrane władze zamiast szukać rozwiązania problemów innymi sposobami, decydują się na inwestycje w nowe rozwiązania technologiczne, nie biorąc pod uwagę możliwych reperkusji, takich jak głęboka ingerencja w prawo obywateli do prywatności [Greenwald 2014; Lyon 2014; Huijboom, Bodea 2015]. Algorytmy i metody profilowania nie są publicznie dostępne, nie możemy uzyskać informacji na temat tego, które nasze dane zostały zebrane, kiedy, gdzie, przez kogo ani jak zostały wykorzystane [Davies 2014; Mazur 2018; Juza 2019; Garfinkel 2000]. W kwietniu 2021 roku z portalu Facebook wyciekły następujące dane ponad 533 milionów osób: numer telefonu, Facebook ID, imię i nazwisko, lokalizacja, poprzednia lokalizacja, data urodzenia, adres e-mail, data utworzenia konta i status związku. Nie wiadomo, czyje dane wyciekły ani co się z nimi stało, a ponieważ były to także dane ponad 2,5 miliona osób z Polski Prezes Urzędu Ochrony Danych Osobowych wystąpił z pismem do władz Facebook Poland, w którym: „[…] zwrócił się o podjęcie działań w celu ograniczenia ryzyka wykorzystania danych osobowych objętych naruszeniem poprzez zaoferowanie usługi umożliwiającej wszystkim polskim

użytkownikom sprawdzenie, czy naruszenie to ich dotyczy" [https://uodo.gov.pl/pl/138/2022]. Co ważne, to nie Facebook poinformował o wycieku, a Alon Gal, specjalista do spraw cyberbezpieczeństwa [https://twitter.com/UnderTheBreach]. Kiedy w 2018 roku weszło w życie *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 (ogólne rozporządzenie o ochronie danych)*, znane jako RODO, wydawało się, że użytkownicy Internetu w krajach UE zyskają nie tylko ochronę swoich danych, ale także prawo do informacji, co z tymi danymi się dzieje. Po dwóch latach fundacja Panoptykon postanowiła przeanalizować, „co w reformie działa, a co wymaga poprawy" [https://panoptykon.org/audyt-rodo]. Na stronie fundacji możemy przeczytać:

> Naszą rolą jest testowanie skuteczności nowego prawa w zderzeniu z praktyką firm i organów państwa, a więc siłą rzeczy dostrzegamy przede wszystkim to, co działa źle na styku konsument–biznes i obywatel–państwo. Żeby nieco rozszerzyć tę perspektywę, poprosiliśmy o opinię zaprzyjaźnionych prawników: wytrawnych praktyków, jeśli chodzi o stosowanie RODO. Niestety, oni też przynieśli nam przykłady mechanizmów, które nadal nie działają tak, jak powinny". Przeprowadzono dziewięć testów, między innymi: Test pracodawcy w czasach koronawirusa, Test osoby, której dane wyciekły, Test odrzuconego kredytobiorcy czy Test internauty, który nie chce być towarem. Wnioski płynące z przeprowadzonych badań wskazują na szereg naruszeń, przytoczymy wyniki ostatniego z nich – Testu internauty, który nie chce być towarem: „Funkcjonowanie giełd reklamowych wysyłających dane użytkowników do setek podmiotów bez ich wiedzy i możliwości kontroli narusza podstawowe zasady RODO. Po pierwsze, na aukcje trafia więcej danych, niż jest to potrzebne, by dopasować reklamę. Po drugie, informacje te mogą ujawniać dane wrażliwe, bo na podstawie lokalizacji, adresów stron, na które wchodzą użytkownicy, czy historii zakupów można wywnioskować, na co chorują, ile zarabiają czy jakie mają poglądy polityczne. Każda strona internetowa ma na takiej giełdzie przypisaną kategorię, która sama w sobie może wskazywać na słabości, problemy czy przekonania użytkowników (takie jak „wsparcie dla ofiar przemocy", „zaburzenia odżywiania" czy „scjentologia"). Jak podkreśla ICO (brytyjski odpowiednik UODO), przetwarzanie danych w celu obsługi aukcji reklamowych wymaga wyraźnej, dobrowolnej i świadomej zgody użytkowników. Tymczasem „zgoda" na tak daleko ingerujące w prywatność przetwarzanie danych jest zbierana hurtowo dla wszystkich firm uczestniczących w aukcjach. Do tego dzieje się to z wykorzystaniem okienek, które utrudniają niewyrażenie zgody lub wręcz stosują cookie walls (jeśli użytkownik nie zaakceptuje śledzących ciasteczek, nie może korzystać ze strony), co wprost narusza wytyczne Europejskiej Rady Ochrony Danych. Internauci często nie są nawet świadomi istnienia profilu reklamowego zawierającego ich dane, nie mówiąc już o jego zawartości. Nie są też w stanie prześledzić, do kogo trafiają ich dane, ani – tym bardziej – skorzystać ze swoich praw, np. prawa do skorygowania lub usunięcia danych.

Powyższe wnioski wskazują, że raczej jako bierni uczestnicy, a nie aktywni gracze bierzemy udział w grze o sumie zerowej, której reguł jeszcze nie znamy.

Mimo rosnących i potwierdzonych zagrożeń dotyczących masowej inwigilacji – a więc praktyk kojarzonych do tej pory raczej z reżimem totalitarnym niż z demokracją – ilość danych, którymi dzielimy się w Internecie, stale rośnie. Pojawiają się zatem pytania: Czy dla zwykłych obywateli ma znaczenie to, że ich działania i aktywności w Internecie są śledzone i monitorowane w większym stopniu, niż są tego świadomi? Jak ważne są te kwestie w codziennym życiu ludzi? Postanowiliśmy zgłębić tę tematykę w kontekście rewelacji ujawnionych przez Edwarda Snowdena, a także zbadać ich potencjalny wpływ na zainteresowanie opinii publicznej tematami, na które Snowden, jak i uczestnicy toczącej się w mediach debaty (dyskursu publicznego) zwracali wielokrotnie uwagę: masowa inwigilacja, potrzeba regulacji prawnych dotyczących ochrony danych i prywatności informacji. Czy był to tylko kolejny medialny skandal, który z czasem przeminął, czy też miał on większe znaczenie i wpływ na nasze zachowanie?

POSTAWY SPOŁECZNE WOBEC PRYWATNOŚCI I NADZORU – PERSPEKTYWY TEORETYCZNE I EMPIRYCZNE

W literaturze przedmiotu wyróżnić można dwa nurty, dwie tendencje dotyczące strategii zachowań stosowanych przez obywateli w odniesieniu do praktyk nadzoru, z którymi się spotykają. Niektóre, jak na przykład kamery zlokalizowane w newralgicznych punktach, mogą pozostać niezauważone, podczas gdy monitorowanie aktywności w Internecie będzie już postrzegane jako poważne naruszenie prywatności. Świadomość tych działań, w połączeniu z brakiem zgody na ich stosowanie, należy do kluczowych wyznaczników zachowań rozumianych jako „zdolność ludzi (jednostek i grup) oraz organizacji do przystosowania się do lub/i oporu wobec inwigilacji, uznając, że podczas gdy niektóre jej formy mogą być akceptowalne lub tolerowane, inne stanowią poważne wyzwanie dla naszych podstawowych praw" [Neumann i in. 2014: 77]. Innymi słowy, przeciwstawianie się inwigilacji może być opisane jako sposoby działania pozwalające uniknąć negatywnych skutków nadzoru i może występować na dwóch poziomach: publicznym i indywidualnym. W sferze publicznej wymaga działań ze strony polityków, urzędników państwowych, organizacji pozarządowych i liderów opinii w celu wprowadzenia i realizacji niezbędnych regulacji, na przykład ujawnienie przez Edwarda Snowdena globalnego programu inwigilacji NSA jest doskonałym przykładem zwrócenia uwagi opinii publicznej na kwestię prawa do prywatności, a także konieczności zainicjowania międzynarodowej debaty. Na poziomie indywidualnym w literaturze przedmiotu zdefiniowano szerokie spektrum działań: od radykalnych inicjatyw obejmujących niszczenie narzędzi inwigilacji po bardziej

pasywne zachowania, takie jak unikanie kamer monitoringu czy ograniczanie korzystania z Internetu i telefonów komórkowych, podawanie fałszywych danych przy zakładaniu konta, szyfrowanie e-maili, korzystanie z oprogramowania zapobiegającego śledzeniu czy korzystanie z anonimowych kanałów komunikacji, takich jak TOR [Neumann i in. 2014; Büchi, Just i Latzer 2017].

