FOLIA 322

Annales Universitatis Paedagogicae Cracoviensis

Studia ad Bibliothecarum Scientiam Pertinentia 18 (2020)
ISSN 2081-1861
DOI 10.24917/20811861.18.24

Hanna Batorowska
Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie
ORCID 0000-0001-6759-5094

Przegląd wizji badaczy na temat bezpieczeństwa i przetrwania człowieka w dobie *big data* i sztucznej inteligencji

Wstęp

Człowiek zawsze chciał wiedzieć, co go może czekać w najbliższej przyszłości, czy zrealizuje swoje marzenia, zdobędzie miłość, sławę, bogactwo lub władzę. Pytania te nigdy nie utraciły znaczenia, ale w cywilizacji technologicznej zyskały szerszą perspektywę. Żyjemy w czasach ryzyka i katastrof, w czasach, w których „płynne pokolenie" o „płynnej kulturze" podejmuje „płynne wybory" oparte na „płynnej etyce" i decyzje wynikające z kwantyfikowania wszystkich elementów rzeczywistości. Uznając danetyzację za główny sposób poznania rzeczywistości społecznej, wielu wizjonerów oparło przewidywanie przyszłości na algorytmizacji danych i wyszukiwaniu związków, jakie pomiędzy nimi istnieją. Wchodzimy w epokę ekstrakcji wiedzy z danych pochodzących z ogromnych, niespójnych, różnorodnych zbiorów, w epokę przewidywania przyszłości na ich podstawie i projektowania jej zgodnie z wynikiem tego przetwarzania dostarczanym przez algorytmy eksploracji danych i programów opartych na sztucznej inteligencji. Człowiek niebędący w stanie przetworzyć wyprodukowanych przez siebie danych musi posłużyć się w procesie ich obróbki coraz doskonalszymi maszynami, wyposażonymi w narzędzia, nad którymi coraz trudniej jest mu utrzymać kontrolę. Zagrożenia, jakie generuje technologia Internetu rzeczy i *big data*, zmuszają człowieka do szukania sposobów zapobiegania im. W pierwszej kolejności uwaga koncentruje się na zabezpieczeniach technologicznych i ustaleniach legislacyjnych. Niestety, im doskonalsze systemy ochrony, tym bardziej przebiegły staje się przeciwnik dążący do ich zniszczenia, a prawo nigdy nie nadąża za zmianami, które są wynikiem rozwoju technologicznego i wirtualizacji życia. Człowiek jako najsłabsze ogniwo w systemie bezpieczeństwa staje się celem ataków różnych destruktorów, także tych dysponujących sztuczną inteligencją. Łatwo jest go złamać, jeżeli nie posiada świadomości istnienia tych zagrożeń, nie zna mechanizmów ich działania, brak mu kompetencji pozwalających ograniczyć wrogie działania. Stąd większość refleksji prowadzonych na temat miejsca i roli człowieka w świecie wysokich technologii odnosi się do potrzeby rozwoju jego świadomości i dojrzałości jako podmiotu bezpieczeństwa.

Prognozowanie w czasach *big data*

Przepowiadanie przyszłości przez wizjonerów, szamanów i wróżki zostaje w społeczeństwach wysoko rozwiniętych technologicznie zastąpione produktami analitycznymi opracowywanymi przez zespoły specjalistów od analizy danych i informacji oraz wyspecjalizowane służby analityczno-informacyjne. Oparte na naukowych przesłankach działania mają wykluczyć subiektywne i irracjonalne elementy z procesu wnioskowania z danych na temat możliwości zaistnienia różnych zdarzeń. W świecie cyfrowych technologii i przeciążenia informacyjnego przyjęto uważać, że przewidywanie oparte na rzetelnych danych powinno być trafne, ponieważ algorytmy do przeszukiwania dużych zbiorów danych są coraz bardziej wyrafinowane i pozwalają na tworzenie doskonałych modeli, wzorców oraz dostrzeganie relacji dzięki wnioskowaniu opartemu na korelacjach. Nate Silver, amerykański statystyk i specjalista od prognoz wyborczych, przestrzega jednak przed naiwną wiarą w prawidłowość wyników zwracanych przez modele statystyczne oraz przed błędnym założeniem, że wzrost ilości informacji, którą jesteśmy w stanie przetworzyć, zbliża człowieka do prawdy. Większość wygenerowanych przez ludzkość danych określa jako szum, którego „natężenie rośnie znacznie szybciej niż natężenie sygnału”[1], a tylko „sygnał jest prawdą. Szumem jest wszystko to, co odciąga od niej naszą uwagę”[2]. Sygnał uznaje za „przejaw prawdy leżącej u podstaw problemu statystycznego lub prognostycznego”[3]. Z informacji jesteśmy w stanie wygenerować wiedzę, ale tylko, gdy są one umieszczone w odpowiednim kontekście. Dzięki temu możemy wydzielić sygnały, czyli prawdę z „morza fałszywie prawdziwych informacji”, czyli z szumu[4].

