Jan Waszewski

Koniec prywatności a spory wokół *big data*, mediów społecznościowych i neuronauki[1]

Artykuł dotyczy wpływu kilku aspektów rozwoju nauki i technologii na prywatność. Porządek wywodu jest następujący: po pierwsze, autor artykułu wskazuje, jak rozumie pojęcie prywatność. Po drugie, przywołuje przykłady nowych technik kontroli społecznej oraz powiązane z nimi najważniejsze spory i kontrowersje pojawiające się wraz z rozwojem systemów *big data*, mediów społecznościowych i badań nad mózgiem. Po trzecie, wskazuje, jakie okoliczności sprawiają, że ukrycie się przed systemami nadzoru jest niemożliwe. Celem kolejnych części artykułu jest zarysowanie mapy powiązań pomiędzy omawianymi w nim zagadnieniami. Ta mapa ma z kolei pozwolić na zademonstrowanie, jak blisko znaleźliśmy się sytuacji, w której nie będziemy w stanie ukryć się przed nowymi technikami kontroli społecznej. W artykule postawiono tezę, że wyłaniająca się sytuacja wynika przede wszystkim z synergii między sposobem wykorzystania systemów *big data*, mediami społecznościowymi i badaniami nad mózgiem.

Niniejszy artykuł to zmienione *Zakończenie* rozprawy doktorskiej, którą autor obronił w 2018 r. na Wydziale Humanistycznym UMK w Toruniu i która nosi tytuł *„Nie ukryjesz się". Nowe techniki kontroli społecznej a spory wokół big data, mediów społecznościowych i ustaleń neuronauki*[2].

Zakończenie rozprawy z założenia nie miało być prostą rekapitulacją prowadzonych rozważań i analiz. Celem autora było pokazanie, na czym polega synergia pomiędzy zjawiskami wskazanymi w tytule pracy i jakie są jej konsekwencje.

Prywatność

Autor artykułu rozumie p r y w a t n o ś ć, zgodnie z powszechnie przyjętą definicją, jako zdolność jednostki lub grupy do nieupubliczniania – zachowania w tajemnicy,

[1] Fragment rozprawy doktorskiej pt. *Nie ukryjesz się. Nowe techniki kontroli społecznej a spory wokół big data, mediów społecznościowych i ustaleń neuronauki* (Uniwersytet Mikołaja Kopernika w Toruniu). Autor wykorzystał *Zakończenie rozprawy*.

[2] Promotorem pracy był dr hab. Andrzej Zybertowicz, prof. UMK w Toruniu, a promotorem pomocniczym – dr hab. Krzysztof Pietrowicz. Obecnie jest przygotowywana publikacja rozprawy w formie książki.

ukrycia przed innymi – wybranych przez siebie informacji na swój temat[3]. Warto przyjrzeć się tej kwestii głębiej.

Prywatność, uznawana za jedno z praw człowieka, jest regulowana traktatami oraz umowami międzynarodowymi. Przykładowo, artykuł 8 europejskiej konwencji praw człowieka[4] mówi o (…) *prawie do poszanowania życia prywatnego i rodzinnego*. Zgodnie z punktem 2. tego artykułu władze nie mogą ingerować w prawo do prywatności (…) *z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie*. Prywatność można naruszać tylko (…) *z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób*[5].

Obecnie regulacje w sferze danych osobowych i związanych z nimi problemów dotyczących prywatności wyznacza w Unii Europejskiej *Rozporządzenie o Ochronie Danych Osobowych* (dalej: RODO), które weszło w życie w maju 2018 r.[6] Dokument ma dać osobom przebywającym na terytorium UE i Europejskiego Obszaru Gospodarczego m.in. możliwość zarządzania własną prywatnością, tj. decydowania o tym, kto i w jaki sposób korzysta z naszych danych osobowych[7]. Najważniejsza powinna tu być zgoda na zrezygnowanie z zachowania prywatności, świadoma i bazująca na dokładnych informacjach o konsekwencjach takiego kroku[8].

Tytułowe dla rozprawy *„Nie ukryjesz się"* sugeruje, że w erze, w której nowe techniki kontroli społecznej są rozwijane i rozbudowywane dzięki systemom analizującym masowe ilości wciąż nowych typów danych cyfrowych (*big data*), mediom społecznościowym oraz ustaleniom neuronauki (badań nad mózgiem), prywatność rozumiana zgodnie z powyższym ujęciem po prostu może zaniknąć. Coraz trudniej jest bowiem znaleźć sfery, w których ludzie są w stanie ją zachować.

---

[3] Zob. np. D.J. Solove, *Conceptualizing Privacy*, „California Law Review" 2002, nr 4, s. 1087–1156. Por. G. Keizer, *Privacy*, New York 2012; D.J. Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security*, New Haven–London 2013.

[4] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r.*, *zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2* (DzU z 1993 r. nr 61 poz. 284.

[5] Tamże.

[6] *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* (Dz. Urz. UE L 119 z 4 V 2016, s. 1).

[7] Zob. np. C.-L. Yeh, *Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers*, „Telecommunications Policy" 2018, nr 4, s. 282–292.

[8] Trudno stworzyć kryteria, które jednoznacznie decydują o tym, kiedy ktoś został w sposób wystarczająco jasny i zrozumiały dla niego poinformowany o konsekwencjach podjętych przez niego działań. Problematyczne jest również to, jak wielu ludzi w ogóle czyta regulaminy opisujące zasady przechowywania, udostępniania, przetwarzania i wykorzystywania ich danych osobowych. Por. A. Szahaj, *Kapitalizm drobnego druku*, Warszawa 2014.

Nowe techniki kontroli społecznej

Pod pojęciem nowe techniki kontroli społecznej autor rozumie nowoczesne technologie informatyczne i telekomunikacyjne, które w coraz większym stopniu są wykorzystywane do zautomatyzowanego zbierania, analizowania i wykorzystywania danych gromadzonych w bazach danych w celu podtrzymywania porządku społecznego. Chodzi tu o różnego rodzaju narzędzia (techniki) służące do nadzorowania czy też monitorowania działań ludzi.

W tym miejscu zostaną wskazane przykłady nowych technik kontroli społecznej, które dobrze ilustrują ich wpływ na zanikanie prywatności. Kolejność przedstawiania poszczególnych technik jest zgodna z tym, jak daleko idąca jest skala przenikania przez nie sfer życia społecznego. Po pierwsze, są to nowe techniki kontroli społecznej, które są systemowo wbudowywane we współczesne społeczeństwa. Po drugie, zostaną wskazane techniki, które są wykorzystywane tylko w ramach wybranych instytucji i tym samym wpisują się w wymiary życia ludzi związane z tymi instytucjami.

Podstawą interpretacji zakresu przenikania sfer życia społecznego jest wiele milczących założeń dotyczących tego, czy i w jakiej sytuacji określone rozwiązania z dużym prawdopodobieństwem staną się powszechne. Spójrzmy na przykład na wykorzystywanie systemów kontroli czasu i jakości pracy w roli technik kontroli społecznej. Istnieje jakościowa różnica pomiędzy wpływem, jaki na sposób funkcjonowania pracownika ma tylko logowanie się za pomocą elektronicznych kart tożsamości przy bramie wejściowej do zakładu pracy a opaskami noszonymi stale na nadgarstku, żeby było możliwe analizowanie efektywności pracy – łącznie z monitorowaniem ruchów wykonywanych przez danego pracownika (jest to patent spółki Amazon[9]). Obie te techniki ewidencjonują obecność w pracy. Pierwsza z nich nie różni się jednak w istotny sposób od prostego podpisywania się na liście obecności. Skorzystanie z karty elektronicznej sprawia, że dane o przybyciu i opuszczeniu zakładu pracy trafiają do cyfrowej bazy danych. Z takim procesem może się też wiązać noszenie opasek opatentowanych przez Amazon. W bazie danych może zostać odnotowane wówczas każde opuszczenie stanowiska pracy, brak uwagi, niska efektywność w danym okresie, zbyt długie korzystanie z toalety lub plotkowanie ze współpracownikami. Ta ostatnia obserwacja wymaga tylko potwierdzenia obecności w tym samym miejscu i czasie dwóch lub więcej osób, które nie mają powodów służbowych, żeby ze sobą rozmawiać. Z takiej obserwacji można wywnioskować, że te osoby marnowały czas opłacony przez pracodawcę.

[9] T. Ong, *Amazon patents wristbands that track warehouse employees' hands in real time*, 1 II 2018 r., https://www.theverge.com/2018/2/1/16958918/amazon-patents-trackable-wristband-warehouse-employees [dostęp: 15 VI 2020]. Spółka już wcześniej była znana ze swoich praktyk polegających na wykorzystywaniu technologii, w tym robotów, do kontrolowania pracowników – ludzi. Zob. K. Krzysztofek, *Technologie cyfrowe w dyskursach o przyszłości pracy*, „Studia Socjologiczne" 2015, nr 4, s. 16.

Do technik kontroli społecznej, wszechobecnych i oddziałujących na życie codzienne ludzi oraz przywołujących ich do porządku (gdy przekraczają normy), należą państwowe systemy[10] bazodanowe i mechanizmy ich przeszukiwania oraz łączenia wyników tych analiz. W Polsce działają takie systemy, jak PESEL, CEPiK, AFIS, CEIDG, KRS oraz SIM[11]. Równolegle coraz większe znaczenie zyskują systemy bazodanowe tworzone przez podmioty prywatne oraz mechanizmy wydobywania z nich użytecznej wiedzy – od firm taksówkarskich i sklepów internetowych, przez media społecznościowe, po prywatną służbę zdrowia.

We współczesne społeczeństwa są systemowo wbudowane złożone systemy nadzoru tworzone przez państwa. Jako przykład jest wskazywany rosyjski SORM-3[12]; pewne cechy takiego systemu miał (ma?) także amerykański program PRISM[13]. Tego typu systemy są coraz częściej i w coraz większym stopniu rozpowszechniane – są już zakorzenione i oddziałują na funkcjonowanie całych grup i kategorii społecznych. Ich działanie polega na podejmowaniu prób gromadzenia przez tajne służby „wszystkich dostępnych" danych (w tym metadanych) „na wszelki wypadek", dzięki współpracy z podmiotami prywatnymi lub włamaniom do ich baz danych. Jednym z aspektów takich systemów są m.in. zasady pobierania danych przez upoważnione do tego służby (również zasady kontroli sądowej lub prokuratorskiej) oraz analizowanie tych danych pod kątem zagrożeń.

Podobny system, zbudowany zgodnie z powyższymi założeniami, jest obecnie tworzony np. w Chinach. Zakłada on współpracę państwa oraz podmiotów prywatnych w budowaniu zaufania społecznego dzięki zautomatyzowanemu, technicznemu systemowi przyznającemu ludziom i przedsiębiorstwom punkty w zamian za działania oceniane pozytywnie i odbierającemu punkty za działania oceniane negatywnie.

Do głęboko zakorzenionych systemów, które mają duży potencjał wykorzystania ich w roli techniki kontroli społecznej, należą mechanizmy wyświetlania reklam użytkownikom Internetu na podstawie wiedzy o ich zainteresowaniach. Systemy reklamowe Google'a i Facebooka obecnie mają na świecie pozycję dominującą[14]. Spółki, o których mowa, profilują ludzi i dzielą ich na kategorie – ten rodzaj techniki

[10] Są to systemy w sensie również administracyjnym, a nie tylko technicznym.