Badacze, którzy zajmują się wyjaśnianiem przyczyn akceptacji praktyk inwigilacyjnych, wskazują trzy czynniki odpowiedzialne za taki stan rzeczy [Bauman i in. 2014]. Pierwszym z nich jest powszedniość i wszechobecność tych praktyk. Począwszy od elektrycznej szczoteczki do zębów, która za pomocą zainstalowanej w telefonie aplikacji łączy się z Internetem[6], przez urządzenia osobiste, jak tablet czy smartfon, po kamery na ulicy – wszystkie te urządzenia zbierają informacje i dane na nasz temat, a są przy tym tak powszechne, że prawie niezauważalne. Ten stan rzeczy został skonceptualizowany przez niektórych badaczy jako kluczowa charakterystyka „społeczeństwa nadzorowanego" [Lyon 1993, 1994; Wood 2009; Wood, Webster 2009].

Drugim czynnikiem jest rozrywka, którą gwarantują platformy internetowe. Media społecznościowe, zwłaszcza platformy takie jak Facebook, swoją ogromną popularność zawdzięczają temu, że użytkownicy chętnie obserwują i komentują siebie nawzajem; te zachowania opisano w literaturze jako *social surveillance*[7] *[Marwick 2012] lub interpersonal surveillance*[8] *[Trottier 2012]. W literaturze przedmiotu poruszany jest dodatkowy aspekt: tam, gdzie istnieją ewidentne korzyści z udostępniania danych osobowych, konsumenci wykazują mniejsze poszanowanie dla własnego prawa do prywatności [Gandy 1993; Raab, Koops 2009]. Na przykład Robert Reich twierdzi, że wraz z procesem postępującej dominacji kapitalizmu i rządzących nim mechanizmów ideały demokratyczne tracą na znaczeniu, a konsument „wypiera" obywatela [Reich 2009]; proces ten można opisać także w kategoriach „kapitalizmu inwigilacji" Shoshany Zuboff [Zuboff 2015].*

[6] Instalując aplikację dla szczoteczki elektrycznej Oral-B, zgadzamy się na udostepnianie i dostęp do: lokalizacji, aparatu, pamięci, plików multimedialnych i informacji identyfikujących sieć i rodzaj telefonu (informacje dostępne w sekcji Uprawnienia na stronie aplikacji Oral-B w sklepie Google Play).

[7] „Social surveillance is the use of Web 2.0 sites like Twitter, Facebook and Foursquare to see what friends, family, and acquaintances are «up to»".

[8] „Author uses ethnographic accounts to describe interpersonal surveillance made possible through Facebook. The findings […] present interpersonal surveillance as a matter of users being both the subject and the agent of surveillance".

Trzecim czynnikiem warunkującym akceptację praktyk inwigilacyjnych jest strach. W konsekwencji ataków terrorystycznych rządy wielu krajów zaczęły masowo monitorować wszystko, co działo się w Internecie, uzasadniając takie działania koniecznością zapewnienia bezpieczeństwa swoim obywatelom. Jak się okazało, wiele osób zaakceptowało tę narrację [Cohrs i in. 2005; Watson, Wright 2013; Friedewald, Pohoryles (red.) 2014; Friedewald i in. 2016; Friedewald i in. (red.) 2017]. Znalazły się wśród nich zarówno osoby, które „nie mają nic do ukrycia", a praktyki inwigilacji uznają za nieuniknione w walce z przestępczością i terroryzmem [Raab, Koops 2009; Solove 2011; Special Eurobarometer 2015], jak i takie, dla których prywatność jest wartością trudną do zdefiniowania i z pewnością nie plasuje się wyżej niż bezpieczeństwo w hierarchii potrzeb [Maslow 1943].

EFEKT SNOWDENA

Sprawa Snowdena i związany z nią rozgłos medialny zapoczątkowały szereg badań prowadzonych zarówno przez instytucje naukowe, jak i komercyjne, których celem było zrozumienie, czy i jaki wpływ ujawnienie informacji o istnieniu globalnego programu szpiegowskiego miało na społeczeństwo.

W jednym z pierwszych badań sondażowych, przeprowadzonych przez Pew Research Center, zapytano respondentów (mieszkańców Stanów Zjednoczonych), czy słyszeli o ujawnionych przez Edwarda Snowdena programach inwigilacji rządowej. Prawie połowa wszystkich respondentów odpowiedziała twierdząco, przy czym wyniki różniły się w poszczególnych grupach wiekowych – im starszy respondent, tym potencjalnie większa świadomość tych doniesień: słyszało o nich 44% respondentów w wieku 18–29 lat, 47% w wieku 30–49 lat, 54% w wieku 50–64 lat oraz 61% w najstarszej grupie wiekowej 65+ [Pew Research Center 2013b].

W międzynarodowym badaniu przeprowadzonym przez Ipsos pięć miesięcy po ujawnieniu informacji przez Snowdena zmierzono poziom świadomości społecznej w 24 krajach. Większość (60%) słyszała o Edwardzie Snowdenie, przy czym najwyższy odsetek wskazań odnotowano w Niemczech i Szwecji (94% i 86%), a najniższy w Pakistanie i Kenii (25% i 14%). Dodatkowo respondenci, którzy słyszeli o Snowdenie, zostali zapytani, czy w związku z tym zaczęli chronić swoją prywatność i bezpieczeństwo online – czterech na dziesięciu respondentów (39%) potwierdziło, że tak [CIGI-Ipsos 2014].

Z kolejnych badań dowiadujemy się, że niektórzy użytkownicy Internetu stosują autocenzurę, polegającą na ograniczaniu zachowań, które według nich

mogłyby zostać sklasyfikowane jako podejrzane przez algorytmy sztucznej inteligencji, z których korzystają agencje rządowe; jest to pojęcie znane w literaturze przedmiotu jako *chilling effect* [Dencik, Cable 2017]. Podobny efekt zaobserwowano po ujawnieniu informacji przez Snowdena – zanotowano spadek liczby odsłon artykułów związanych z terroryzmem w Wikipedii [Penney 2016], uczestnicy wywiadów grupowych przyznali, że powstrzymują się od udziału w dyskusjach na tematy wrażliwe w mediach społecznościowych, gdy uważają, że ich własny punkt widzenia nie jest powszechnie podzielany; ta koncepcja jest znana w literaturze jako *spiral of silence* [Noelle-Neumann 1993], w badaniach nad inwigilacją jej występowanie zostało potwierdzone co najmniej dwukrotnie [Hampton i in. 2014; Stoycheff 2016].

Ciekawym aspektem wyłaniającym się z dotychczasowych badań jest zaobserwowana różnorodność postaw wobec kwestii inwigilacji, prywatności i ochrony danych w Internecie. Dlatego niezwykle ważne jest monitorowanie zainteresowania tą tematyką, w tym także poznanie roli determinantów je warunkujących.

CZYNNIKI DETERMINUJĄCE POSTAWY SPOŁECZEŃSTWA WOBEC PRYWATNOŚCI I INWIGILACJI

Badania poświęcone zrozumieniu postaw obywateli wobec kwestii inwigilacji, prywatności i ochrony danych w Internecie wskazują z jednej strony na wzrost świadomości konieczności ochrony danych, a także brak akceptacji dla wykorzystywania ich bez naszej zgody i wiedzy, z drugiej strony nie przekłada się to jednak w żaden sposób na ograniczenie przez te osoby ujawniania informacji osobistych w Internecie. Ta niespójność postaw wobec prywatności i zachowań w tym zakresie jest znana w literaturze jako *privacy paradox* [Kokolakis 2017] Dotychczasowe badania wykazały, że czynniki socjodemograficzne, takie jak wiek, płeć i wykształcenie, odgrywają tutaj znaczącą rolę. Na przykład osoby starsze mają więcej obaw dotyczących swojej prywatności i są bardziej negatywnie nastawione do praktyk inwigilacyjnych [Watson, Wright 2013] niż osoby młodsze, które płynnie poruszają się w świecie Internetu i wiedzą, jak chronić swoją prywatność [Watson, Wright 2013; Van den Broeck, Poels, Walrave 2015; Kezer i in. 2016]. Zaobserwowano także istotne różnice pomiędzy mężczyznami i kobietami – kobiety częściej niż mężczyźni martwią się o prywatność i konsekwencje praktyk inwigilacyjnych, jednocześnie rzadziej niż mężczyźni wiedzą o istnieniu narzędzi, które zapewniają bezpieczeństwo danych i w rezultacie

korzystają z nich w mniejszym stopniu [Sheehan 1999; Hoy, Milne 2010; Watson, Wright 2013]. Istotnym czynnikiem jest wykształcenie – osoby lepiej wykształcone częściej mają świadomość istnienia technik inwigilacyjnych, są także bardziej zaniepokojone stosowaniem tych praktyk wobec obywateli [Svenonius, Björklund 2018], a także kwestiami prywatności swoich danych [Flash Eurobarometer 2008; Special Eurobarometer 2011]. Dodatkowo częściej niż osoby z niższym wykształceniem przeciwdziałają tym praktykom poprzez zastosowanie rozwiązań, które pozwalają chronić prywatność danych i informacji online [Watson, Wright 2013; Friedewald i in. (red.) 2017]. Wszystko to pokazuje, jak ważne są umiejętności cyfrowe. Ich posiadanie staje się kluczowe w zarządzaniu zachowaniami związanymi z ochroną prywatności w celu zmniejszenia ryzyka utraty informacji osobistych i odzyskania kontroli nad prywatnością jednostki [Krzysztofek 2012].