Autor książki o szumach i sygnałach twierdzi, że istnieje duże prawdopodobieństwo ryzyka wygenerowania złych prognoz, jeżeli błędnie odczytamy i zinterpretujemy liczby, nadając im subiektywne znaczenie. Pisarz przywołuje przykłady pozwalające uznać, że pomimo wielości dostępnych informacji tylko niewielki ich procent jest faktycznie użyteczny. Selekcjonując je, często nie kierujemy się sprecyzowanymi dokładnie kryteriami, wybieramy je w sposób przypadkowy, nie zwracamy uwagi na zniekształcenia, do których dochodzi na skutek takiego postępowania. „Zanieczyszczenie danych” łączy Silver ze skłonnościami człowieka do preferowania informacji najnowszych, przemilczania, np. przez dziennikarzy faktu, że sondaże mogą być obarczone błędem prognozy, a komentarze są oparte na niedokładnych danych statystycznych[5].

Koncepcja prognozowania Nate'a Silvera bazuje na teorii Thomasa Bayesa, zgodnie z którą „powinniśmy myśleć zupełnie inaczej o naszych ideach i sposobie ich testowania i oswoić się z prawdopodobieństwem i niepewnością”[6]. Musimy dostrzec niedoskonałości w naszym myśleniu[7] i zaakceptować fakt, że nasza wiedza o świecie jest niepewna i dlatego nie jest możliwe sformułowanie idealnej prognozy[8].

1 N. Silver, *Sygnał i szum. Sztuka prognozowania w erze technologii*, Gliwice 2014, s. 21.
2 Tamże, s. 25.
3 Tamże, s. 384.
4 Tamże, s. 415.
5 Tamże, s. 416.
6 Tamże, s. 23.
7 Tamże, s. 415.
8 Tamże, s. 410.

Katarzyna Materska, badacz problemów zarządzania informacją w organizacjach, powołując się na koncepcję *Imperfect Knowledge Economics* sformułowaną przez Romana Frydmana i Michaela D. Goldberga, podkreśla, że nie można bagatelizować faktu „nieprzewidywalności ludzkich reakcji na sygnały, informacje, polecenia i bodźce", ponieważ racjonalne podejście do procesów zarządzania informacją często nie jest realizowane. Oznacza to, że podejmowanie decyzji, oceny i selekcji informacji, tworzenie prognoz oparte na systematycznej analizie danych i logicznym myśleniu obarczone są błędem wynikającym z irracjonalności ludzkich zachowań informacyjnych, z czynników afektywnych i związanych z osobowością, z przyjętego systemu wartości, ze skłonności do ryzyka i popełniania błędów, z poziomu ambicji i nastawienia do eksperymentowania, ze stylów uczenia się, ograniczeń kognitywnych, niepewności traktowanej jako subiektywny stan umysłu człowieka, z braku wystarczających kompetencji informacyjnych, w tym ograniczania się do informacji nie do końca satysfakcjonującej odbiorcę[9]. Do tych czynników Nate Silver zalicza skłonność człowieka do mylenia nieznanego z nieprawdopodobnym. Uważa ją za przyczynę urealnienia wielu niebezpieczeństw[10], dlatego „wiedząc więcej o tym czego nie wiemy, możemy sprawić, że przynajmniej część naszych prognoz będzie lepsza"[11]. Udowadnia, że prognozowanie zawsze będzie obarczone błędem, ponieważ dokonuje się w przestrzeni, w której granica między obiektywizmem a subiektywizmem jest bardzo niewyraźna[12]. Konieczne jest zatem uwzględnienie badań nad konsekwencjami opierania się na wiedzy niepełnej i niedoskonałej. Katarzyna Materska dostrzega konsekwencje braku wiedzy człowieka na temat swojej niewiedzy, jakie mają miejsce we współczesnej rzeczywistości społecznej. Uważa, że nie wystarczy w podejmowaniu decyzji i formułowaniu prognoz polegać tylko na zasobach, zbiorach zasad i technologiach informacyjnych, ale należy uwzględniać także