[11] Powszechny Elektroniczny System Ewidencji Ludności, Centralna Ewidencja Pojazdów i Kierowców, Automatyczny System Identyfikacji Daktyloskopijnej, Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowy Rejestr Sądowy, System Informacji Medycznej.

[12] Ros. Система оперативно-розыскных мероприятий (System Działań Operacyjno-Śledczych). Jest to element tytułu zarządzenia rosyjskiego ministra łączności i komunikacji masowej z 2014 r., które reguluje nadzór nad systemami telekomunikacyjnymi w Rosji.

[13] Zob. np. D. Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, „Big Data & Society" 2014, nr 2, s. 1–14.

[14] Zob. np. J. Koetsier, *Digital Duopoly Declining? Facebook's, Google's Share Of Digital Ad Dollars Dropping*, forbes.com, 19 III 2018 r., https://www.forbes.com/sites/johnkoetsier/2018/03/19/digital-duopoly-declining-facebooks-googles-share-of-digital-ad-dollars-dropping/#22396bf360a8 [dostęp: 15 VI 2020].

kontroli nie jest jednak ograniczony do pokazywania precyzyjnie kierowanych reklam. Podział ludzi na grupy jest również wykorzystywany w ramach innych systemów. Konsekwencje społeczne profilowania osób w celu sprawowania nad nimi kontroli prezentuje wspomniany wyżej system budowany w Chinach.

Systemy techniczne działające na bazie technik identyfikowania obiektów za pomocą sztucznej inteligencji z dużym prawdopodobieństwem zostaną w przeciągu najbliższych lat wbudowane w życie społeczne. Coraz powszechniejsze bowiem stają się systemy zautomatyzowanego rozpoznawania obrazu. Są to przykładowo systemy: rozpoznawania twarzy[15], marek samochodów i (lub) ich tablic rejestracyjnych[16] oraz emocji (a nawet intencji?[17]) ze sposobu poruszania się człowieka[18]. Te rozwiązania są stopniowo wbudowywane w szersze systemy kontroli społecznej. Najważniejszy jest tu przykład Chin, które rozbudowują krajowy system rozpoznawania twarzy[19].

Przykładem rozpoznawania człowieka po sposobie jego poruszania się jest analiza sposobu pisania na klawiaturze w celu dodatkowej weryfikacji, czy np. hasło do konta bankowego wpisuje jego właściciel[20]. Tego typu rozwiązania nadal nie są rozpowszechnione i dopiero znajdują się – przynajmniej w Polsce – w fazie prototypowej[21]. Techniki biometryczne usprawniające logowanie się do stron internetowych zmieniają sposób życia ludzi tylko w niektórych wymiarach. Wspierają walkę z wyłudzeniami, ale raczej nie mają możliwości przebudowania kontroli społecznej na większą skalę.

Konsekwencje społeczne – przynajmniej potencjalnie – mają takie pomysły jak ten firmy Uber (znanej z tego, że stworzyła aplikację mobilną, która kojarzy kierowcę samochodu z pasażerem i umożliwia temu drugiemu zamówienie przejazdu). Złożyła ona wniosek o opatentowanie techniki wykrywania, czy potencjalny pasażer jest nietrzeźwy[22]. Miałoby to być ustalane za pomocą algorytmów sztucznej inteligencji,

---

[15] Zob. np. K.A. Gates, *Our Biometric Future. Facial Recognition Technology and the Culture of Surveillance*, New York 2011.

[16] Zob. np. artykuł przeglądowy o badaniach na ten temat: S. Du i in., *Automatic license plate recognition (ALPR): A state-of-the-art review*, „IEEE Transactions on Circuits and Systems for Video Technology" 2013, nr 2, s. 311–325.

[17] Zob. np. E. Kemeny, *AI hunts for crimes caught on camera*, „New Scientist" z 18 sierpnia 2018 r., s. 10.

[18] Przykładowa analiza: C. Prakash, R. Kumar, N. Mittal, *Recent developments in human gait research: parameters, approaches, applications, machine learning techniques, datasets and challenges*, „Artificial Intelligence Review" 2018, nr 1, s. 1–40.

[19] H. Jacobs, *China's 'Big Brother' surveillance technology isn't nearly as all-seeing as the government wants you to think*, „Business Insider", 15 VII 2018 r., https://www.businessinsider.com/china-facial-recognition-limitations-2018-7 [dostęp: 15 VI 2020].

[20] Zob. np. P.H. Pisani i in., *Enhanced template update: Application to keystroke dynamics*, „Computers & Security" 2016, s. 134–153.

[21] B. Szafrański, *Biometria przyszłością bankowości*, relacja z „International Biometric Congress 2017", 27 IX 2017 r., https://alebank.pl/biometria-przyszloscia-bankowosci/ [dostęp: 15 VI 2020].

[22] J. Crook, *Uber applies for patent that would detect drunk passengers*, 11 VI 2018 r., https://tech-

na podstawie sposobu pisania wiadomości tekstowych przez prawdopodobnego podróżnego, sposobu trzymania przez niego telefonu oraz miejsca, z którego jest zamawiany kurs. Patent Ubera wskazuje, jak niebagatelny potencjał jako źródło technik kontroli społecznej mają smartfony oraz inne „inteligentne" urządzenia przenośne. Przykładowo, smartfon „uczy" się swojego użytkownika oraz dopasowuje się do jego potrzeb i w związku z tym zbiera dane na jego temat. W podobny sposób działają aplikacje, które są na nim zainstalowane – również one potrzebują jak najwięcej danych o użytkowniku.

Współcześnie coraz bardziej popularne stają się tzw. inteligentne domy[23]. Mają one możliwość wywoływania dużych zmian w życiu ludzi – dzięki temu, że wzory życia mieszkańców takich domów są analizowane w celu podnoszenia „inteligencji" urządzeń w nich wykorzystywanych, żeby można było poprawić kierujące nimi algorytmy. Tumaczy to się chęcią ułatwienia życia mieszkańcom. Obecnie „inteligentne domy" wpływają na życie tylko tych ludzi, którzy podążyli za pewną modą. Przez to, że tego typu domy dopiero się upowszechniają, wiedza o wzorcach życia ich mieszkańców ma tylko potencjalne zastosowanie jako masowo wykorzystywana nowa technika kontroli społecznej[24]. Warto jednak pamiętać o innych „inteligentnych" systemach, które również pojawiają się na rynku. Chodzi tu głównie o tzw. inteligentne samochody[25]. To prawdopodobnie właśnie one będą wskaźnikiem, czy „inteligentne systemy" zakorzenią się jako nowa technika kontroli społecznej o znaczeniu systemowym.

Wciąż tylko punktowo przenikają życie społeczne komercyjnie dostępne urządzenia działające dzięki technikom neuronauki, które analizują pracę mózgu i ją stymulują, aby poprawić wydajność uczenia się czy grania w gry komputerowe lub wzmożyć wysiłek fizyczny[26]. Te urządzenia zbierają dane, które mogą naruszać prywatność

---

crunch.com/2018/06/11/uber-applies-for-patent-that-would-detect-drunk-passengers/ [dostęp: 15 VI 2020].

[23] Zob. np. artykuł przeglądowy dotyczący opracowań na temat domowych zastosowań Internetu rzeczy: M. Alaa i in., *A review of smart home applications based on Internet of Things*, „Journal of Network & Computer Applications" 2017, nr 97, s. 48–65. Por. K. Gubański, *Smart city – sformatowany produkt czy narzędzie demokratyzacji? Dwa scenariusze rozwoju współczesnych polityk miejskich*, „Studia Socjologiczne" 2018, nr 1, s. 99–116.

[24] K. Gubański, *Smart city*…, s. 109.

[25] Zob. raporty o wyzwaniach, również dla prywatności, związanych z rozwojem rynku inteligentnych samochodów – *Monetizing car data: New service business opportunities to create new customer benefits*, 2016, McKinsey&Company, https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx [dostęp: 15 VI 2020]. Por. KPMG, *Your connected car is talking. Who's listening?*, 2016, https://assets.kpmg.com/content/dam/kpmg/se/pdf/komm/2016/se-your-connected-car-is-talking.pdf [dostęp: 15 VI 2020].

[26] L. Bradley, *NFL players using Halo headsets to get more out of their workouts*, „Sports Illustrated", 28 XII 2016 r., https://www.si.com/tech-media/2016/12/28/nfl-players-using-halo-headsets-get-more-out-their-brains [dostęp: 15 VI 2020]; M. Childs, *Neurostimulation Could Optimize Our Brains — If It Can Overcome the Stigma*, wpis na blogu „Think Leaders", 6 IX 2017 r.,

mózgu, czyli pozbawiają człowieka zdolności do ukrycia własnych emocji, a nawet myśli. Podobne urządzenia są testowane i tworzone przez siły zbrojne – z pewnością USA[27]. Istnieją jednak informacje wskazujące na to, że podobne próby przeprowadzają również Chiny[28].

Powyższy fragment odnosił się do nowych technik kontroli społecznej, stosowanych powszechnie i głęboko wbudowanych w życie społeczne, a także technik, których oddziaływanie jest wyłącznie punktowe, i technik o dopiero wyłaniającym się potencjale. Celem autora jest pokazanie, o jak złożonym polu jest tu mowa. Większość nowych technologii można wykorzystać nie tylko do realizacji ich zadań wyjściowych. Działanie tych technologii wiąże się z tworzeniem danych ułatwiających zdobywanie pogłębionej wiedzy o ludziach, łącznie z danymi, które ludzie bardzo chcieliby ukryć i utrzymać w sferze prywatnej (tajemnicy).

Kontrowersje wokół *big data,* mediów społecznościowych i ustaleń neuronauki

Wokół *big data*, mediów społecznościowych i ustaleń neuronauki pojawiło się wiele kontrowersji. Co jednak najważniejsze, w tych trzech sferach działalności biznesowej i naukowej można zaobserwować efekt synergii. Przykładowo, media społecznościowe i badania nad mózgiem są źródłem danych, które można przechowywać i analizować na dużą skalę dzięki systemom *big data*. To dzięki nim są możliwe zwiększanie zysków z działalności biznesowej oraz rozwój wiedzy naukowej. Media społecznościowe korzystają z badań nad mózgiem i powstających w ich trakcie danych, żeby jeszcze skuteczniej „uzależniać" swoich użytkowników i tym samym zwiększać zyski dzięki ich obecności przed ekranami telefonów i monitorów. Pojawiająca się synergia nie tylko sprzyja powstawaniu nowych technik nadzoru i nie tylko jest przyczyną zanikania prywatności. Jednocześnie trwa także inny proces. W jego ramach większość kontrowersji wyłaniających się wokół jednej z trzech sfer tytułowych dla artykułu

publikowanym na stronach IBM, https://web.archive.org/web/20170906160133/https://www.ibm.com/blogs/think-leaders/new-thinking/neurostimulation-optimize-brains-can-overcome-stigma/ [dostęp: 15 VI 2020]; T. Collins, *SF Giants trying Halo headphones to get back to World Series*, „c|net", 29 III 2017 r., https://www.cnet.com/news/sf-giants-halo-headphones-world-series-baseball/ [dostęp: 15 VI 2020]; D. McMahon, *America's top cyclist entering the Tour de France has been using a portable brain stimulator to try to gain an edge, and he says it actually works*, 26 VI 2017 r., http://www.businessinsider.com/tour-de-france-cyclist-talansky-halo-neuroscience-headset-technology-2017-6?IR=T [dostęp: 15 VI 2020].