Nie ma wątpliwości, że w ostatnich latach wzrosło zainteresowanie kwestiami inwigilacji, prywatności i ochrony danych w Internecie, także w kontekście informacji ujawnionych przez Edwarda Snowdena, a mimo to nadal istnieją niezagospodarowane obszary skrywające potencjał badawczy. Zacznijmy od czynników różnicujących zainteresowanie i postawy respondentów wobec tematyki inwigilacji i prywatności. Brakuje międzynarodowych badań porównawczych, w których to determinanty na poziomie krajowym byłyby wykorzystywane jako zmienne w analizie statystycznej (dotychczas badano tylko uwarunkowania na poziomie indywidualnym). Pomimo szeroko zakrojonej debaty na temat związku między demokracją a nadużyciami władzy w korzystaniu z szerokiego dostępu do danych brakuje empirycznych dowodów na to, że jakość demokracji może determinować postawy wobec inwigilacji i prywatności. Dodatkowo największe międzynarodowe badanie obejmuje 28 krajów, ale tylko z Europy [Special Eurobarometer 2015], drugie co do wielkości badanie, przeprowadzone przez Ipsos, objęło 24 kraje i miało szerszy zasięg geograficzny, ponieważ włączono do niego również Australię, USA, Chiny czy Brazylię [CIGI-Ipsos 2014]; wciąż jednak istnieją kraje, w których kwestie podnoszone w tej pracy nie zostały do tej pory zbadane.

W kontekście badań nad inwigilacją i prywatnością eksperci zwracają uwagę na jeszcze jeden bardzo istotny aspekt badawczy, mianowicie na rozróżnienie pomiędzy deklaracją w badaniu sondażowym a tym, co naprawdę zajmuje ludzi w życiu codziennym: „badania sondażowe nakłaniają uczestników do wypowiadania się na tematy, o których wcześniej myśleli bardzo niewiele i które są tylko częściowo istotne dla ich codziennych rutynowych działań" [Haggerty, Gazso 2005: 173]. Narrację tę kontynuuje Neumann: „Pomimo niedawnej debaty

publicznej w związku z rewelacjami Snowdena zakładamy, że tylko nieliczni ludzie organizują swoje codzienne życie, biorąc pod uwagę fakt, że są (lub mogą być) nieustannie inwigilowani. Chociaż badania sondażowe sugerują, że wielu obywateli nie aprobuje masowej inwigilacji, nie należy wyciągać pochopnych wniosków na temat codziennych zachowań na podstawie odpowiedzi na jednoznaczne pytania sondażowe" [Neumann i in. 2014: 14]. W naszym badaniu zajmiemy się zaadresowaniem tych luk.

Po pierwsze, do zmierzenia poziomu zainteresowania opinii publicznej kwestiami inwigilacji, prywatności i ochrony danych w Internecie w kontekście ujawnionych przez Edwarda Snowdena informacji wykorzystamy słowa kluczowe z wyszukiwarki Google. Przyjmuje się, że im więcej zapytań jest wpisywanych do wyszukiwarki, tym istotniejszy jest dany problem w badanej populacji [Maurer, Holbach 2016; Turner, Zielinski, Słomczyński 2018]. W dotychczasowych badaniach dane Google były wykorzystywane do konstrukcji:

– wskaźnika ważności tematu debaty publicznej (*public agenda setting*) [Granka 2010; Scharkow, Vogelgesang 2011; Ragas, Hai Tran 2013; Maurer, Holbach 2015];

– barometru istotności bieżących spraw (*issue salience barometer*) [Mellon 2014; Ragas, Hai Tran 2013; Maurer, Holbach 2015];

– wskaźnika nastawień opinii publicznej (*search queries as indicators of public opinion*) [Zhu i in. 2012].

Dodatkowym atutem danych z wyszukiwarki Google jest to, że pozwalają badaczom na poznanie zachowań i zainteresowań użytkowników z zupełnie nowej perspektywy. Informacje zebrane w badaniach sondażowych powstają w wyniku interakcji (bezpośredniej lub telefonicznej) między respondentem a ankieterem, co jest wielką zaletą przy ich interpretacji w konkretnym kontekście ekonomicznym, społecznym, politycznym czy kulturowym. Dane z wyszukiwarki Google są przydatne w badaniu rzeczywistych codziennych zachowań użytkowników – wyszukiwanie informacji odzwierciedla zainteresowania – w przeciwieństwie do badań sondażowych, w których mierzona jest intencja zachowania [Zhu i in. 2012; Mellon 2013; 2014; Ragas, Hai Tran 2013; Lai i in. 2017]. Należy też zwrócić uwagę na specyficzny charakter danych internetowych – wyszukiwania są dokonywane anonimowo, przez co mają potencjalnie większą wiarygodność niż odpowiedzi uzyskane w procesie zadawania pytań przez ankietera [Krzysztofek 2011; Nowak 2012].

Po drugie, w naszym badaniu zmienna zależna (zainteresowanie opinii publicznej mierzone za pomocą wyszukiwań w Google) jest wyjaśniana na poziomie

kraju, dlatego różnice między krajami są również wyjaśniane za pomocą cech kraju jako jednostek obserwacji.

Po trzecie, ze względu na duży zasięg wyszukiwarki Google[9] niniejsze badanie obejmuje 116 krajów ze wszystkich kontynentów, w tym pełne demokracje w Europie Zachodniej, Australii i Ameryce Północnej, reżimy autorytarne (Arabia Saudyjska, Kongo, Kazachstan) oraz demokracje wadliwe w Europie i Ameryce Łacińskiej. Takie podejście wypełni lukę w międzynarodowej perspektywie porównawczej i wniesie wartość dodaną do istniejącej literatury poświęconej zagadnieniom inwigilacji, prywatności i ochrony danych.

DANE

Dane z wyszukiwarki Google, na podstawie których określono poziom zainteresowania opinii publicznej, obejmują okres 24 miesięcy, od kwietnia 2013 roku do marca 2015 roku. Te dane tworzą *zmienne zależne*. Natomiast aby odzwierciedlić poziom demokracji w danym kraju, zastosowaliśmy wskaźnik demokracji. W modelowaniu statystycznym wskaźnik demokracji jest *zmienną niezależną*: w tym przypadku został obliczony jako średnia z lat 2011, 2012 i 2013 dla każdego kraju osobno przy użyciu danych dostarczonych z The Economist Intelligence Unit. Wskaźnik demokracji jest dostępny dla 112 krajów uwzględnionych w badaniu. Uwzględnione zostaną także *zmienne kontrolne* (ludnościowe charakterystyki krajów).

NARZĘDZIE POMIARU

Jako źródło danych wykorzystano Planer słów kluczowych – narzędzie udostępnione przez Google w 2004 roku i do tej pory szeroko wykorzystywane głównie w marketingu i badaniach marketingowych. Kontrastuje to z badaniami w naukach społecznych, gdzie jako źródło danych wykorzystywano jedynie Google Trends, narzędzie ciekawe, ale jednak z mocno okrojonymi danymi (ilość zapytań dla każdego z słów kluczowych jest przedstawiona w formie znormalizowanego do 100 indeksu). W Planerze słów kluczowych wartości te są przedstawione o wiele bardziej precyzyjnie, ponieważ narzędzie udostępnia średnią miesięczną liczbę wyszukiwań dla każdego słowa kluczowego. Analizy wykazały, że Google przyporządkowuje każde słowo kluczowe do jednego

[9] Tylko w trzech krajach Google nie jest największą wyszukiwarką, są to: Rosja, Chiny i Korea Południowa.

z 82 segmentów zapytań, które są proporcjonalnie zlogarytmizowane[10]. Najmniejsza wartość wyszukiwań dla każdego słowa to 10, największa 3 760 000 000. Im wyższa liczba wyszukiwań, tym większa różnica między wartościami skrajnymi segmentu. Dane do badania zostały oryginalnie pobrane na przestrzeni kilku tygodni w roku 2015, następnie w roku 2016 sprawdzono ilość zapytań dla tych samych słów kluczowych dla tego samego okresu. Liczba wyszukiwań nie zmieniła się.