> zachowania i działania człowieka, w czym przejawia się humanistyczno-społeczny wymiar zarządzania informacją. W ostatecznym rachunku to człowiek decyduje, które z informacji dostarczanych przez technologie są satysfakcjonujące, wystarczająco dobre. W niedoskonałym środowisku informacji i wiedzy racjonalność i intuicja stają się równouprawnione w ZI[13].

Prognozowanie jako proces opisywany przez Nate'a Silvera dotyczy przede wszystkim zagrożeń, których nie znamy zbyt dobrze. W jego książce, która ukazała się w 2012 roku, przewidywał, że zagrożeniem takim może być użycie broni biologicznej, narażającej ludzkość na choroby zakaźne. Prognozował, że zagrożenie takie „utrzymywałoby się przez wiele tygodni lub miesięcy, szkoły i sklepy byłyby zamknięte, szpitale objęte kwarantanną, a granice państw uszczelnione (…) Trudno byłoby oszacować liczbę ofiar śmiertelnych (…), ponieważ rozwoju epidemii choroby zakaźnej w zasadzie nie da się prognozować, dopóki się ona nie zacznie"[14]. Rok

9 K. Materska, *Zarządzanie informacją w warunkach wiedzy niedoskonałej*, [w:] *Zarządzanie informacją*, red. W. Babik, Warszawa 2019, s. 347.
10 N. Silver, dz. cyt., s. 387.
11 Tamże, s. 410.
12 Tamże, s. 417.
13 K. Materska, dz. cyt., s. 351.
14 N. Silver, dz. cyt., s. 403.

2020 przyniósł przedsmak takiego przerażającego scenariusza, w którym ludzkości przyszło zmierzyć się z pandemią COVID-19. Doświadczamy życia w warunkach ryzyka, uczymy się nowych reguł, współodpowiedzialności i walczymy z bezsilnością, oczekując na otrzymanie szczepionki, z którą łączymy nadzieję na powrót do normalności. Z każdym miesiącem powrót ten będzie powrotem do innej rzeczywistości, w której zmienią się zapewne nasze przyzwyczajenia, sposób porozumiewania się, osłabną więzi, wzmoże się agresywność, normalnością stawać się będą zachowania egoistyczne. Mam nadzieję, że się mylę, ale po pandemii będzie to już inny świat.

Jan Zych, analityk i ekspert w dziedzinie bezpieczeństwa, analizując paradygmat, którego kanwą jest „myślenie korelacyjne zastępujące dotychczas preferowane myślenie przyczynowo-skutkowe", wskazuje na wykorzystanie tegoż paradygmatu do prognozowania lub budowania mechanizmów weryfikujących występujących między bytami lub zjawiskami. Przy tego typu myśleniu nie ma potrzeby, aby we wnioskowaniu wystąpiła pewność, że obserwowane zjawisko jest rzeczywistą przyczyną domniemanych skutków[15]. W praktyce oznacza to, jak dobitnie wyraża to Victor Mayer-Schönberger, profesor Uniwersytetu Oksfordzkiego zajmujący się problematyką nadzoru i regulowania Internetu, że istnieje niebezpieczeństwo, „że będziemy sądzić ludzi nie za ich rzeczywiste działania, ale za posiadane przez nich predyspozycje, które wywnioskujemy z danych"[16]. Nate Silver wskazuje na wiele przykładów sytuacji świadczących, że autorzy prognoz błędnie uznawali statystyczną korelację za związek przyczynowo-skutkowy i brali szum za sygnał. Dlatego ostrzega przed sytuacją, w której „szum w danych może skutecznie maskować sygnał, nawet wtedy, gdy nie ma wątpliwości co do tego, że ów sygnał istnieje"[17]. Sytuacja taka może spowodować, że zbagatelizujemy sygnały zapowiadające nadejście katastrofy czy innej tragedii, ponieważ wyda się nam sytuacją zupełnie nieprawdopodobną.