[27] J. Nelson i in., *The Effects of Transcranial Direct Current Stimulation (tDCS) on Multitasking Throughput Capacity*, „Frontiers in Human Neuroscience" 2016, t. 10, artykuł 589, s. 1–13.

[28] S. Chen, *„Forget the Facebook leak": China is mining data directly from workers' brains on an industrial scale*, „South China Morning Post", 29 IV 2018 r., http://www.scmp.com/news/china/society/article/2143899/forget-facebook-leak-china-mining-data-directly-workers-brains [dostęp: 15 VI 2020].

przeradza się w kontrowersje dotyczące dwóch pozostałych. Warto przyjrzeć się tym zjawiskom bliżej.

Pod pojęciem *big data* autor artykułu rozumie systemy informatyczne zbierające, przetwarzające i analizujące w sposób zautomatyzowany gigantyczne ilości zróżnicowanych danych w celu stworzenia dodatkowej wartości.

Najbardziej kontrowersyjne jest to, że w związku z rozwojem systemów *big data* pojawiają się wątpliwości dotyczące sprawstwa ludzi. Skoro decyzje są podejmowane na podstawie pracy algorytmów sterujących tymi systemami, to czy ludzie, którzy nie rozumiejąc zasad ich działania, korzystają z ich rad, zachowują swoją podmiotowość? A może to właśnie kontrola nad danymi jest źródłem podmiotowości?[29]

Spory wywołuje również to, że zwolennicy i twórcy systemów *big data* albo pomijają kwestie etyczne, albo podkreślają neutralność etyczną technologii oraz algorytmów zarządzających takimi systemami[30]. Natomiast zdaniem krytyków tego typu systemy wcale nie są narzędziami neutralnymi społecznie, a błędy i (lub) uprzedzenia społeczne w algorytmach zarządzających nimi mogą mieć daleko idące negatywne konsekwencje[31].

Wątpliwości wywołuje także pytanie, czy systemy *big data* mogą doprowadzać do nasilania się m.in. nierówności społecznych: klasowych, etnicznych, wynikających z płci biologicznej czy kulturowej itd., ponieważ bazują na dotychczasowych danych i ekstrapolują głównie obecne w nich zjawiska[32]. W rezultacie tego typu systemy mają być – zdaniem ich krytyków – źródłem intensyfikacji zjawiska znanego jako efekt św. Mateusza[33]. Zarzuty wobec *big data* dotyczą na przykład tego, że w USA jest zakazane takie sterowanie rynkiem nieruchomości, które doprowadziłoby do powstawania sąsiedztw jednolitych etnicznie. W systemy *big data* firm pośredniczących w handlu nieruchomościami w USA były jednak wbudowane mechanizmy, które sprawiały,

---

[29] M. McCarthy, *The big data divide and its consequences*, „Sociology Compass" 2016, nr 10, s. 1136–1137. Por. K. Krzysztofek, *Kierunki ewaluacji technologii cyfrowych w działaniu społecznym. Próba systematyzacji problemu*, „Studia Socjologiczne" 2017, nr 1, s. 205.

[30] Zob. np. D. Boyd, *Undoing the Neutrality of Big Data*, „Florida Law Review" 2016, nr 67, s. 226–232; M. Frank, P. Roehrig, B. Pring, *What to do When Machines do Everything*, Hoboken 2017.

[31] Zob. np. D. Boyd, K. Crawford, *CRITICAL QUESTIONS FOR BIG DATA: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, „Information, Communication & Society" 2012, nr 5, s. 662–679.

[32] Zjawiska te opisała Cathy O'Neil (C. O'Neil, *Bronie matematycznej zagłady*, Warszawa 2019). Por. J. Piekutowski, *Bronie matematycznego zniszczenia*, „Nowa Konfederacja" 2017, nr 8, s. 3–10, https://nowakonfederacja.pl/bronie-matematycznego-zniszczenia/ [dostęp: 15 VI 2020]; Federal Trade Comission Report, *Big Data. A Tool for Inclusion or Exclusion?*, styczeń 2016 r., https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [dostęp: 15 VI 2020].

[33] Efekt św. Mateusza – zasada wywiedziona przez socjologa Roberta Mertona w latach 60. XX w. z Ewangelii św. Mateusza. Zgodnie z nią bogaci stają się jeszcze bogatsi, a biedni jeszcze bardziej ubożeją. Ta zasada dotyczy nie tylko kapitału, lecz także prestiżu, władzy itp.

że ludziom proponowało się zakup domów w miejscach zamieszkiwanych przez osoby takiej samej narodowości i o takim samym statusie materialnym[34].

Przykładem tego, że systemy *big data* mogą prowadzić do narastania strukturalnych nierówności, ma być wbudowana w nie asymetria pomiędzy tymi, którzy je wykorzystują, a tymi, których dotyczą gromadzone dane[35]. Według niektórych autorów ta różnica może doprowadzać do głębokich zmian w sferze władzy[36].

Łączenie danych z różnych baz pozwala uzyskać wiedzę o ludziach, którą ci woleliby ukryć[37]. Wątpliwości wywołuje również to, czy osoby udostępniające dane na swój temat w pełni rozumieją konsekwencje takiego kroku. Przykładowo, jednym z rezultatów działania systemów *big data* jest profilowanie ludzi[38]. Zasady przydzielania ich do poszczególnych kategorii mają dla nich poważne i często negatywne konsekwencje. Istniejące systemy prawne nie zawsze dostrzegają ten problem lub nie potrafią sobie z nim poradzić.

Kontrowersje dotyczą również tego, czy w systemy *big data* w sposób nieunikniony są wbudowywane uprzedzenia ich twórców[39]. Z jednej strony mamy do czynienia ze wskazanym wyżej podejściem, zgodnie z którym technologia ma być neutralna etycznie. Negatywne konsekwencje jej stosowania mają wynikać tylko ze sposobu jej wykorzystywania – w tym ujęciu to użytkownicy są odpowiedzialni za nieprawidłowości i problemy. Z drugiej strony pojawiają się tezy, że trudne – a czasami niemożliwe (ze względu na ochronę własności intelektualnej kodów źródłowych) – jest odkrycie uprzedzeń, które są wbudowane w systemy, o których mowa. Rodzi to daleko idące konsekwencje ze względu na rosnącą rolę oceny algorytmicznej różnych kwestii – np. wniosków ubezpieczeniowych, kredytowych, procesu rekrutacji do pracy lub podań o przyjęcie do służby. Zwraca się uwagę na to, że wyniki działania algorytmów

---

[34] T. Haber, *The Big Data Real Estate Controversy*, „The Huffington Post", 19 V 2014 r., https://www.huffingtonpost.com/toni-haber/the-big-data-real-estate-_b_5352573.html [dostęp: 15 VI 2020].

[35] M. Andrejevic, K. Gates, *Editorial. Big Data Surveillance: Introduction*, „Surveillance and Society" 2014, nr 12, s. 185–196.

[36] R. Mansell, *Power, Hierarchy and the Internet: Why the Internet Empowers and Disempowers*, „The Global Studies Journal" 2016, nr 2, s. 19–25; E. Ruppert, E. Isin, D. Bigo, *Data politics*, „Big Data & Society" 2017, z. 2, s. 1–7.

[37] Por. D. Lyon, *Surveillance, Snowden, and Big Data*…; Z. Tufekci, *Engineering the public: Big data, surveillance and computational politics*, „First Monday", 7 VII 2014 r., nr 7, http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097 [dostęp: 15 VI 2020].

[38] Zob. np. P.S. Gangadharan, *The Dangers of High-Tech Profiling, Using Big Data*, „The New York Times" z 7 sierpnia 2014 r., https://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/the-dangers-of-high-tech-profiling-using-big-data [dostęp: 15 VI 2020].

[39] Zob. M. Gurtowski, J. Waszewski, *Cyfrowy rasizm? Zautomatyzowane techniki nadzoru jako narzędzie segregacji i dyskryminacji*, „Transformacje" 2015, nr 1–2, s. 88–107.

kierujących *big data* można porównać do zachowania „rasistowskiego psa”[40], który ujada na ludzi innej rasy niż jego właściciel, co może być spowodowane uprzedzeniami (być może nawet nieuświadomionymi) tegoż właściciela.

Systemy *big data* mają coraz większy wpływ na działanie rynków (w tym na podejmowanie decyzji o inwestowaniu[41], na ocenę ryzyka[42] i przewidywanie kryzysów finansowych[43]). Jednocześnie podkreśla się neutralność technologii w ogóle i w szczególności systemów *big data*, a także szanse wynikające z ich wykorzystywania. Spór dotyczy pomijania przez apologetów takich systemów tego, że ich nieprawidłowe działanie może mieć konsekwencje dla stabilności systemu gospodarczego[44].

Systemy korzystające z *big data* zmieniają wymiar sprawiedliwości. Coraz częściej jest oceniany potencjał łamania prawa przez konkretnych ludzi, a nie ich czyny. Inaczej: ocenia się nie przeszłe działania i świadome decyzje leżące u ich podstaw, tylko raczej samo prawdopodobieństwo popełnienia czynu zabronionego[45]. Źródłem kontrowersji jest tu problem, czy władze publiczne mają prawo do podejmowania działań wobec osób, które zostały wskazane przez algorytmy jako tylko potencjalni przestępcy.

Jak pokazały zdarzenia z ostatniej dekady, media społecznościowe niewystarczająco dbają o prywatność swoich użytkowników[46]. W związku z tym troskę powinno budzić to, że systemy *big data* korzystają z danych tych mediów. Za pomocą takich systemów media społecznościowe umożliwiają poznawanie najistotniejszych

---

[40] J. Weisberg, *The Digital Poorhouse*, „The New York Review of Books”, 7 VI 2018 r., https://www.nybooks.com/articles/2018/06/07/algorithms-digital-poorhouse [dostęp: 15 VI 2020].

[41] C. Curme i in., *Quantifying the semantics of search behavior before stock market moves*, „Proceedings of the National Academy of Sciences”, 28 VII 2014 r., https://doi.org/10.1073/pnas.1324054111 [dostęp: 15 VI 2020]; M. Kolanovic, R. Krishnamachari, *Big Data and AI Strategies: Machine Learning and Alternative Data Approach to Investing*, JP Morgan, V 2017 r., https://www.cfasociety.org/cleveland/Lists/Events%20Calendar/Attachments/1045/BIG-Data_AI-JPMmay2017.pdf [dostęp: 15 VI 2020].

[42] F. Corea, *Big Data and Risk Management in Financial Markets: A Survey*, Note technique NT 16-01, Montreal Institute of Structured Finance and Derivatives, 2016, http://cdi-icd.org/wp-content/uploads/2018/03/NT-16-01_Corea_CDI.pdf [dostęp: 15 VI 2020].

[43] Zob. np. J. Rodrigues, A. Speciale, *How Central Banks Are Using Big Data to Help Shape Policy*, 18 XII 2017 r., https://www.bloomberg.com/news/articles/2017-12-18/central-banks-are-turning-to-big-data-to-help-them-craft-policy [dostęp: 15 VI 2020].

[44] Por. Y.N. Harari, *Homo deus. Krótka historia jutra*, Warszawa 2018, s. 395–396.