BAZA SŁÓW KLUCZOWYCH

Proces selekcji słów kluczowych został podzielony na trzy etapy. W pierwszym etapie wybrano słowa kluczowe wraz z występującymi w danym języku synonimami w celu sprawdzenia liczby wyszukiwań. Należy podkreślić, że w proces ten zaangażowano ponad 65 rodzimych użytkowników wszystkich języków, albowiem zapytania sprawdzano w lokalnych językach. Ważne jest, aby ostrożnie i wnikliwie definiować słowa kluczowe dla każdego z tematów, ponieważ wiele z nich ma więcej niż jedno znaczenie, co może zniekształcić wyniki. W przypadku naszego badania nie ma drugiego powszechnie znanego Edwarda Snowdena, Juliana Assange'a czy WikiLeaks, ale NSA może występować w wielu językach, stanowiąc skrótowiec utworzony od nazw różnych organizacji, na przykład w języku polskim od Naczelnego Sądu Administracyjnego, w języku angielskim między innymi – National Sheep Association. W drugim etapie sprawdzono wybrane słowa kluczowe w Planerze słów kluczowych. Specyfiką tego narzędzia jest to, że zwraca ono dodatkowe słowa kluczowe (do 1000 podobnych słów dla każdego zapytania). Ta przydatna funkcjonalność umożliwia rozszerzenie bazy słów o nowe przykłady, nawet rzadko używane. Łącznie liczba słów kluczowych (wraz z tymi dodanymi przez Google) wyniosła około 2500 na

[10] Segmenty zapytań: 10, 20, 30, 40, 50, 70, 90, 110, 140, 170, 210, 260, 320, 390, 480, 590, 720, 880, 1000, 1300, 1600, 1900, 2400, 2 900, 3600, 4400, 6600, 8100, 9900, 12 100, 14 800, 18 100, 22 200, 27 100, 40 050, 49 500, 60 500, 74 000, 90 500, 110 000, 135 000, 165 000, 201 000, 246 000, 301 000, 368 000, 450 000, 550 000, 673 000, 823 000, 1 000 000, 1 220 000, 1 500 000, 1 830 000, 2 240 000, 2 740 000, 3 350 000, 4 090 000, 5 000 000, 6 120 000, 7 480 000, 9 140 000, 11 100 000, 13 600 000, 16 600 000, 20 400 000, 24 900 000, 30 400 000, 37 200 000, 45 500 000, 55 600 000, 68 000 000, 83 100 000, 124 000 000, 151 000 000, 185 000 000, 226 000 000, 414 000 000, 506 000 000, 923 000 000, 1 120 000 000, 3 760 000 000. Jeżeli zapytanie „Barack Obama" ma 74 000 miesięcznych wyszukiwań, to nie znaczy, że jest to dokładna liczba tych wyszukiwań. 74 000 jest pomiędzy segmentem 60 500 a 90 500 (co znaczy, że średnia miesięczna liczba wyszukiwań tego słowa jest bliska 74000, ale wciąż oscyluje pomiędzy 60 500 a 74 000 lub 74 000 a 90 500). Im większa liczba wyszukiwań, tym większe potencjalne różnice.

kraj, co pomnożone przez 116 daje 290 000 słów kluczowych. W trzecim etapie, korzystając z pomocy native speakerów, wyczyszczono bazę danych, zostawiając słowa kluczowe związane z tematami uwzględnionymi w badaniu. Ostatecznie baza danych zawierała ponad 10 000 słów kluczowych dla wszystkich krajów. Finalnie w badaniu uwzględnione zostały następujące tematy i słowa kluczowe:

a) Edward Snowden – w ramach tego tematu uwzględniono frazy, które zawierają słowa „Snowden" i „Edward Snowden", np. „wiadomości na temat Edwarda Snowdena" czy „Snowden PRISM".
b) NSA – uwzględniono frazy zawierające słowo „NSA" i dodatkowe słowo związane z tematyką inwigilacji, np. „NSA PRISM", „NSA inwigilacja", „NSA przecieki danych" itp.
c) WikiLeaks – to organizacja od lat nagłaśniająca sprawy, które rządy chciałyby ukryć. Mocno zaangażowana w pomoc Snowdenowi po ujawnieniu przez niego tajnych informacji. W badaniu uwzględniono frazy zawierające słowo „WikiLeaks", usunięto frazy, które nie były związane z tematyką naszego badania, takie jak: „WikiLeaks ufo" czy „logo WikiLeaks".
d) Julian Assange – założyciel WikiLeaks, aktywista i dziennikarz, równie mocno zaangażowany we wsparcie Snowdena. W badaniu uwzględniono frazy zawierające słowa „Assange" i „Julian Assange", np. „wywiad z Julianem Assange", "Assange NSA".
e) Inwigilacja (*surveillance*) – uwzględniono wszystkie frazy zawierające słowa typu „inwigilacja internetowa", „inwigilacja w sieci".
f) Ochrona danych/prywatność informacji (*data security*/*information privacy*) – w badaniu uwzględniono następujące frazy: „prywatność w Internecie", „ochrona danych", „ochrona informacji", „bezpieczeństwo danych", „bezpieczeństwo informacji" itp.
g) Regulacje prawne dotyczące ochrony danych (*data protection law*) – w badaniu uwzględniono następujące frazy: „polityka prywatności", „polityka bezpieczeństwa informacji", „ustawa o ochronie danych" itp., a więc pojęcia odnoszące się do przepisów ustawowych, wykonawczych i aktów prawnych dotyczących ochrony informacji i prywatności danych.

MODEL POMIARU

Do przeprowadzenia analiz porównawczych nie mogliśmy użyć całkowitej liczby wyszukiwań w każdym kraju, gdyż jest ona determinowana przez wielkość populacji; im większa liczba osób korzystających z Internetu i wyszukiwarki Google, tym więcej wyszukiwań. Dlatego też stworzyliśmy *wskaźnik wyszukiwań* (*search*

index) dla wszystkich zmiennych zależnych (siedmiu tematów: Edward Snowden, NSA, Julian Assange, WikiLeaks, inwigilacja, ochrona danych, regulacje prawne). Algorytm opisany wzorem pozwala na oszacowanie porównywalnego między krajami zainteresowania opinii publicznej.

$$\frac{\text{Nr of searches Snowden}}{\text{Nr of people using Google}} \times 100\,000 = \boxed{\begin{array}{c}\text{Number of searches Snowden}\\ \text{per 100.000 GU}\end{array}}$$

Tak obliczony wskaźnik został następnie powiększony o 1 i poddany transformacji logarytmicznej logarytmem naturalnym. Logarytmizacja miała na celu znormalizowanie rozkładu wskaźnika, który pierwotnie był silnie prawoskośny. Zwiększenie wartości wskaźnika o 1 przed logarytmizacją było związane z jego własnością log_N⟦(0)⟧= ∄. Tym samym kraje, w których liczba wyszukiwań wynosiła 0, zostałyby wyłączone z dalszych analiz.

Po zindeksowaniu i zsumowaniu liczby wyszukiwań w ujęciu miesięcznym otrzymujemy dane o charakterze powtarzanego pomiaru (*repeated measures*), gdzie liczba wyszukiwań każdego tematu w każdym kraju zmierzona została w 24 punktach czasowych (miesiącach, w których mierzono liczbę wyszukiwań).

$$SearchIndex = \log_N\{[\left(\frac{(Z_{1\ldots24})}{Gu}\right) * 100000] + 1\}$$

Gdzie:

$(Z_{1\ldots24})$ – średnia liczba wyszukiwań na każdy temat w każdym z kolejnych 24 miesięcy (od kwietnia 2013 do marca 2015)

Gu – liczba użytkowników Google w danym kraju

W dalszych analizach wykorzystano zlogarytmizowany *wskaźnik wyszukiwań* dla każdego tematu.

ZAŁOŻENIA TEORETYCZNE

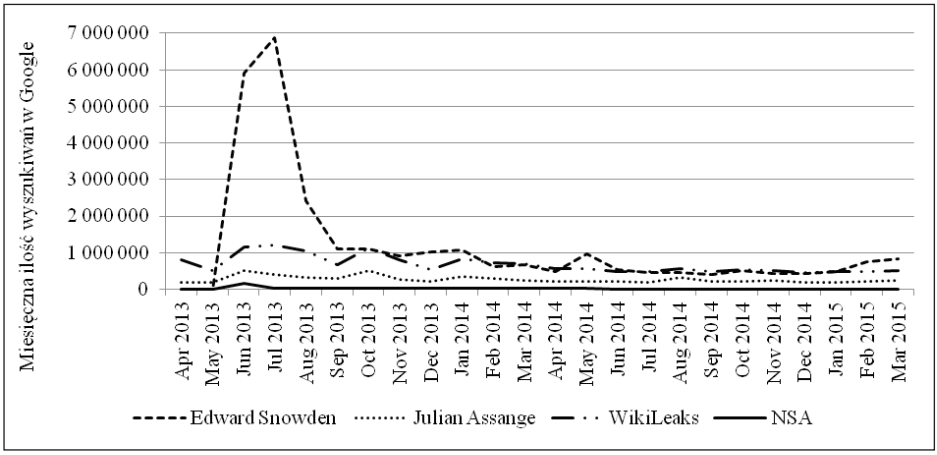
Model pomiarowy opiera się na następujących założeniach. Po pierwsze, przypuszczamy, że cztery zmienne zależne: Snowden, NSA, Assange i WikiLeaks stanowią jakościowo inną grupę niż pozostałe trzy zmienne zależne: inwigilacja, ochrona danych, regulacje prawne; po drugie, że istnieje związek pomiędzy nimi. Zastosowana analiza czynnikowa (*confirmatory factor analysis*) potwierdziła redukowalność siedmiu wskaźników do dwóch zmiennych latentnych (dwóch wymiarów konceptualnych). Pierwsza grupa obejmuje osoby i instytucje najbardziej zaangażowane w ujawniony globalny program masowej inwigilacji: NSA,

Edward Snowden, Julian Assange i WikiLeaks. Nazwaliśmy tę grupę *data leaks*, ponieważ symbolizuje ona dwie strony tej samej monety: tych, których celem jest tworzenie tajnych programów masowej inwigilacji danych i tych, którzy informacje na temat istnienia takich programów ujawniają. Druga grupa obejmuje kwestie, na które zwrócili uwagę Edward Snowden i media: skalę masowej inwigilacji, znaczenie ochrony prywatności informacji oraz konieczność stworzenia odpowiednich regulacji prawnych; tę grupę nazwaliśmy *data surveillance*.