Rezygnacja z intuicyjnego przewidywania przyszłości na rzecz jej prognozowania na podstawie faktów, informacji, danych pozyskanych z różnych źródeł informacji, np. z Internetu rzeczy, tych gromadzonych przez służby wywiadowcze, uzyskanych w procesie analizy informacji pochodzących ze źródeł otwartych analizowanych w ramach tzw. białego wywiadu, przez agentów od monitorowania działalności konkurencyjnej, szpiegów gospodarczych, zbieranych przez systemy inwigilacji konsumenckiej, wygenerowanych przez środowiska akademickie, naukowców, wydaje się działaniem bardziej profesjonalnym. Przygotowane na tej podstawie scenariusze rozwoju wydarzeń uwzględniają różne ich warianty, opisują spodziewane efekty i konsekwencje realizacji przedsięwzięcia zgodnie z wybranym planem. Sugerowane przez ekspertów prognozy mają ułatwić decydentom podejmowanie decyzji strategicznych w celu zapewnienia społeczeństwu bezpieczeństwa, wolności, rozwoju, dostatku, godnych warunków życia. Niestety, jak dostrzegła amerykańska matematyczka Cathy O'Neil, zasilane matematyką aplikacje, napędzające ekonomię danych, bazują na wyborach dokonywanych przez człowieka popełniającego błędy i odzwierciedlają charakterystyczne dla niego uprzedzenia, brak zrozumienia oraz stronniczość. Wykorzystywane modele (tzw. beemzety), nawet jeżeli okazałyby się

15 J. Zych, *Teleinformatyka dla bezpieczeństwa 2.0*, Poznań 2019, s. 33.

16 V. Mayer-Schönberger, K. Cukier, *Big data efektywna analiza danych. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa 2017, s. 252.

17 N. Silver, dz. cyt., s. 344.

szkodliwe, nie podlegałyby dyskusji, bowiem akceptowano by algorytmy pozwalające karać osoby ubogie i wykluczone oraz pomnażać bogactwo ludzi zamożnych. Jak czytamy w książce C. O'Neil, algorytmy te, zamiast być obiektywne i pozbawione uprzedzeń, stają się bronią matematycznej zagłady dla słabych, zdesperowanych, przyczyniając się do wzrostu nierówności społecznych i zagrożeń dla demokracji[18].

Prognozowanie obarczone może być jednak wieloma błędami, o których pisze Nate Silver, i może wynikać ze złej jakości informacji, z ignorowania przez człowieka sygnałów i z niemożności wydzielenia z szumu informacyjnego danych o znaczeniu strategicznym dla rozwiązania danego problemu. Dlatego, zgodnie z ustaleniami amerykańskiego statystyka, tworzenie scenariuszy rozwoju wypadków wymaga od ich twórców dużej pokory. Powinni oni skromniej myśleć o swoich zdolnościach prognostycznych, co pozwoli im rzadziej powtarzać własne błędy[19].

Jeden z wizjonerów przyszłości świata zdominowanego przez technologie cyfrowe Kevin Kelly prorokował istnienie świata bez książek zastąpionych przez ich płynną wersję (zlinkowane zasoby wszystkich bibliotek świata) oraz bez bibliotekarzy i księgarzy[20]. Tymczasem jak udowadniali Derick de Kerrckhove, Nicholas Carr i Henry Jenkins, w świecie nowych mediów i technologii interaktywnych zmienia się tylko funkcja i status książki[21]. Książka przetrwa, ponieważ daje odpór manipulacji i zmusza czytelnika do wysiłku intelektualnego, do tworzenia własnych schematów myślowych niezależnych od wpływu mediów i sposobów porządkowania wiedzy przez systemy informatyczne[22]. Jednak w wyniku nadawania wszystkim mediom charakteru społecznościowego konstytuuje się odmienny sposób czytania i powstaje nowy sposób pisania. Zmiana dotyczy kontekstu czytania, który z prywatnego przyjmuje formę wspólną, sieciową, grupową. Jak konkluduje amerykański pisarz Nicholas Carr, współcześnie „ludzie czytają przede wszystkim po to, by mieć poczucie przynależności, a nie po to, by pogłębiać wiedzę, albo dobrze się bawić"[23].