[45] Zob. np. D. Kehl, P. Guo, S. Kessler, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing*, 2017, Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School, https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf [dostęp: 15 VI 2020]; S. Corbett-Davies, S. Goel, S. González-Bailón, *Even Imperfect Algorithms Can Improve the Criminal Justice System*, 20 XII 2017 r., https://www.nytimes.com/2017/12/20/upshot/algorithms-bail-criminal-justice-system.html [dostęp: 15 VI 2020].

[46] W. Orliński, *Facebook niczym obora*, „Blog Wojciecha Orlińskiego”, 4 XI 2010 r., http://wo.blox.pl/2010/11/Facebook-niczym-obora.html [dostęp: 15 VI 2020].

lęków społecznych oraz ich wykorzystywanie np. w kampaniach politycznych. W tym kontekście było odczytywane wykorzystanie Facebooka w trakcie prezydenckiej kampanii wyborczej w USA oraz kampanii referendalnej w Wielkiej Brytanii w sprawie brexitu. Wątpliwości są związane z pytaniem, czy to właśnie systemy *big data* odpowiadają np. za skuteczność populistycznych polityków lub zwiększanie polaryzacji społeczeństw[47].

Nie ma zgody co do tego, kto powinien być właścicielem danych zgromadzonych w ramach systemów *big data* (w tym danych osobowych) oraz jak powinny być dzielone prawa własności z nimi związane[48]. Szczególne zastrzeżenia wywołuje problem własności danych gromadzonych przez urządzenia, które są włączone do Internetu rzeczy[49].

Należy zauważyć, że podstawą modelu biznesowego mediów społecznościowych jest przede wszystkim zbieranie danych na temat ich użytkowników i wykorzystywanie tych danych do takiego pokazywania im reklam, które będzie wartościowe dla reklamodawców[50]. Współcześnie nie sposób prowadzić takiej działalności bez systemów *big data*.

Podstawowe wątpliwości związane już bezpośrednio z mediami społecznościowymi dotyczą tego, czy powinny one brać na siebie odpowiedzialność (jak media klasyczne) za to, co komunikują (publikują) ich użytkownicy[51]. Żeby uniknąć nadzorowania czy raczej cenzurowania aktywności swoich użytkowników, media społecznościowe przedstawiają się jako wyłącznie „platformy", które umożliwiają nawiązywanie ludziom kontaktów między sobą i które nie powinny odpowiadać za publikowane

---

[47] Tę kwestię jako kontrowersyjną przedstawiały głównie media. Brytyjska gazeta „The Guardian" podała, że z jej perspektywy *big data* jest zagrożeniem, bo może sprawić, że będziemy funkcjonować w mniej demokratycznym społeczeństwie. Zob. *The Guardian view on big data: the danger is less democracy*, 26 II 2017 r., https://www.theguardian.com/commentisfree/2017/feb/26/the-guardian-view-on-big-data-the-danger-is-less-democracy [dostęp: 15 VI 2020].

[48] Zob. np. B. Darrow, *The Question of Who Owns the Data Is About to Get a Lot Trickier*, 6 IV 2016 r., http://fortune.com/2016/04/06/who-owns-the-data/ [dostęp: 15 VI 2020]; C.S. Mullins, *Who Owns the Data?*, „Database Trends and Applications", 1 VI 2018 r., http://www.dbta.com/Columns/DBA-Corner/Who-Owns-the-Data-125485.aspx [dostęp: 15 VI 2020]; M. Nielsen, *Who Owns Big Data?*, 2014, https://www.bbvaopenmind.com/wp-content/uploads/2014/03/BBVA-OpenMind-Who-Owns-Big-Data-Michael-Nielsen.pdf.pdf [dostęp: 15 VI 2020].

[49] C. Donato, *The #BigData Revolution: Who Owns Our Information?*, 11 IV 2016 r., https://www.forbes.com/sites/sap/2016/04/11/the-bigdata-revolution-who-owns-our-data/#2f2739bb68dd [dostęp: 15 VI 2020].

[50] Zob. np. L. Sherman, *Why Facebook Will Never Change Its Business Model*, forbes.com, 16 IV 2018 r., https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model [dostęp: 15 VI 2020].

[51] O tej kwestii w kontekście Facebooka pisał magazyn „Wired" zajmujący się nowymi technologiami. Zob. E. Griffith, *Memo to Facebook: How To Tell If You're a Media Company*, 12 X 2017 r., https://www.wired.com/story/memo-to-facebook-how-to-tell-if-youre-a-media-company/ [dostęp: 15 VI 2020].

na nich treści[52]. Przeciwnicy takiego podejścia wskazują, że mediaspołecznościowe powinny podlegać takim samym regułom jak media tradycyjne i ponosić odpowiedzialność za działania osób publikujących na ich łamach[53].

Wynikiem walki z niepożądanymi zachowaniami użytkowników są zarzuty wobec mediów społecznościowych o ograniczanie wolności słowa i stosowanie cenzury[54]. Wątpliwości budzi to, czy prywatna firma powinna podejmować decyzje, o czym wolno mówić i jakie dane można rozsyłać. Równolegle toczy się debata o tym, czy globalne media społecznościowe powinny cenzurować treści zgodnie z żądaniami władz danego państwa[55]. Poważne problemy dla Facebooka wywołały zarzuty, że firma zrobiła za mało, żeby uniemożliwić wykorzystywanie jej mediów społecznościowych (Facebooka oraz Instagramu) i komunikatorów internetowych (WhatsAppa i Facebooka Messengera) do szerzenia przemocy na tle etnicznym, np. w Mjanmie[56].

Jako źródło sporów bywa przedstawiane blokowanie mediów społecznościowych przez państwa, gdy tego typu media są uznawane za narzędzia zbierania informacji wywiadowczych i wywierania wpływu przez inne państwa. Z tych przyczyn była ograniczana działalność chińskich (w Australii[57]) i rosyjskich (na Ukrainie) mediów społecznościowych[58]. Przeciwnicy tego typu blokad utożsamiają je z działaniami państw niedemokratycznych i przedstawiają je jako przykład cenzury[59]. Kontrowersje

---

[52] Podkreślał to w przesłuchaniu przed amerykańskim Kongresem w kwietniu 2018 r. Mark Zuckerberg – założyciel i właściciel pakietu kontrolnego Facebooka. Zob. np. M. Castillo, *Zuckerberg tells Congress Facebook is not a media company: „I consider us to be a technology company"*, 11 IV 2018 r., https://www.cnbc.com/2018/04/11/mark-zuckerberg-facebook-is-a-technology-company-not-media-company.html [dostęp: 15 VI 2020].

[53] Zob. np. J. Kiss, C. Arthur, *Publishers or platforms? Media giants may be forced to choose*, „The Guardian", 29 VII 2013 r., https://www.theguardian.com/technology/2013/jul/29/twitter-urged-responsible-online-abuse [dostęp: 15 VI 2020].

[54] Zob. np. L. Bershidsky, *No, Big Data Didn't Win the U.S. Election*, 8 XII 2016 r., https://www.bloomberg.com/view/articles/2016-12-08/no-big-data-didn-t-win-the-u-s-election [dostęp: 15 VI 2020].

[55] Istotną rolę odegrał spór wokół niemieckiej ustawy NetzDG, skierowanej przeciwko mowie nienawiści. Zob. np. M. Scott, J. Delcker, *Free speech vs. censorship in Germany*, „politico.eu", 4 I 2018 r., https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech/ [dostęp: 15 VI 2020].

[56] S. Stecklow, *Why Facebook is losing the war on hate speech in Myanmar*, 15 VIII 2018 r., https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/ [dostęp: 15 VI 2020].

[57] Zob. np. C. Cheng, I. Deng, *WeChat joins list of Chinese technology banned by overseas militaries on security worries*, „South China Morning Post", 15 III 2018 r., https://www.scmp.com/tech/china-tech/article/2137232/wechat-joins-list-chinese-technology-banned-overseas-militaries [dostęp: 15 VI 2020].

[58] A. Luhn, *Ukraine blocks popular social networks as part of sanctions on Russia*, 16 V 2017 r., https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war [dostęp: 15 VI 2020].

[59] Międzynarodowa organizacja Freedom House, która bada m.in. wolność w Internecie, zablokowanie rosyjskich mediów społecznościowych nazwała wprost cenzurą. Zob. *Freedom on the Net.*

budzi w tym wypadku miejsce, w którym powinna zostać wyznaczona granica decydująca o tym, kiedy jest uzasadniona obrona interesów narodowych.

Kontrowersje wywołuje także uzależnianie się od mediów społecznościowych. Byli pracownicy Facebooka wskazują, że zdają sobie sprawę z takiego zjawiska[60]. W wersji słabej do zachowań powierzchownie przypominających uzależnienia w sposób niezamierzony doprowadza model biznesowy mediów społecznościowych, który wiąże się z zachęcaniem ludzi do spędzania jak najdłuższego czasu na danym portalu. W wersji mocnej jest mowa o świadomych pracach nad wykorzystaniem mechanizmów uzależniających. Tworzenie mediów społecznościowych w tym ujęciu jest odpowiednikiem budowania kasyn i konnych torów wyścigowych. Należy dodać, że na możliwość uzależniania ma wpływ wiedza o sposobie działania mózgów użytkowników oraz przetwarzanie pozyskiwanych informacji za pomocą systemów *big data*.

Spory wokół informacji zbieranych przez media społecznościowe koncentrują się zazwyczaj wokół prywatności użytkowników. Chodzi o to, czy ludzie w pełni zdają sobie sprawę z poważnych konsekwencji, jakie może mieć dzielenie się danymi na swój temat z prywatnymi firmami. Przykładowo, historia Facebooka wiąże się ze skandalami, które polegały na tym, że spółka naruszała prywatność swoich użytkowników[61].

Oficjalnie media społecznościowe wykorzystują swoją wiedzę o użytkownikach oraz ich wzajemnych relacjach do tworzenia dla ludzi miejsca, w którym czują się dobrze i do którego chcą powracać[62]. Dzięki temu mogą – tak przynajmniej deklarują – pokazywać im reklamy dopasowane do ich potrzeb i zarabiać na ich sprzedaży. Zaniepokojenie budzi to, że głęboka wiedza o użytkownikach może jednak zostać wykorzystana również do innych celów, niezgodnych z interesami tych osób[63].

Ukraine 2017, https://freedomhouse.org/sites/default/files/FOTN%202017_Ukraine.pdf [dostęp: 15 VI 2020].

[60] J.C. Wong, *Former Facebook executive: social media is ripping society apart*, „The Guardian", 12 XII 2017 r., https://www.theguardian.com/technology/2017/dec/11/facebook-former-executive-ripping-society-apart [dostęp: 15 VI 2020]; T. Harris, *How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist*, „Thrive Global", 18 V 2016 r., https://journal.thriveglobal.com/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 [dostęp: 15 VI 2020]; tenże, *Our Minds Have Been Hijacked by Our Phones*, rozmawiał Nicholas Thompson, 26 VII 2017 r., https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/ [dostęp: 15 VI 2020].

[61] Zob. np. N. Lomas, *A brief history of Facebook's privacy hostility ahead of Zuckerberg's testimony*, 10 IV 2018 r., https://techcrunch.com/2018/04/10/a-brief-history-of-facebooks-privacy-hostility-ahead-of-zuckerbergs-testimony/ [dostęp: 15 VI 2020].