W pierwszym etapie sprawdziliśmy rozkład danych mierzonych liczbą wyszukiwań dla każdego tematu w czasie.

Wykres 1.1 pokazuje zainteresowanie opinii publicznej tematami z grupy *data leaks* w odstępach miesięcznych we wszystkich 116 krajach objętych badaniem, mierzone za pomocą całkowitej liczby wyszukiwań w Google. Możemy obserwować, jak zmienia się ono na przestrzeni 24 miesięcy (od kwietnia 2013 do marca 2015) i porównać je między czterema tematami zaliczanymi do tej grupy.

WYKRES 1.1 Zainteresowanie opinii publicznej *data leaks* – miesiąc po miesiącu



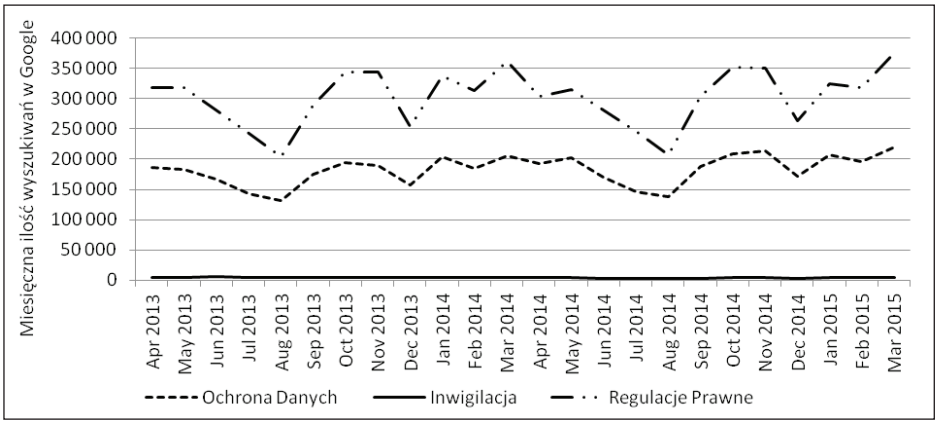
Źródło: opracowanie własne.

W okresie od kwietnia 2013 do marca 2015 roku zainteresowanie opinii publicznej wszystkimi tematami było wysokie, ale największy wzrost można zaobserwować w czerwcu i lipcu 2013 roku – w czasie, gdy doniesienia o Snowdenie pojawiły się w „The Guardian" i „The Washington Post". Spośród wszystkich tematów największy wzrost zainteresowania opinii publicznej dotyczył Edwarda Snowdena (z 10 840 wyszukiwań w maju 2013 roku do 5 910 980 w czerwcu 2013 roku i 6 882 470 w lipcu 2013 roku). Zainteresowanie społeczeństwa

tematem NSA było najmniejsze, z wyjątkiem niewielkiego wzrostu zainteresowania w czerwcu 2013 roku (165 900 wyszukiwań na świecie) – miesięczne zainteresowanie oscylowało wokół 20 000 wyszukiwań miesięcznie. Począwszy od sierpnia 2013 roku zainteresowanie opinii publicznej wszystkimi tematami zaczęło spadać, z niewielkimi wzrostami w kolejnych miesiącach, ale ogólnie pozostając stabilne w czasie.

Wykres 1.2 pokazuje zainteresowanie opinii publicznej tematami z grupy *data surveillance* w odstępach miesięcznych we wszystkich 116 krajach objętych badaniem, mierzone za pomocą całkowitej liczby wyszukiwań w Google. Możemy obserwować, jak zmienia się ono na przestrzeni 24 miesięcy (od kwietnia 2013 do marca 2015) i porównać je między trzema tematami zaliczanymi do tej grupy.

WYKRES 1.2 Zainteresowanie opinii publicznej *data surveillance* – miesiąc po miesiącu



Źródło: opracowane własne.

W przeciwieństwie do poprzedniego wykresu w czerwcu 2013 roku nie odnotowano wzrostu zainteresowania opinii publicznej tematami związanymi z *data surveillance*. Wzrost zainteresowania tematami związanymi z ochroną danych i regulacjami prawnymi w tym zakresie nastąpił we wrześniu 2013 roku. W ciągu kolejnych 20 miesięcy oba tematy wykazywały niemal identyczny trend zainteresowania i zauważalną sezonowość; ze spadkiem zainteresowania w lipcu, sierpniu i grudniu oraz wzrostem w październiku, listopadzie, styczniu i marcu. Zainteresowanie związane z inwigilacją było niskie – średnio tylko 4 000 wyszukiwań miesięcznie.

Dodatkowo analiza potwierdziła, że pomiędzy *data leaks* i *data surveillance* istnieje dodatnia korelacja (współczynnik korelacji Pearsona = 0,62). Obserwacja związku między *data leaks* i *surveillance* wskazuje, że ujawnienie informacji przez Edwarda Snowdena mogło wpłynąć na zachowania ludzi, którzy w wyszukiwarce Google najpierw szukali tematów związanych z samym Snowdenem (*data leaks*), a następnie zainteresowali się tematami, na które w wyniku ujawnionych przez niego informacji zwracano szczególną uwagę (*data surveillance*).

Aby potwierdzić występowanie wpływu *data leaks* na *data surveillance*, zastosowano analizę korelacji krzyżowej. Metoda ta pozwala na porównanie dwóch szeregów czasowych w celu oszacowania, jak się one do siebie mają i identyfikacji przesunięcia czasowego o najlepszym dopasowaniu.

TABELA 1. Korelacja krzyżowa pomiędzy *data leaks* i *data surveillance*

Time lag	Cross-correlation	Standard error
–10	0,011	0,267
–9	0,000	0,258
–8	–0,002	0,250
–7	0,006	0,243
–6	0,002	0,236
–5	–0,012	0,229
–4	–0,003	0,224
–3	0,004	0,218
–2	–0,031	0,213
–1	–0,214	0,209
0	–0,452	0,204
1	–0,552	0,209
2	–0,239	0,213
3	0,079	0,218
4	0,128	0,224
5	–0,017	0,229
6	–0,035	0,236
7	0,115	0,243
8	0,258	0,250
9	0,223	0,258
10	0,072	0,267

Źródło: opracowanie własne.

Współczynniki korelacji krzyżowych zaprezentowane w tabeli 1 wskazują, że najsilniejszy związek pomiędzy *data leaks* i *data surveillance* występuje przy przesunięciu czasowym o jeden miesiąc (–0,552). Wynika z tego, że najsilniejszy wpływ zainteresowania *data leaks* na zainteresowanie *data surveillance* występował w miesiąc po ujawnieniu informacji przez Snowdena, w czasie, gdy zainteresowanie tymi informacjami już słabło, na co wskazuje negatywny znak korelacji krzyżowej. Nie jest to nic niezwykłego, zważywszy, że ujawnienie informacji przez Snowdena miało charakter wydarzenia jednostkowego, rzadkiego (*rare event*), o dynamice specyficznej dla przebiegu tego typu zdarzeń, a zatem charakteryzowało się gwałtownym, punktowym wręcz nasileniem w momencie wystąpienia, by wraz z upływem czasu przybrać postać krzywej opadającej. Jeśli konsekwencją takiego zdarzenia miałby być wzrost zainteresowania problematyką inwigilacji, związek między obydwoma zjawiskami, poza czasowym przesunięciem, musi pozostawać negatywny.

W rezultacie – wracając do pytań postawionych wcześniej – można stwierdzić, że ujawnienie informacji przez Edwarda Snowdena nie było jedynie „medialnym skandalem". Początkowe zainteresowanie Snowdenem przełożyło się na wzrost zainteresowania tematami, na które zwrócił on uwagę: inwigilacją w sieci, prywatnością i ochroną danych, a także koniecznością stworzenia regulacji prawnych.

HIPOTEZA

Stałe monitorowanie i wykorzystywanie informacji umożliwiających identyfikację osób bez ich wiedzy i zgody wykracza poza retorykę demokratycznego rządu, który takie działania legitymizuje i uzasadnia koniecznością zapewnienia bezpieczeństwa swoim obywatelom. Ujawnione przez Edwarda Snowdena tajne programy masowej inwigilacji z definicji nie są przejrzyste ani dostępne, podważają zaufanie do instytucji rządowych i kwestionują istnienie demokratycznych wartości i rządów prawa, za które obywatele rozliczają demokratyczne państwo. Informacje przekazane przez Snowdena ujawniły coś więcej niż tajny program, były jak sygnał ostrzegawczy, oskarżający demokratyczne władze o zdradę ich najwyższych wartości, w tym o nieprzestrzeganie jednego z podstawowych praw człowieka – prawa do prywatności. Benjamin Goold przekonuje, że członkowie społeczeństw demokratycznych mogą okazywać zaniepokojenie praktykami naruszającymi prywatność, jeśli odbiorą je jako zagrożenie dla demokratycznych praw i wolności człowieka [Goold 2010]. Negatywna percepcja może skutkować różnorakimi zachowaniami, z których niektóre charakteryzują się pasywnością, jak na przykład opisane wcześniej praktyki autocenzury, w ramach których

internauci unikają określonych dyskusji w sieci lub wchodzenia na strony, które mogą zostać uznane za potencjalnie niebezpieczne; a inne mają charakter aktywny, na przykład regularne czyszczenie pamięci podręcznej i plików cookie, korzystanie z przeglądarki i serwisów, które nie zbierają danych o użytkownikach, ale także zaangażowanie w działania mające na celu zwrócenie uwagi publicznej na istotność kwestii dotyczących prywatności i bezpieczeństwa danych w Internecie. W naszym badaniu przyjmujemy, że wyszukiwanie informacji w Google na tematy związane z inwigilacją, ochroną danych i prywatnością w Internecie jest przejawem zainteresowania, które z definicji wskazuje, że dany temat był dla użytkownika istotny.

Natomiast w reżimach totalitarnych, gdzie stały monitoring i kontrola są warunkiem koniecznym do zapewnienia stabilności i utrzymania władzy, nadzór rządu sam w sobie byłby czynnikiem hamującym zdolność lub chęć obywatela do poszukiwania informacji na tematy drażliwe, w tym na temat prawa do prywatności, ochrony danych czy inwigilacji. W związku z tym stawiamy hipotezę, że będzie istniała pozytywna korelacja pomiędzy jakością demokracji w danym kraju a poziomem zainteresowania opinii publicznej badanymi tematami w Google.

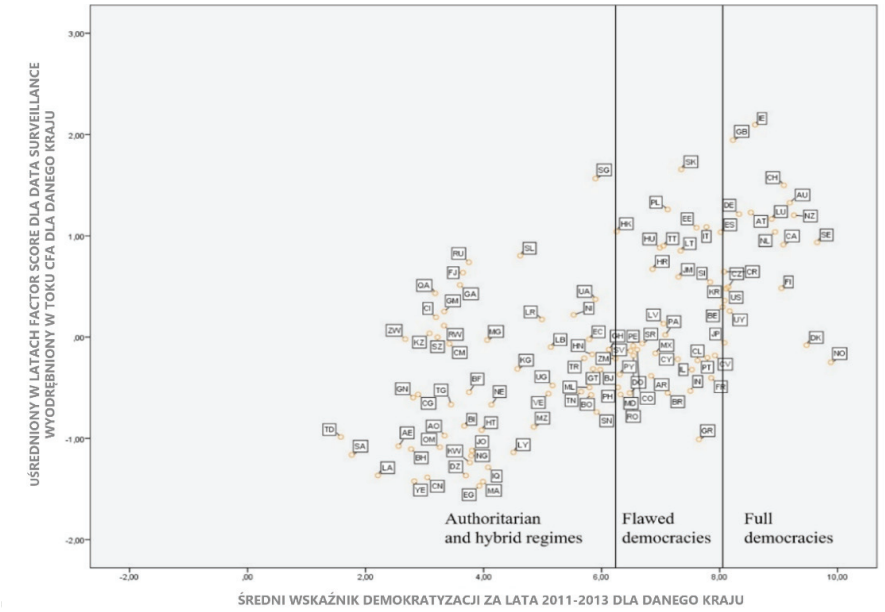
WYNIKI

Ponieważ potwierdzony został efekt wzmocnienia zainteresowania opinii publicznej tematami *data leaks* w związku z zainteresowaniem opinii publicznej tematami *data surveillance*, do testowania hipotezy wykorzystamy *data surveillance* jako *zmienną zależną*, której wartości zostały uśrednione dla wszystkich 24 punktów pomiarowych, oraz wskaźnik demokracji (*zmienna niezależna*) uśredniony dla trzech lat (2011, 2012, 2013) oddzielnie dla każdego kraju (112 krajów). Przedstawione poniżej wyniki obrazują zależność pomiędzy zmiennymi i potwierdzają, że wykres rosnącej funkcji liniowej odpowiada postawionej hipotezie. Zainteresowanie opinii publicznej tematyką *data surveillance* jest pozytywnie skorelowane z poziomem jakości demokracji (współczynnik korelacji 0,40 i istotny statystycznie).

Pierwszą grupę stanowią kraje zaliczane do reżimów autorytarnych i demokracji hybrydowych, w których zainteresowanie *data surveillance* jest niskie lub średnie. Najniższy poziom zainteresowania występuje w krajach afrykańskich i azjatyckich. Wśród krajów o wyższym poziomie zainteresowania pojawiają się Rosja, Fidżi, Sierra Leone. Ciekawym przypadkiem w tej grupie jest Singapur, w którym poziom zainteresowania opinii publicznej tematyką *data surveillance*

jest jednym z najwyższych. Od 2014 roku Singapur jest klasyfikowany jako demokracja wadliwa (*flawed democracy*).

GRAF 1. Związek pomiędzy zainteresowaniem opinii publicznej tematyką *data surveillance* a poziomem jakości demokracji



Źródło: opracowanie własne.

Drugą grupę stanowią kraje sklasyfikowane jako demokracje wadliwe (*flawed democracies*), w których zainteresowanie społeczne tematyką *data surveillance* oscyluje najczęściej na średnim poziomie. W tej grupie znajdują się kraje z Ameryki Południowej oraz kraje europejskie wyróżniające się jednym z niższych poziomów zainteresowania, takie jak Francja, Grecja i Rumunia. Na przeciwległym końcu skali dominują kraje postkomunistyczne: Słowenia, Chorwacja, Litwa, Węgry, Estonia, Polska i Słowacja, gdzie zainteresowanie było najwyższe.

W grupie krajów sklasyfikowanych jako demokratyczne dominuje wysoki poziom zainteresowania społeczeństwa tematyką *data surveillance*. Zaczynając od krajów, w których zainteresowanie to jest na średnim poziomie, wymienić należy trzy kraje skandynawskie, a także Urugwaj, Japonię, Belgię, Koreę Południową, Stany Zjednoczone, Czechy i Kostarykę. Co ciekawe, niektóre kraje

zostały zdegradowane i są obecnie klasyfikowane jako demokracje wadliwe (Belgia, Czechy, Kostaryka, Stany Zjednoczone).

Kraje o najwyższym stopniu zainteresowania opinii publicznej tematyką *data surveillance* to głównie państwa z Europy Zachodniej, ale także Kanada, Nowa Zelandia i Australia.

PODSUMOWANIE

Celem przedstawionego projektu badawczego było zbadanie poziomu zainteresowania opinii publicznej tematyką inwigilacji online, prywatności i ochrony danych w kontekście informacji ujawnionych przez Edwarda Snowdena. W badaniu porównano na szeroką skalę, czy polityczne makrodeterminanty różnicują ten poziom zainteresowania publicznego w poszczególnych krajach. Potwierdzono empirycznie hipotezę, że w krajach o wyższym poziomie demokracji zainteresowanie opinii publicznej tematem inwigilacji jest większe niż w pozostałych krajach. Jako źródło danych wykorzystano dane z wyszukiwarki Google dla 116 krajów, a zapytania sprawdzono w lokalnych językach.

Uzyskane wyniki wpisują się w teorię Benjamina Goolda, według której członkowie społeczeństw demokratycznych będą zaniepokojeni praktykami naruszającymi ich prywatność, jeśli odbiorą je jako zagrożenie dla demokratycznych praw i wolności człowieka, co w konsekwencji może prowadzić do zachowań mających na celu ochronę przed takimi praktykami [Goold 2010]. W naszym podejściu dokonaliśmy pewnej interpretacji teorii Goolda, rozszerzając wachlarz zachowań stosowanych przez osoby zaniepokojone zbyt dużą ingerencją władz w prywatne życie obywateli, nawet jeśli tylko w świecie wirtualnym. Otóż, zdefiniowaliśmy szereg dodatkowych zachowań, mierzalnych za pomocą wyszukiwarki Google: wyszukiwanie informacji na tematy związane z prywatnością danych i informacji, sprawdzanie, czy istnieją akty i regulacje prawne, które je chronią, monitorowanie organizacji pozarządowych (WikiLeaks) i aktywistów zaangażowanych w nagłaśnianie podobnych spraw (np. Edward Snowden czy Julian Assange).