[62] Facebook, opisując swoją misję, wyjaśnił, że chce „(…) dać ludziom możliwość zbudowania wspólnoty i sprawić, że część świata się bardziej zbliży do siebie. Ludzie używają Facebooka, żeby utrzymywać kontakt z przyjaciółmi i rodziną, żeby odkrywać, co się dzieje na świecie i żeby wyrażać rzeczy ważne i dzielić się nimi z innymi". Zob. https://investor.fb.com/resources/default.aspx [dostęp: 15 VI 2020].

[63] Unaoczniła to sprawa Cambridge Analytica i wykorzystanie danych zgromadzonych przez Facebook do mikrotargetingu politycznego.

Media społecznościowe posługują się zebranymi przez siebie danymi w celu prowadzenia badań naukowych. Wątpliwości budzi ich niejednoznaczny status etyczny. Cechą tego typu mediów jest to, że wcześniej tak bogate, spontanicznie powstające dane nie były dostępne dla uczonych[64]. Wiadomo, że badania eksperymentalne prowadził sam Facebook. Wśród eksperymentów znalazły się nie tylko te weryfikujące, jaki układ strony lub jakie jej kolory i dźwięki zachęcają do dłuższej obecności na tej stronie (testy AB[65]), lecz także próby wpływania na emocje użytkowników oraz sprawdzanie, czy rodzaj informacji pokazywanych użytkownikom w trakcie głosowania może zmienić frekwencję wyborczą[66].

Facebook udostępniał dane o swoich użytkownikach badaczom. Nie kontrolował jednak, jak je wykorzystywano. Działalność Cambridge Analytica i próby zastosowania mikrotargetingu politycznego prowadzone m.in. przez tę spółkę ujawniły, że dane gromadzone przez media społecznościowe i za ich pomocą mogą powodować duże zagrożenia[67].

Potencjalne kontrowersje są związane z możliwością przechwytywania i wykorzystywania danych zgromadzonych przez media społecznościowe, które już upadły (np. polskie grono.net) lub straciły początkową popularność (np. nasza-klasa.pl). Istnieje wiele możliwych sposobów wykorzystania takich danych. Mamy do czynienia z sytuacją, w której od ponad 20 lat powstają podmioty internetowe zbierające dane – często zasadnicze z punktu widzenia prywatności – na temat ludzi. Te dane, o których powstaniu użytkownik mógł zapomnieć, mogą posłużyć do szantażu, modelowania typów zachowań wrażliwych, ekstremistycznych, stymulowania mód, wzniecania niepokojów społecznych albo namierzania potencjalnych liderów buntów społecznych lub tylko aktywistów. W wypadku takich danych zarówno RODO, jak i działalność takich instytucji, jak Prezes Urzędu Ochrony Danych Osobowych, nie są panaceum.

---

[64] O. Rodak, *Twitter jako przedmiot badań socjologicznych i źródło danych społecznych. Perspektywa konstruktywistyczna*, „Studia Socjologiczne" 2017, nr 3, s. 209–236.

[65] Ich przykładem jest testowanie, która nazwa linku wywoła większe zainteresowanie użytkowników danej strony. Nazwa odnośnika może być modyfikowana do momentu, aż zostanie zmaksymalizowana jego współczynnika klikalności. Podobnie można badać układ strony internetowej, wykorzystane na niej kolory, czcionki itd.

[66] A.D.I. Kramer, J.E. Guillory, J.T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks*, „Proceedings of the National Academy of Sciences" 2014, nr 24, s. 8788–8790. Wykaz tekstów na temat tego badania i reakcji na nie opisał J. Grimmelman, 30 VI 2014 r., http://laboratorium.net/archive/2014/06/30/the_facebook_emotional_manipulation_study_source [dostęp: 15 VI 2020].

[67] Zob. np. Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns. Investigation update*, raport brytyjskiej instytucji chroniącej dane osobowe, 11 VII 2018 r., https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf [dostęp: 15 VI 2020].

Neuronauka to zbiorcza nazwa dla dyscyplin naukowych zajmujących się badaniem ludzkiego mózgu (umysłu). Wokół tych dyscyplin rodzi się wiele kontrowersji, ponieważ tego typu badania dotyczą istotnych wymiarów człowieczeństwa.

Wątpliwości budzi podejście znacznej części neuronaukowców do analizowania i prezentowania danych[68]. Część badaczy pomija to, że algorytmy komputerowe są niezbędne do interpretowania danych gromadzonych za pomocą różnych technik badawczych, które w dalszej części artykułu będą zbiorczo nazywane neurotechnikami[69]. Błędy w tych algorytmach przekładają się na nieprawidłowe interpretacje – często następnie rozpowszechniane przez media[70]. Przykładem takiej pomyłki jest traktowanie interpretacji (np. kolorystycznego odzwierciedlenia aktywności mózgu) jako realnego wyrazu reakcji układu nerwowego na bodźce. To odpowiedni algorytm może decydować, że wyniki badań neuronaukowych zostaną uznane za istotne, że zyskają rozgłos i przynajmniej potencjalny wpływ na procesy społeczne. Innymi słowy, wątpliwości budzi przypisywanie zbyt dużej wagi ustaleniom dokonywanym w wyniku stosowania mało precyzyjnych technik neuronauki.

Spory wywołują także pytania, czy i na jakich polach jest dopuszczalne korzystanie z odkryć i technik neuronauki. Ta nauka obiecuje bowiem odkrycie tajemnic umysłu (mózgu). Stąd blisko do obietnicy rozwiązywania różnych problemów dzięki modyfikowaniu pracy mózgu za pomocą precyzyjnie działających leków, technik magnetycznego lub elektrycznego oddziaływania przezczaszkowego czy implantów wszczepianych w mózg[71]. Wątpliwości co do dopuszczalności wykorzystywania ustaleń neuronauki są związane z szerszą dyskusją na temat neurowspomagania, czyli udoskonalania mózgu człowieka[72]. Jednym z wymiarów tej dyskusji jest spór o ideologię

---

[68] A. Raz, *From Neuroimaging to Tea Cup Leaves in the Bottom of a Cup*, w: *Critical Neuroscience. A Handbook of the Social and Cultural Contexts of Neuroscience*, S. Choudhury, J. Slaby (red.), Chichester 2012, s. 265–272.

[69] W znanym przykładzie z 2009 r. okazało się, że algorytmy odkryły aktywność mózgu zdechłej ryby. Zob. C.M. Bennett i in., *Neural correlates of interspecies perspective taking in the post-mortem Atlantic Salmon: An argument for multiple comparisons correction*, poster przedstawiony na konferencji „Human Brain Mapping" w 2009 r.

[70] Przykładem są badania poświęcone „politycznemu mózgowi" i różnicom pomiędzy mózgami osób o poglądach prawicowych i lewicowych. Zob. np. D. Gellene, *Study finds left-wing brain, right-wing brain*, „Los Angeles Times", 10 IX 2007 r., http://www.latimes.com/local/obituaries/la-sci-politics10sep10-story.html [dostęp: 15 VI 2020].

[71] V.P. Clark, *The ethical, moral, and pragmatic rationale for brain augmentation*, „Frontiers in Systems Neuroscience" 2014, nr 8, s. 1–4.

[72] Zob. np. M.J. Farah, *Neuroethics: The Ethical, Legal, and Societal Impact of Neuroscience*, „Annual Review of Psychology" 2012, nr 63, s. 571–591.

transhumanistyczną[73] oraz o związany z nią postulat wolności morfologicznej[74]. Zgodnie z tym ostatnim człowiek ma mieć prawo do modyfikowania swojego własnego ciała oraz umysłu i to od jego decyzji zależy, jak daleko idące będą te zmiany[75]. Badania nad mózgiem mogą doprowadzić do zdobywania przewagi poznawczej tylko przez ludzi, którzy posiadają odpowiednie zasoby i możliwości, czyli mogą przyczynić się do powstania nowego typu kastowości społecznej[76]. Przykładem są tu wątpliwości związane z wyczynowym uprawianiem sportu[77], tzn. czy dopuszczalne jest na przykład podnoszenie koncentracji w strzelectwie lub zmniejszenie znużenia powtarzalnym treningiem za pomocą specjalnych urządzeń. Urządzenia przeznaczone do realizacji takich celów przez stymulację mózgu już są wprowadzane na rynek[78].

Źródłem sporów są problemy etyczne związane ze stosowaniem przymusu wobec ludzi – również przez stawianie ich w sytuacjach, w których alternatywą dla poddania się badaniom za pomocą technik neuronauki jest zwolnienie z pracy lub konieczność zmiany stanowiska. Przykładem może być przyznanie dostępu do informacji niejawnych tylko na podstawie badania mózgu. Celem jest odkrycie, czy dany mózg kryje w sobie potencjalne zagrożenia[79].

W przyszłości kontrowersje wywoła prawdopodobnie konieczność rozstrzygnięcia, czy nadzór nad koncentracją np. maszynisty kolei wielkich prędkości w trakcie prowadzenia przez niego lokomotywy jest ważniejszy od jego prywatności. Techniki skanowania mózgów maszynistów są już wprowadzane w Chinach. Mniej wiadomo o podobnych projektach, które są wprowadzane konkretnie w siłach zbrojnych tego kraju[80]. W społeczeństwach demokratycznych konieczne będzie przedyskutowanie, a następnie określenie, czy nadzór nad skupieniem na pracy innych typów pracowników – i w których zawodach – jest istotniejszy od ich prywatności.

---

[73] Rozumianą jako przekonanie, że ulepszanie człowieka jest pożądane i możliwe. Najważniejszą rolę mają odgrywać technologie, które powstrzymają starzenie się oraz usprawnią fizyczne i poznawcze możliwości ludzi. Zob. np. *The Transhumanist FAQ, v. 3.0.*, World Transhumanist Association, https://humanityplus.org/philosophy/transhumanist-faq/ [dostęp: 15 VI 2020].

[74] Tamże. Por. K. Krzysztofek, *Kierunki ewaluacji technologii cyfrowych*…, s. 203.

[75] C. Coenen, *Transhumanism in Emerging Technoscience as a Challenge for The Humanities and Technology Assessment*, „Teorija in Praksa" 2014, nr 51, s. 754–771.

[76] Zob. Y.N. Harari, *Homo deus*…

[77] D. McMahon, *America's top cyclist entering the Tour de France has been using a portable brain stimulator...* (przypis do tekstu na temat nowych technologii, pochodzącego z portalu internetowego; brak wersji papierowej).

[78] Tamże.

[79] F.H. Sahito, W. Slany, *Functional Magnetic Resonance Imaging and the Challenge of Balancing Human Security with State Security*, „Human Security Perspectives" 2012, nr 9, s. 38–66.

[80] S. Chen, *„Forget the Facebook leak": China is mining data directly from workers' brains*… (źródłem jest tekst z portalu chińskiej (HK) gazety; brak dostępu do jej wersji papierowej).

Część neuronaukowców twierdzi, że dzięki rozwojowi technik badawczych neuronauki będzie w stanie odkrywać kłamstwo[81]. Szczególnie problematyczne jednak jest tu osiągnięcie pewności. To wywołuje spory pomiędzy przeciwnikami a zwolennikami wykorzystywania technik neuronauki do ustalania prawdy, np. w postępowaniach karnych. Po pierwsze, istnieją problemy z udowodnieniem, że systemy wykrywania kłamstw korzystające z neurotechnik rzeczywiście działają skutecznie[82]. Po drugie, jest to potencjalne źródło wątpliwości – skutecznie działający, powszechnie lub choćby tylko łatwo dostępny system wykrywania kłamstw zmieniłby zasady, którymi rządzi się społeczeństwo[83].

Neuronauka zyskuje wpływ na podejmowanie decyzji o sposobie karania przestępców i o ich resocjalizacji. Równocześnie jednak przeciwnicy wykorzystywania tego zbioru dyscyplin w tym celu porównują je do fizjonomiki, frenologii i antropometrii Cesare Lombroso[84]. Reakcja na masowe zastosowanie niektórych ustaleń neuronauki w postępowaniach karnych byłaby prawdopodobnie podobna do tej, jaką wywołały badania Yilun Wanga i Michała Kosińskiego nad wykorzystaniem systemów *big data* działających dzięki sztucznej inteligencji do rozpoznawania orientacji seksualnej osób na podstawie ich zdjęć[85].

Spory wokół neuronauki dotyczą sposobu jej uprawiania (w tym zasad etycznych), popularyzacji wyników badań nad mózgiem oraz ich wykorzystywania. Jak można zauważyć, znaczna część wątpliwości wskazanych powyżej dotyczy zastosowania ustaleń neuronauki w ramach sprawowania kontroli społecznej. Konsekwencje badań nad mózgiem są dla podtrzymywania porządku społecznego obecnie najwyżej potencjalne. Niezwykle rzadkie są analizy, które bezpośrednio wskazują, że tego typu

---

[81] G. Ganis, J.P. Keenan, *The cognitive neuroscience of deception*, „Social Neuroscience" 2009, nr 6, s. 465–472.

[82] D.D. Langleben, J.C. Moriarty, *Using Brain Imaging for Lie Detection: Where Science, Law and Policy Collide*, „Psychology, Public Policy, and Law" 2013, nr 2, s. 222–234.

[83] Kłamstwo jest uważane za ważny czynnik rozwoju gatunku *Homo sapiens* i jest wpisane w jego naturę (zob. T. Witkowski, *Inteligencja makiaweliczna. Rzecz o pochodzeniu natury ludzkiej*, Taszów 2005). Zmniejszenie roli kłamstwa w relacjach interpersonalnych wywołałoby trudne do przewidzenia konsekwencje. Osoby, którym postawiono zarzuty karne, mogą milczeć, a nawet kłamać w trakcie przesłuchań. Ograniczenie tych praw zmieniłoby podstawowe zasady, którymi rządzi się system sprawiedliwości (niedozwolone zmuszanie do samooskarżenia).

[84] Zob. np. A. Dobrin, *Is Neuroscience Today's Phrenology?*, 22 VIII 2016 r., https://www.psychologytoday.com/us/blog/am-i-right/201608/is-neuroscience-todays-phrenology [dostęp: 15 VI 2020]. Por. O. Parker Jones, F. Alfaro-Almagro, S. Jbabdi, *An empirical, 21st century evaluation of phrenology*, „Cortex" 2018, t. 106, wrzesień (zapis specyficzny – wydawanych jest 12 tomów rocznie; zamiast numerów są podawane nazwy miesięcy – przyp. red.), s. 26–35.

[85] Projekt artykułu na temat badania ukazał się w lutym 2017 r.: Y. Wang, M. Kosiński, *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*; ostatnia aktualizacja tego roboczego artykułu pochodzi z 26 V 2020 r., https://osf.io/zn79k/ [dostęp: 15 VI 2020]. O badaniu pisał m.in. „The New York Times" – H. Murphy, *Why Stanford Researchers Tried to Create a 'Gaydar' Machine*, „The New York Times", 9 X 2017 r., https://www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html [dostęp: 15 VI 2020].

badania i stosowane w ich trakcie narzędzia mogą być wykorzystywane w takim celu. Mimo to warto jednak rozważyć, jak wielki wpływ na sferę prywatności mają badania naukowe, w wyniku których można odkryć to, czego ludzie nie tylko nie chcą ujawnić, lecz także czego mogą sami o sobie nie wiedzieć.

Już samo wskazanie tylko wybranych typów nowych technik kontroli społecznej oraz trzech pól sporów pozwala na ujawnienie konsekwencji zjawisk analizowanych w artykule. Łącznie powodują one, że prywatność zanika.

„Nie ukryjesz się"

Powyższe zagadnienia wskazują m.in. na to, że coraz trudniej jest się ukrywać przed nowymi technikami kontroli społecznej. Spójrzmy na kilka przykładów, które pokazują, jak bardzo staliśmy się przejrzyści dla systemów nadzoru.

Zachowanie prywatności jest utrudnione m.in. dlatego, że obojętnie, jakie przebranie się wybierze, coraz łatwiej jest zidentyfikować ludzi na nagraniach np. kamer telewizji przemysłowej. Nie muszą one rejestrować twarzy człowieka, żeby go rozpoznać. Systemy analizujące obrazy z kamer oceniają nie tylko standardowe cechy biometryczne (rozmiary części ciała), lecz także sposób przemieszczania się[86]. Media społecznościowe również rozwijają systemy zautomatyzowanej analizy zdjęć i filmów[87]. Robią to, żeby na podstawie publikowanych w nich fotografii wskazywać ludziom prawdopodobnych znajomych.

Ludzie coraz częściej stale noszą przy sobie telefony (lub smartfony). Ciągłe korzystanie z telefonu pozwala na wykorzystanie danych i metadanych[88] na temat jego użytkownika do zrekonstruowania jego sposobu życia, nawyków, relacji społecznych i przekonań za pomocą systemów *big data*. Przykładowo, za pomocą analizy danych z czujników smartfonów, które analizują sposób przemieszczania się użytkownika, można określić jego płeć[89] lub wiek[90].

Coraz trudniej jest się ukryć, ponieważ na urządzeniach elektronicznych codziennego użytku są instalowane programy mające na celu rozpoznanie użytkowników

---

[86] S. Mohapatra i in., *Real time biometric surveillance with gait recognition*, „AIP Conference Proceedings" 2018, nr 1.

[87] J. Frankle, *How Russia's New Facial Recognition App Could End Anonymity*, 23 V 2016 r., https://www.theatlantic.com/technology/archive/2016/05/find-face/483962/ [dostęp: 15 VI 2020]; N. Singer, *Facebook's Push for Facial Recognition Prompts Privacy Alarms*, „The New York Times", 9 VII 2018 r., https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html [dostęp: 15 VI 2020].

[88] Czyli, w największym skrócie i dużym uproszczeniu, danych dotyczących danych.

[89] A. Jain, V. Kanhangad, *Gender classification in smartphones using gait information*, „Expert Systems with Applications" 2018, nr 93, s. 257–266.

[90] N. Mansouri, M. Aouled Issa, Y. Ben Jemaa, *Gait features fusion for efficient automatic age classification*, „IET Computer Vision" 2018, nr 1, s. 69–75.

określonych urządzeń oraz skłonienie ich do określonych działań. Przykładem są „inteligentne opaski" dla ćwiczących fizycznie i aplikacje na smartfony, wykorzystywane do zarządzania czasem poświęconym na aktywność fizyczną (np. określające liczbę kroków wykonanych dziennie). Aplikacje (urządzenia), na których są zainstalowane, zbierają również inne dane na temat użytkowników i dążą do tego, aby zachęcić ich do udostępniania jak największej ilości informacji na swój temat. Powstają swoiste sieci społecznościowe, w których ludzie dzielą się wiadomościami na temat aktywności fizycznej[91].

Na prywatność będzie miało wpływ prawdopodobnie również to, że niezwykle szybko jest obecnie rozwijany Internet rzeczy (coraz częściej nazywany również Internetem wszystkiego)[92]. Ludzie są zachęcani do korzystania np. z tzw. inteligentnych domów, inteligentnych samochodów, inteligentnych ubrań. Prowadzi to do tworzenia danych na temat różnych aspektów ich życia. Dużą część doby mogą oni przecież spędzać w sytuacjach, w których zbieranie danych na ich temat jest niezbędne do prawidłowego działania „inteligentnych" systemów. Przykładowo, odkurzacz robot musi dokładnie poznać mieszkanie i styl życia jego mieszkańców, żeby móc realizować swoje zadania polegające na mało kłopotliwym lub nawet niezauważalnym dla domowników utrzymaniu czystości podłogi[93]. Stosowanie uniwersalnych algorytmów sprzątających rozwiązuje tylko część problemów.

Na zmniejszanie się sfery prywatności wpływa również to, że tworzenie cyfrowych bliźniaków – rekonstrukcji ludzi na podstawie danych zawartych na ich temat w cyfrowych bazach danych – jest biznesowo opłacalne. Umożliwia to bowiem bardziej precyzyjne docieranie do potencjalnych nabywców określonych towarów i usług. To z kolei przekłada się na większe zyski ze sprzedawanych reklam. Z tego między innymi wynikają sukcesy Google'a i Facebooka – spółek dominujących na rynku reklamy internetowej[94]. Te same techniki nadzoru, polegające na łączeniu baz danych przy wykorzystaniu systemów *big data*, są też wydatnym wsparciem dla systemów, które wspomagają sprawowanie kontroli społecznej.

Brak możliwości zachowania prywatności wiąże się także z tym, że zagrożenia bezpieczeństwa stają się uzasadnieniem dla zmniejszania sfery prywatności i wprowadzania w życie nowych technik kontroli społecznej. Obecnie, w czasach terroryzmu i niepewności, powyższe twierdzenie nabiera szczególnego znaczenia i dotyczy to nie tylko państw autorytarnych i totalitarnych, w których sfera bezpieczeństwa obejmuje również m.in. utrzymanie władzy przez rządzących.

---

[91] A. Pressman, *Fitbit Adds Social Feed to Keep Users Motivated*, „Fortune.com", 5 I 2017 r., http://fortune.com/2017/01/05/fitbit-social-feed-motivated/ [dostęp: 15 VI 2020].

[92] Przegląd i typologia badań na temat tego zjawiska zob. M. Alaa i in., *A review of smart home applications*…

[93] J. Wolfe, *Roomba vacuum maker iRobot betting big on the 'smart' home*, 24 VII 2017 r., https://www.reuters.com/article/us-irobot-strategy/roomba-vacuum-maker-irobot-betting-big-on-the-smart-home-idUSKBN1A91A5 [dostęp: 15 VI 2020].

[94] Zob. np. J. Koetsier, *Digital Duopoly Declining*… (przypis do artykułu internetowego).

Ukrywanie się przed nowymi technikami kontroli społecznej jest coraz trudniejsze, gdyż zgodnie z obecnymi trendami każda osoba, która usiłuje się skryć przed nadzorem, może być traktowana jako ktoś podejrzany. Bardziej lub mniej otwarcie zaczyna dominować interpretacja, że próbują się ukrywać tylko ci, którzy mają coś do ukrycia[95]. Jednocześnie powstają techniki zwiększania własnej prywatności, zastępujące formy komunikacji łatwe do nadzorowania. Przykładowo, szyfrowane komunikatory zastępują wysyłanie SMS-ów, a korzystanie z sieci TOR i prywatnych sieci wirtualnych utrudnia wykrywanie, skąd ktoś łączy się z siecią oraz namierzenie tej osoby[96]. Z kolei odpowiedzią na techniki zwiększania prywatności jest rozwój technik łamiących te zabezpieczenia. Trwa swoisty wyścig zbrojeń, który w państwach autorytarnych staje się często sprawą życia i śmierci.