W wyniku przeprowadzenia analizy korelacji krzyżowej pomiędzy tematami w obrębie dwóch grup: *data leaks* i *data surveillance*, potwierdzono empirycznie, że ujawnienie informacji przez Edwarda Snowdena i tocząca się następnie debata o międzynarodowym zasięgu były czymś więcej niż kolejnym newsem w mediach. Innymi słowy, tuż po ujawnieniu skandalu najczęściej wyszukiwano informacje na temat osoby Edwarda Snowdena, natomiast w dłuższej perspektywie, kiedy dyskurs polityczny zataczał coraz szersze kręgi, zwiększyło się

zainteresowanie także tematami, na które Snowden zwracał uwagę: masowa inwigilacja, konieczność ochrony prywatności danych i informacji, wprowadzenie odpowiednich regulacji prawnych.

W przedstawionym projekcie badawczym odnieśliśmy się także do teorii, których autorzy zwracają uwagę na problem ignorowania przez internautów kwestii prywatności i lekceważenia poważnych konsekwencji praktyk inwigilacyjnych, czy to w wyniku otrzymywania korzyści i gratyfikacji w zamian za udostępnienie przez użytkownika danych osobowych [Gandy 1993; Raab, Koops 2009; Zuboff 2015], czy też z powodu korodujących skutków kapitalizmu, który osłabia wartości demokratyczne, prowadząc do tego, że konsument „wypiera" obywatela [Reich 2009]. Wstępne wyniki naszych badań tego nie potwierdzają. Zainteresowanie opinii publicznej badanymi tematami było bardzo wysokie w krajach kapitalistycznych, w których gospodarka opiera się na prywatnym biznesie, a ceny ustalane są przez wolny rynek, głównie w oparciu o podaż i popyt oraz stałą relację między producentem a konsumentem, przy niewielkiej lub żadnej kontroli ze strony rządu. W interesie właścicieli firm leży decydowanie i regulowanie alokacji zasobów, określanie, jakie dobra są produkowane i gdzie będą sprzedawane, a do poszczególnych obywateli należy dokonywanie wyborów ekonomicznych. W związku z tym członkowie społeczeństw kapitalistycznych są tak mocno zaangażowani w codzienne transakcje gospodarcze (z których większość odbywa się online, szczególnie w okresie pandemii), że prawdopodobnie będą bardziej zainteresowani zabezpieczeniem swoich danych online i korzystaniem z Google jako źródła informacji na ten temat. Proponujemy zweryfikować tę hipotezę w kolejnym badaniu.

Podczas analiz zwróciliśmy także uwagę na pewne różnice w rozkładzie krajów w odniesieniu do poziomu zainteresowania opinii publicznej i zmiennych na poziomie kraju. Zainteresowanie opinii publicznej tematami związanymi z *data surveillance* było bardzo podobne w krajach postkomunistycznych, podczas gdy w innych krajach europejskich było ono wyższe, ale i bardziej zróżnicowane. Zalecana byłaby dalsza analiza – przeprowadzona tylko dla krajów europejskich i z dodatkowymi zmiennymi – w celu potwierdzenia poprawności wstępnych wyników.

Istotną kwestią, której nie poruszyliśmy w badaniu, jest także rola mediów. Wszak to, jak często i w jaki sposób dany problem jest przedstawiany, może determinować poziom zainteresowania opinii publicznej danym tematem.

BIBLIOGRAFIA

Alon Gal (Under The Breach). https://twitter.com/UnderTheBreach [access: 03.04.2021].

Bauman Zygmunt, **Didier Bigo**, **Paulo Esteves**, **Elspeth Guild**, **Vivienne Jabri**, **David Lyon**, **R.B.J. Walker**. 2014. "After Snowden: Rethinking the impact of surveillance". *International Political Sociology* 8(2): 121–144.

Beck Ulrich. 2008. *World at risk*. 2 edition. Cambridge: Polity Press.

Beck Ulrich. 2009. *Risk society: Towards a new modernity*. Repr. Theory, Culture and Society. London: Sage.

Beniger James R. 1986. *The control revolution. Technological and economic origins of the information society*. Cambridge: Harvard University Press.

Büchi Moritz, **Natascha Just**, **Michael Latzer**. 2017. "Caring is not enough: The importance of internet skills for online privacy protection". *Information, Communication and Society* 20(8): 1261–1278.

Castells Manuel. 2011. *The rise of the network society*. Hoboken: John Wiley & Sons.

CIGI-Ipsos. 2014. Global survey on internet security and trust. Centre for International Governance Innovation https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/ [access: 07.02.2021].

Cohrs J. Christopher, **Sven Kielmann**, **Jürgen Maes**, **Barbara Moschner**. 2005. "Effects of right-wing authoritarianism and threat from terrorism on restriction of civil liberties". *Analyses of Social Issues and Public Policy* 5: 263–276.

Davies Simon. 2014. A crisis of accountability. A global analysis of the impact of the Snowden revelations. Privacy Surgeon. https://www.academia.edu/7305250/A_Crisis_of_Accountability_-_A_Global_Analysis_of_the_Impact_of_the_Snowden_Revelations_2014_University_of_Amsterdam_and_Vrie_Universiteit_of_Brussels_ [access: 07.02.2021].

Dencik Lina, **Jonathan Cable**. 2017. "Digital citizenship and surveillance. The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks". *International Journal of Communication* 11: 763–781.

Dwa lata RODO: „Testy zderzeniowe" na dwie gwiazdki. https://panoptykon.org/audyt-rodo [dostęp: 01.03.2021].

Facebook monthly active users worldwide. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [access: 07.02.2021].

Flash Eurobarometer. 2008. Flash Eurobarometer series 226: Data protection in the European Union. Brussels: The Gallup Organization. https://data.europa.eu/data/datasets/s666_226 [access: 07.02.2021].

Friedewald Michael, **Peter J. Burgess**, **Johann Cas**, **Rocco Bellanova**, **Walter Peissl** (eds.). 2017. *Surveillance, privacy and security: Citizens' perspectives*. 1st edition (Hardback). London & New York: Routledge.

Friedewald Michael, **Marc van Lieshout**, **Sven Rung**, **Merel Ooms**. 2016. The context-dependence of citizens'. Attitudes and preferences regarding privacy and security. In: *Data protection on the move: Current developments in ICT and privacy/data protection*, S. Gutwirth, R. Leenes, P. De Hert (eds.), 51–74. Dordrecht: Springer Netherlands.

Friedewald Michael, **Ronald J. Pohoryles** (eds.). 2014. *Privacy and security in the digital age*. London & New York: Routledge. https://www.routledge.com/Privacy-and-Security-in-the-Digital-Age-1st-Edition/Friedewald-Pohoryles/p/book/9781138787308.

Gandy Oscar H. 1993. *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview.

Garfinkel Simson. 2000. *Database nation: The death of privacy in the 21st century*. Sebastopol: O"Reilly Media, Inc.

Goold Benjamin J. 2010. How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. In: *Overvåkning i en rettsstat – surveillance in a constitutional government*, D.W. Schartum (ed.), 38–48. Bergen: Fagbokforlaget.

Granka Laura A. 2010. "Measuring agenda setting with online search traffic: Influences of online and traditional media". SSRN Scholarly Paper ID 1658172. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=1658172.

Greenwald Glenn. 2014. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Metropolitan Books.

Haggerty Kevin D., **Amber Gazso**. 2005. "The public politics of opinion research on surveillance and privacy". *Surveillance & Society* 3(2/3): 173–180.

Hampton Keith, **Lee Rainie**, **Weixu Lu**, **Maria Dwyer**, **Inyoung Shin**, **Kristen Purcell**. 2014. Social media and the 'spiral of silence'. Pew Research Center: Internet, Science & Tech (blog). 26 August 2014. https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/ [access: 07.02.2021].

Hoy Mariea Grubbs, **George R. Milne**. 2010. "Gender differences in privacy-related measures for young adult Facebook users". *Journal of Interactive Advertising* 10(2): 28–45.

Huijboom Noor, **Gabriela Bodea**. 2015. "Understanding the political PNR debate in Europe: A discourse analytical perspective". *European Politics and Society* 16(2): 241–255.

Internet live stats. Internet usage and social media statistics. https://www.internetlivestats.com/ [access: 07.02.2021].

Internet users in the world 2021. https://www.statista.com/statistics/617136/digital-population-worldwide [access 07.02.2021].

Juza Marta. 2019. *Między wolnością a nadzorem: Internet w zmieniającym się społeczeństwie*. Warszawa: Wydawnictwo Naukowe Scholar.