Wyzwania na przyszłość

Zanikanie możliwości ukrywania swoich działań, poglądów, a ostatecznie nawet myśli, jest zjawiskiem cywilizacyjnie fundamentalnym. Jest też wielkim wyzwaniem, które powinniśmy rozumieć nie tylko jako niezwykłą szansę, lecz także jako potencjalne zagrożenie.

Sprawowanie kontroli społecznej i związana z nim ewolucja systemów nadzoru są w coraz większym stopniu wspomagane przez systemy komputerowe działające w sposób zautomatyzowany. Najważniejsze wydają się tu systemy przetwarzania danych cyfrowych, których ilość rośnie wraz ze wzrostem ich wartości biznesowej.

Swoistym paliwem dla systemów *big data* są między innymi media społecznościowe. Ich model biznesowy łączy się z jak najdokładniejszym poznawaniem użytkowników. Im lepiej są oni zrozumiani (w sensie socjologicznym i co gorsza – psychologicznym), im więcej danych na ich temat da się zgromadzić, tym łatwiej pokazywać im reklamy przynoszące zyski. Efektem ubocznym jest możliwość przechwytywania danych gromadzonych przez media społecznościowe przez inne podmioty. W wyniku takich przejęć różne podmioty, w tym służby wywiadowcze i policyjne, zdobywają wiedzę o jednostkach, a dzięki systemom *big data* – również o wybranych zbiorowościach, a nawet o całości populacji.

Media społecznościowe obecnie stały się jednym z istotniejszych źródeł informacji wykorzystywanych przez nowe techniki kontroli społecznej, które posiłkują się systemami *big data*. W opracowaniach naukowych i analizach publikowanych przez media pojawiają się informacje, które wskazują, że warto poszukiwać również punktów wspólnych dla mediów społecznościowych i badań nad mózgiem. Obecnie trwają

[95] O tym problemie pisał m.in. D.J. Solove, *Nothing to Hide. The False Tradeoff*…

[96] Te i inne techniki dogłębnie są opisane na stronie internetowej międzynarodowej organizacji Electronic Frontiers Foundation: https://ssd.eff.org/module-categories/tool-guides [dostęp: 15 VI 2020].

próby stworzenia modeli biznesowych na bazie narzędzi badających lub stymulujących albo tłumiących (inaczej: zmieniających) aktywność mózgu. W rezultacie na rynek są wprowadzane nowe technologie, które nie tylko pozwalają określić, jak działają ludzie, lecz także umożliwiają zmianę ich sposobów postępowania.

Na zakończenie należy podkreślić, że rozważania prowadzone w niniejszym artykule dotyczą głównie obecnego stanu rzeczy. Sytuacja jest jednak dynamiczna, a zjawiska tu przedstawiane są bardzo płynne. Bez ich rzetelnego opisu mogą umknąć istotne aspekty współczesnego świata. Niniejszy artykuł jest próbą naszkicowania fragmentu zachodzących w nim zmian.

Bibliografia

Alaa M. i in., *A review of smart home applications based on Internet of Things*, „Journal of Network & Computer Applications" 2017, nr 97, s. 48–65.

Andrejevic M., Gates K., *Editorial. Big Data Surveillance: Introduction*, „Surveillance and Society" 2014, nr 12, s. 185–196.

Bennett C.M. i in., *Neural correlates of interspecies perspective taking in the post-mortem Atlantic Salmon: An argument for multiple comparisons correction*, poster przedstawiony na konferencji „Human Brain Mapping" w 2009 r.

Bershidsky L., *No, Big Data Didn't Win the U.S. Election*, 8 XII 2016 r., https://www.bloomberg.com/view/articles/2016-12-08/no-big-data-didn-t-win-the-u-s-election [dostęp: 15 VI 2020].

Big Data. A Tool for Inclusion or Exclusion?, Federal Trade Comission Report, styczeń 2016 r., https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [dostęp: 15 VI 2020].

Boyd D., Crawford K., *CRITICAL QUESTIONS FOR BIG DATA: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, „Information Communication & Society" 2012, nr 5, s. 662–679.

Boyd D., *Undoing the Neutrality of Big Data*, „Florida Law Review" 2016, nr 67, s. 226–232.

Bradley L., *NFL players using Halo headsets to get more out of their workouts*, „Sports Illustrated", 28 XII 2016 r., https://www.si.com/tech-media/2016/12/28/nfl-players-using-halo-headsets-get-more-out-their-brains [dostęp: 15 VI 2020].

Castillo M., *Zuckerberg tells Congress Facebook is not a media company: 'I consider us to be a technology company'*, 11 IV 2018 r., https://www.cnbc.com/2018/04/11/mark-zuckerberg-facebook-is-a-technology-company-not-media-company.html [dostęp: 15 VI 2020].

Chen S., *„Forget the Facebook leak": China is mining data directly from workers' brains on an industrial scale*, „South China Morning Post", 29 IV 2018 r., http://www.scmp.

com/news/china/society/article/2143899/forget-facebook-leak-china-mining-data-directly-workers-brains [dostęp: 15 VI 2020].

Cheng C., Deng I., *WeChat joins list of Chinese technology banned by overseas militaries on security worries*, „South China Morning Post", 15 III 2018 r., https://www.scmp.com/tech/china-tech/article/2137232/wechat-joins-list-chinese-technology-banned-overseas-militaries [dostęp: 15 VI 2020].

Childs M., *Neurostimulation Could Optimize Our Brains — If It Can Overcome the Stigma*, wpis na blogu „Think Leaders" publikowanym na stronach IBM, 6 IX 2017 r., https://web.archive.org/web/20170906160133/https://www.ibm.com/blogs/think-leaders/new-thinking/neurostimulation-optimize-brains-can-overcome-stigma/ [dostęp: 15 VI 2020].

Clark V.P., *The ethical, moral, and pragmatic rationale for brain augmentation*, „Frontiers in Systems Neuroscience" 2014, nr 8, s. 1–4.

Coenen C., *Transhumanism in Emerging Technoscience as a Challenge for the Humanities and Technology Assessment*, „Teorija in Praksa" 2014, nr 51, s. 754–771.

Collins T., *SF Giants trying Halo headphones to get back to World Series,* „c|net", 29 III 2017 r., https://www.cnet.com/news/sf-giants-halo-headphones-world-series-baseball/ [dostęp: 15 VI 2020].

Corbett-Davies S., Goel S., González-Bailón S., *Even Imperfect Algorithms Can Improve the Criminal Justice System*, 20 XII 2017 r., https://www.nytimes.com/2017/12/20/upshot/algorithms-bail-criminal-justice-system.html [dostęp: 15 VI 2020].

Corea F., *Big Data and Risk Management in Financial Markets: A Survey*, Note technique NT 16-01, Montreal Institute of Structured Finance and Derivatives, 2016, http://cdi-icd.org/wp-content/uploads/2018/03/NT-16-01_Corea_CDI.pdf [dostęp: 15 VI 2020].

Crook J., *Uber applies for patent that would detect drunk passengers*, 11 VI 2018 r., https://techcrunch.com/2018/06/11/uber-applies-for-patent-that-would-detect-drunk-passengers/ [dostęp: 15 VI 2020].

Curme C. i in., *Quantifying the semantics of search behavior before stock market moves*, „Proceedings of the National Academy of Sciences", 28 VII 2014 r., https://doi.org/10.1073/pnas.1324054111 [dostęp: 15 VI 2020].

Darrow B., *The Question of Who Owns the Data Is About to Get a Lot Trickier*, 6 IV 2016 r., http://fortune.com/2016/04/06/who-owns-the-data/ [dostęp: 15 VI 2020].

Dobrin A., *Is Neuroscience Today's Phrenology?*, 22 VIII 2016 r., https://www.psychologytoday.com/us/blog/am-i-right/201608/is-neuroscience-todays-phrenology [dostęp: 15 VI 2020].

Donato C., *The #BigData Revolution: Who Owns Our Information?*, 11 IV 2016 r., https://www.forbes.com/sites/sap/2016/04/11/the-bigdata-revolution-who-owns-our-data/#2f2739bb68dd [dostęp: 15 VI 2020].

Du S. i in., *Automatic license plate recognition (ALPR): A state-of-the-art review*, „IEEE Transactions on Circuits and Systems for Video Technology" 2013, nr 2, s. 311–325.

Farah M.J., *Neuroethics: The Ethical, Legal, and Societal Impact of Neuroscience*, „Annual Review of Psychology" 2012, nr 63, s. 571–591.

Frank M., Roehrig P., Pring B., *What to do When Machines do Everything*, Hoboken 2017, Wiley.

Frankle J., *How Russia's New Facial Recognition App Could End Anonymity*, 23 V 2016 r., https://www.theatlantic.com/technology/archive/2016/05/find-face/483962/ [dostęp: 15 VI 2020].

Freedom on the Net. Ukraine 2017, https://freedomhouse.org/sites/default/files/FOTN%20 2017_Ukraine.pdf [dostęp: 15 VI 2020].

Gangadharan P.S., *The Dangers of High-Tech Profiling, Using Big Data*, „The New York Times", 7 VIII 2014 r., https://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/the-dangers-of-high-tech-profiling-using-big-data [dostęp: 15 VI 2020].

Ganis G., Keenan J.P., *The cognitive neuroscience of deception*, „Social Neuroscience" 2009, nr 4, s. 465–472.

Gates K.A., *Our Biometric Future. Facial Recognition Technology and the Culture of Surveillance*, New York 2018.

Gellene D., *Study finds left-wing brain, right-wing brain*, „Los Angeles Times", 10 IX 2007 r., http://www.latimes.com/local/obituaries/la-sci-politics10sep10-story.html [dostęp: 15 VI 2020].

Griffith E., *Memo to Facebook: How To Tell If You're a Media Company*, 12 X 2017 r., https://www.wired.com/story/memo-to-facebook-how-to-tell-if-youre-a-media-company/ [dostęp: 15 VI 2020]).

Grimmelman J., 30 VI 2014, http://laboratorium.net/archive/2014/06/30/the_facebook_emotional_manipulation_study_source [dostęp: 15 VI 2020].

Gubański K., *Smart city – sformatowany produkt czy narzędzie demokratyzacji? Dwa scenariusze rozwoju współczesnych polityk miejskich*, „Studia Socjologiczne" 2018, nr 1, s. 99–116.

Gurtowski M., Waszewski J., *Cyfrowy rasizm? Zautomatyzowane techniki nadzoru jako narzędzie segregacji i dyskryminacji*, „Transformacje" 2015, nr 1–2, s. 88–107.

Haber T., *The Big Data Real Estate Controversy*, „The Huffington Post", 19 V 2014 r., https://www.huffingtonpost.com/toni-haber/the-big-data-real-estate-_b_5352573.html [dostęp: 15 VI 2020].

Harari Y.N., *Homo deus. Krótka historia jutra*, Warszawa 2018, Wydawnictwo Literackie.

Harris T., *How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist*, „Thrive Global", 18 V 2016 r., https://journal.thriveglobal.com/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 [dostęp: 15 VI 2020].

Harris T., *Our Minds Have Been Hijacked by Our Phones*, rozmawiał Nicholas Thompson, 26 VII 2017 r., https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/ [dostęp: 15 VI 2020].

Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns. Investigation update*, raport brytyjskiej instytucji chroniącej dane osobowe, 11 VII 2018 r., https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf [dostęp: 15 VI 2020].

Jacobs H., *China's 'Big Brother' surveillance technology isn't nearly as all-seeing as the government wants you to think*, „Business Insider", 15 VII 2018 r., https://www.businessinsider.com/china-facial-recognition-limitations-2018-7 [dostęp: 15 VI 2020].

Jain A., Kanhangad V., *Gender classification in smartphones using gait information*, „Expert Systems with Applications" 2018, nr 93, s. 257–266.

Kehl D., Guo P., Kessler S., *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing*, 2017, Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School, https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf [dostęp: 15 VI 2020].

Keizer G., *Privacy*, New York 2012, Picador.

Kemeny E., *AI hunts for crimes caught on camera*, „New Scientist" z 18 sierpnia 2018 r., s. 10.

Kiss J., Arthur C., *Publishers or platforms? Media giants may be forced to choose*, „The Guardian" z 29 lipca 2013 r., https://www.theguardian.com/technology/2013/jul/29/twitter-urged-responsible-online-abuse [dostęp: 15 VI 2020].

Koetsier J., *Digital Duopoly Declining? Facebook's, Google's Share Of Digital Ad Dollars Dropping*, forbes.com, 19 III 2018 r., https://www.forbes.com/sites/johnkoetsier/2018/03/19/digital-duopoly-declining-facebooks-googles-share-of-digital-ad-dollars-dropping/#22396bf360a8 [dostęp: 15 VI 2020].

Kolanovic M., Krishnamachari R., *Big Data and AI Strategies: Machine Learning and Alternative Data Approach to Investing*, JP Morgan, maj 2017 r., https://www.cfasociety.org/cleveland/Lists/Events%20Calendar/Attachments/1045/BIG-Data_AI-JPMmay2017.pdf [dostęp: 15 VI 2020].

KPMG, *Your connected car is talking. Who's listening?*, 2016, https://assets.kpmg.com/content/dam/kpmg/se/pdf/komm/2016/se-your-connected-car-is-talking.pdf [dostęp: 15 VI 2020].

Kramer A.D.I., Guillory J.E., Hancock J.T., *Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks*, „Proceedings of the National Academy of Sciences" 2014, nr 24, s. 8788–8790.

Krzysztofek K., *Kierunki ewaluacji technologii cyfrowych w działaniu społecznym. Próba systematyzacji problemu*, „Studia Socjologiczne" 2017, nr 1, s. 195–224.

Krzysztofek K., *Technologie cyfrowe w dyskursach o przyszłości pracy*, „Studia Socjologiczne" 2015, nr 4, s. 5–31.

Langleben D.D., Moriarty J.C., *Using Brain Imaging for Lie Detection: Where Science, Law and Research Policy Collide*, „Psychology, Public Policy, and Law" 2013, nr 2, s. 222–234.

Lomas N., *A brief history of Facebook's privacy hostility ahead of Zuckerberg's testimony*, 10 IV 2018 r., https://techcrunch.com/2018/04/10/a-brief-history-of-facebooks-privacy-hostility-ahead-of-zuckerbergs-testimony/ [dostęp: 15 VI 2020].

Luhn A., *Ukraine blocks popular social networks as part of sanctions on Russia*, 16 V 2017 r., https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war [dostęp: 15 VI 2020].

Lyon D., *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, „Big Data & Society" 2014, nr 2, s. 1–14.

Mansell R., *Power, Hierarchy and the Internet: Why the Internet Empowers and Disempowers*, „The Global Studies Journal" 2016, nr 2, s. 19–25.

Mansouri N., Aouled Issa M., Ben Jemaa Y., *Gait features fusion for efficient automatic age classification*, „IET Computer Vision" 2018, nr 1, s. 69–75.

McCarthy M., *The big data divide and its consequences*, „Sociology Compass" 2016, nr 12, s. 1131–1140.

McMahon D., *America's top cyclist entering the Tour de France has been using a portable brain stimulator to try to gain an edge, and he says it actually works*, 26 VI 2017 r., http://www.businessinsider.com/tour-de-france-cyclist-talansky-halo-neuroscience-headset-technology-2017-6?IR=T [dostęp: 15 VI 2020].

Mohapatra S. i in., *Real time biometric surveillance with gait recognition*, „AIP Conference Proceedings" 2018, nr 1.

Monetizing car data: New service business opportunities to create new customer benefits, 2016, McKinsey&Company, https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx [dostęp: 15 VI 2020].

Mullins C.S., *Who Owns the Data?*, „Database Trends and Applications", 1 VI 2018 r., http://www.dbta.com/Columns/DBA-Corner/Who-Owns-the-Data-125485.aspx [dostęp: 15 VI 2020].

Murphy H., *Why Stanford Researchers Tried to Create a 'Gaydar' Machine*, „The New York Times", 9 X 2017 r., https://www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html [dostęp: 15 VI 2020].

Nelson J. i in., *The Effects of Transcranial Direct Current Stimulation (tDCS) on Multitasking Throughput Capacity*, „Frontiers in Human Neuroscience" 2016, t. 10, artykuł 589, s. 1–13.

Nielsen M., *Who Owns Big Data?*, 2014, https://www.bbvaopenmind.com/wp-content/uploads/2014/03/BBVA-OpenMind-Who-Owns-Big-Data-Michael-Nielsen.pdf.pdf [dostęp: 15 VI 2020].

O'Neil C., *Bronie matematycznej zagłady*, Warszawa 2019, Wydawnictwo Naukowe PWN.

Ong T., *Amazon patents wristbands that track warehouse employees' hands in real time*, 1 II 2018 r., https://www.theverge.com/2018/2/1/16958918/amazon-patents-trackable-wristband-warehouse-employees [dostęp: 15 VI 2020].

Orliński W., *Facebook niczym obora*, „Blog Wojciecha Orlińskiego", 4 XI 2010 r., http://wo.blox.pl/2010/11/Facebook-niczym-obora.html [dostęp: 15 VI 2020].

Parker Jones O., Alfaro-Almagro F., Jbabdi S., *An empirical, 21st century evaluation of phrenology*, „Cortex" 2018, t. 106, s. 26–35.

Piekutowski J., *Bronie matematycznego zniszczenia*, „Nowa Konfederacja" 2017, nr 8, s. 3–10, https://nowakonfederacja.pl/bronie-matematycznego-zniszczenia/ [dostęp: 15 VI 2020].

Pisani P.H. i in., *Enhanced template update: Application to keystroke dynamics*, „Computers & Security" 2016, t. 60, s. 134–153.

Prakash C., Kumar R, Mittal N., *Recent developments in human gait research: parameters, approaches, applications, machine learning techniques, datasets and challenges*, „Artificial Intelligence Review" 2018, nr 1, s. 1–40.

Pressman A., *Fitbit Adds Social Feed to Keep Users Motivated*, Fortune.com, 5 I 2017 r., http://fortune.com/2017/01/05/fitbit-social-feed-motivated/ [dostęp: 15 VI 2020].

Raz A., *From Neuroimaging to Tea Cup Leaves in the Bottom of a Cup*, w: *Critical Neuroscience. A Handbook of the Social and Cultural Contexts of Neuroscience*, S. Choudhury, J. Slaby (red.), Chichester 2012, Wiley-Blackwell, s. 265–272.

Rodak O., *Twitter jako przedmiot badań socjologicznych i źródło danych społecznych. Perspektywa konstruktywistyczna*, „Studia Socjologiczne" 2017, nr 3, s. 209–236.

Rodrigues J., Speciale A., *How Central Banks Are Using Big Data to Help Shape Policy*, 18 XII 2017 r., https://www.bloomberg.com/news/articles/2017-12-18/central-banks-are-turning-to-big-data-to-help-them-craft-policy [dostęp: 15 VI 2020].

Ruppert E., Isin E., Bigo D., *Data politics*, „Big Data & Society" 2017, nr 2, s. 1–7.

Sahito F.H., Slany W., *Functional Magnetic Resonance Imaging and the Challenge of Balancing Human Security with State Security*, „Human Security Perspectives" 2012, nr 9, s. 38–66.

Scott M., Delcker J., *Free speech vs. censorship in Germany*, „politico.eu", 4 I 2018 r., https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech/ [dostęp: 15 VI 2020].

Sherman L., *Why Facebook Will Never Change Its Business Model*, Forbes.com, 16 IV 2018 r., https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model [dostęp: 15 VI 2020].

Singer N., *Facebook's Push for Facial Recognition Prompts Privacy Alarms*, „The New York Times", 9 VII 2018 r., https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html [dostęp: 15 VI 2020].

Solove D.J., *Conceptualizing Privacy*, „California Law Review" 2002, nr 4, s. 1087–1156.

Solove D.J., *Nothing to Hide. The False Tradeoff between Privacy and Security*, New Haven–London 2013, Yale University Press.

Stecklow S., *Why Facebook is losing the war on hate speech in Myanmar*, 15 VIII 2018 r., https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/ [dostęp: 15 VI 2020].

Szafrański B., *Biometria przyszłością bankowości*, relacja z „International Biometric Congress 2017", 27 IX 2017 r., https://alebank.pl/biometria-przyszloscia-bankowosci/ [dostęp: 15 VI 2020].

Szahaj A., *Kapitalizm drobnego druku*, Warszawa 2014, Instytut Wydawniczy Książka i Prasa.

The Guardian view on big data: the danger is less democracy, 26 II 2017 r., https://www.theguardian.com/commentisfree/2017/feb/26/the-guardian-view-on-big-data-the-danger-is-less-democracy [dostęp: 15 VI 2020].

The Transhumanist FAQ, v. 3.0., World Transhumanist Association, https://humanityplus.org/philosophy/transhumanist-faq/ [dostęp: 15 VI 2020].

Tufekci Z., *Engineering the public: Big data, surveillance and computational politics*, „First Monday", 7 VII 2014 r., nr 7, http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097 [dostęp: 15 VI 2020].

Wang Y., Kosiński M., *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*; ostatnia aktualizacja tego roboczego artykułu pochodzi z 26 V 2020 r., https://osf.io/zn79k/ [dostęp: 15 VI 2020].

Weisberg J., *The Digital Poorhouse*, „The New York Review of Books", 7 VI 2018 r., https://www.nybooks.com/articles/2018/06/07/algorithms-digital-poorhouse [dostęp: 15 VI 2020].

Witkowski T., *Inteligencja makiaweliczna. Rzecz o pochodzeniu natury ludzkiej*, Taszów 2005, Moderator.

Wolfe J., *Roomba vacuum maker iRobot betting big on the 'smart' home*, 24 VII 2017 r., https://www.reuters.com/article/us-irobot-strategy/roomba-vacuum-maker-irobot-betting-big-on-the-smart-home-idUSKBN1A91A5 [dostęp: 15 VI 2020].

Wong J.C., *Former Facebook executive: social media is ripping society apart*, „The Guardian", 12 XII 2017 r., https://www.theguardian.com/technology/2017/dec/11/facebook-former-executive-ripping-society-apart [dostęp: 15 VI 2020].

Yeh C.-L., *Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers*, „Telecommunications Policy" 2018, nr 4, s. 282–292.

ORCID: 0000-0002-7370-3714