Kezer Murat, **Barış Sevi**, **Zeynep Cemalcilar**, **Lemi Baruh**. 2016. "Age differences in privacy attitudes, literacy and privacy management on Facebook". *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10(1). https://cyberpsychology.eu/article/view/6182/5912.

Kokolakis Spyros. 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon". *Computers & Security* 64 (January): 122–134.

Kowalczyk Marcin. 2019. *Cyfrowe państwo: uwarunkowania i perspektywy*. Warszawa: Wydawnictwo Naukowe PWN.

Krzysztofek Kazimierz. 2011. „W stronę maszyn społecznych. Jaka będzie socjologia, której nie znamy?". *Studia Socjologiczne* 2(201): 123–145.

Krzysztof Kazimierz. 2012. „Zmiana permanentna? Refleksje o zmianie społecznej w epoce technologii cyfrowych". *Studia Socjologiczne* 4(207): 7–39.

Lai Kaisheng, **Yan Xin Lee**, **Hao Chen**, **Rongjun Yu**. 2017. "Research on web search behavior: How online query data inform social psychology". *Cyberpsychology, Behavior, and Social Networking* 20(10): 596–602.

Lyon David. 1993. "An electronic panopticon? A sociological critique of surveillance theory". *The Sociological Review* 41(4): 653–678.

Lyon David. 1994. *The electronic eye: The rise of surveillance society*. NED-New edition. Minneapolis: University of Minnesota Press.

Lyon David. 2014. "Surveillance, Snowden, and big data: Capacities, consequences, critique". *Big Data & Society* 1(2): 1–13.

Lyon David. 2017. "Surveillance culture: Engagement, exposure, and ethics in digital modernity". *International Journal of Communication* 11: 1–18.

Lyon David. 2018. *The culture of surveillance: Watching as a way of life*. Hoboken: John Wiley & Sons.

Marwick Alice. 2012. "The public domain: Surveillance in everyday life". *Surveillance & Society* 9(4): 378–393.

Maslow A.H. 1943. "A theory of human motivation." *Psychological Review* 50(4): 370–396.

Mau Steffen. 2019. *The metric society: On the quantification of the social*. Hoboken: John Wiley & Sons.

Maurer Marcus, **Thomas Holbach**. 2016. "Taking online search queries as an indicator of the public agenda: The role of public uncertainty". *Journalism & Mass Communication Quarterly* 93(3): 572–586.

Mazur Joanna. 2018. "Right to access information as a collective-based approach to the GDPR"s right to explanation in European law". *Erasmus Law Review* 11(3): 178–189.

Mellon Jonathan. 2013. "Where and when can we use Google Trends to measure issue salience?". *PS: Political Science & Politics* 46(02): 280–290.

Mellon Jonathan. 2014. "Internet search data and issue salience: The properties of Google Trends as a measure of issue salience". *Journal of Elections, Public Opinion and Parties* 24(1): 45–72.

Neumann Alexander, **Regina Berglez**, **Reinhald Kreissl**, **Nils Zurawski**, **Chiara Fonio**, **Keith Spiller**, **Charles Leleux**, **C. William R.**, **Webster**, **Walter Peissl**, **Eric Lastic**, **Martin Kovanic**. 2014. "IRISS increasing resilience in surveillance societies. Deliverable D 6.1: Doing privacy in everyday encounters with eurveillance". http://epub.oeaw.ac.at/0xc1aa5576%200x0031e819.pdf.

Noelle-Neumann Elisabeth. 1993. *The spiral of silence. Public opinion – our social skin.* Chicago: University of Chicago Press.

Nowak Stefan. 2012. *Metodologia badań społecznych*. Warszawa: Wydawnictwo Naukowe PWN.

Number of internet users. https://www.internetlivestats.com/internet-users/ [access: 07.02.2021].

Penney Jon. 2016. "Chilling effects: Online surveillance and Wikipedia use". SSRN Scholarly Paper ID 2769645. Rochester, *Berkeley Technology Law Journal* 31(1): p. 117–182.

Pew Research Center. 2013. Public split over impact of NSA leak, but most want Snowden prosecuted. Pew Research Center for the People and the Press (blog). https://www.people-press.org/2013/06/17/public-split-over-impact-of-nsa-leak-but-most-want-snowden-prosecuted/ [access: 07.02.2021].

Raab Charles D., **Bert-Jaap Koops**. 2009. "Privacy actors, performances and the future of privacy protection". In: *Reinventing data protection?*, S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt, 207–221. Dordrecht: Springer Netherlands.

Ragas Matthew W., **Hai Tran**. 2013. "Beyond cognitions: A longitudinal study of online search salience and media coverage of the president". *Journalism & Mass Communication Quarterly* 90(3): 478–499.

Reich Robert B. 2009. How capitalism is killing democracy. Foreign Policy (blog). 2009. https://foreignpolicy.com/2009/10/12/how-capitalism-is-killing-democracy/ [access: 07.02.2021].

Scharkow Michael, **Jens Vogelgesang**. 2011. "Measuring the public agenda using search engine queries". *International Journal of Public Opinion Research* 23(1): 104–113.

Sheehan Kim Bartel. 1999. "An investigation of gender differences in on-line privacy concerns and resultant behaviors". *Journal of Interactive Marketing* 13(4): 24–38.

Solove Daniel J. 2011. *Nothing to hide: The false tradeoff between privacy and security*. New Heaven: Yale University Press.

Special Eurobarometer. 2011. Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union. Brussels: TNS Opinion & Social. https://data.europa.eu/data/datasets/s864_74_3_ebs359 [access: 07.02.2021].

Special Eurobarometer. 2015. Special Eurobarometer 431: Data protection. Directorate-General for Communication. https://data.europa.eu/data/datasets/s2075_83_1_431_eng [access: 07.02.2021].

Stoycheff Elizabeth. 2016. "Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring". *Journalism & Mass Communication Quarterly* 93(2): 296–311.

Svenonius Ola, **Fredrika Björklund**. 2018. "Explaining attitudes to secret surveillance in post-communist societies". *East European Politics* 34(2): 123–151.

Szpunar Magdalena. 2012. *Nowe-stare medium: Internet między tworzeniem nowych modeli komunikacyjnych a reprodukowaniem schematów komunikowania masowego*. Warszawa: Wydawnictwo IFiS PAN.

Trottier Daniel. 2012. "Interpersonal surveillance on social media". *Canadian Journal of Communication* 37(2): 319–332.

Turner Anna, **Marcin W. Zielinski**, **Kazimierz M. Slomczynski**. 2018. „Google Big Data: charakterystyka i zastosowanie w naukach społecznych". *Studia Socjologiczne* 4(231): 49–71.

Van den Broeck Evert, **Karolien Poels**, **Michel Walrave**. 2015. "Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood". *Social Media + Society* 1(2): 1–11.

Watson Hayley, **David Wright**. 2013. The PRIvacy and security mirrorS: Towards a European framework for integrated decision making. Deliverable 7.1: Report on existing surveys. https://publica.fraunhofer.de/documents/N-502279.html [access: 07.02.2021].

Wimmer Jeffrey, **Thorsten Quandt**. 2006. "Living in the risk socety: An interview with Ulrich Beck". *Journalism Studies* 7(2): 336–347.

Wood David Murakami. 2009. "The 'surveillance society': Questions of history, place and culture". *European Journal of Criminology* 6(2): 179–194.

Wood David Murakami, **C. William R. Webster**. 2009. "Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britains' bad example". *Journal of Contemporary European Research* 5(2): 259–273.

Wystąpienie UODO do władz Facebook Poland. https://uodo.gov.pl/pl/138/2022 [access: 30.04.2021].

Zhu J., **Xiaohua Wang**, **Jie Qin**, **L. Wu**. 2012. Assessing public opinion trends based on user search queries: validity, reliability, and practicality. https://scholars.cityu.edu.hk/en/publications/assessing-public-opinion-trends-based-on-user-search-queries(54cc3372-239d-40cd-8e3f-1a6e875ecfd7).html. [access: 07.02.2021]

Zuboff Shoshana. 2015. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89. Doi:10.1057/jit.2015.5.

Anna Turner
Marcin W. Zieliński

PUBLIC INTEREST IN TOPICS OF SURVEILLANCE, PRIVACY AND DATA PROTECTION. GOOGLE BIG DATA IN COMPARATIVE SOCIOLOGY

Abstract

This paper presents the results of a research project that examined the impact of macro--determinants on public interest in the topics of surveillance, data protection and online privacy in the context of Edward Snowden's revelations about the existence of a global mass surveillance program. The level of public interest was estimated based on the number of Google searches related to surveillance in 116 countries, in which comparative analyses were then conducted. We are going to verify the hypothesis that in countries with a higher level of democracy there is greater public interest in surveillance than in other countries. The paper will also present ways of adapting Google data to the needs of the social sciences.

Keywords: Google Keyword Planner, big data, Google Trends, internet data, Edward Snowden, surveillance, privacy, data protection, public opinion research