Podobnie zawód bibliotekarza, który Kevin Kelly i Clifford Stoll łączyli z dysponowaniem wąską wiedzą na temat udostępniania zbiorów, pozwoliło im na prorokowanie upadku profesji, uznanej przez nich za „archaiczną". Tymczasem rozwój technologii wymaga wciąż nowych kompetencji od pracowników bibliotek, przyczyniając się do metamorfozy ich zawodu, szczególnie w odniesieniu do osób zatrudnionych w placówkach naukowych zajmujących się datafikacją (danetyzacją) rzeczywistości oraz zarządzaniem dużymi zasobami danych (*big data*). W tej nowej roli bibliotekarz staje się badaczem danych (*data scientit*), czyli specjalistą od analizy danych i zarządzania nimi lub bibliotekarzem danych (*data librarian*), czyli specjalistą od baz i hurtowni danych, eksploracji danych, ich ekstrakcji ze źródeł cyfrowych i wizualizacji wyników dostarczonych przez agregator *big data*. Pełnić on powinien funkcję asystenta badacza w realizowanym przez niego procesie

18 C. O'Neil, *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówność i zagrażają demokracji*, Warszawa 2017, s. 27.

19 N. Silver, dz. cyt., s. 418.

20 Ł. Gołębiewski, *Śmierć książki. No future book*, Warszawa 2008, s. 76–77; Tenże, *Książka/book. Szerokopasmowa kultura*, Warszawa 2009, s. 81.

21 H. Jenkins, *Kultura konwergencji. Zderzenie starych i nowych mediów*, Warszawa 2007, s. 249.

22 D. Kerckhove, *Inteligencja otwarta. Narodziny społeczeństwa sieciowego*, Warszawa 2001, s. 139–140.

23 N. Carr, *Płytki umysł. Jak Internet wpływa na nasz mózg*, Gliwice 2012, s. 135.

badawczym i wspomagać go poprzez tworzenie i zarządzanie danymi badawczymi. Dane te są w ramach otwartego dostępu gromadzone przez biblioteki naukowe i stanowią część zasobów repozytoriów instytucjonalnych. Zarządzanie dużymi zespołami nieustrukturyzowanych danych wymaga nowych kompetencji od bibliotekarzy przyszłości, którzy będą mieli więcej wspólnego ze specjalistami od informatyki niż z ekspertami w obszarze nauk humanistycznych. To tylko jeden z przykładów zmian jakościowych dokonujących się pod wpływem wzmożonej aktywności człowieka w wymiarach rzeczywistości rozszerzonej i wirtualnej[24].

Przed nauką o informacji otwierają się zatem nowe obszary penetracji naukowej związane ze studiowaniem zachowań informacyjnych użytkowników korzystających z narzędzi AR i VR podczas różnych etapów procesu informacyjnego, z zagrożeniami, jakie generuje technologia AR dla bezpieczeństwa ich użytkowników (np. z zagrożeniami dla zachowania prywatności lub przyczyniającymi się do osłabienia odporności na perswazję, z zagrożeniami potęgującymi zjawisko stresu informacyjnego w obliczu nadmiarowości bodźców i danych, wzmacniającymi lęk przed technologią informacyjną – narzędziami AR i VR – z bagatelizowaniem problemu inwigilacji, kłopotami z opanowaniem emocjonalności, możliwości wykluczenia), z kształceniem specjalistycznych kompetencji informacyjnych, z kulturą informacyjną osób „zanurzonych" w rzeczywistości wirtualnej, z analizą cech informacji udostępnianej za pośrednictwem technologii AR lub funkcjonalności bibliotecznych aplikacji AR.

Trudne pytania dotyczące przyszłości

Współcześnie szczególnie humanistycznego podejścia będzie wymagać formułowanie odpowiedzi na pytania stawiane przez specjalistów od tworzenia prognoz przyszłości zdominowanej przez technologie informacyjno-komunikacyjne. Są to pytania nurtujące takich badaczy współczesnych problemów masowej inwigilacji wykorzystującej narzędzia sztucznej inteligencji jak Julia Angwin, Zygmunt Bauman, Bruce Schneier, Kevin Kelly, David Lyon, Victor Mayer-Schönberger, Kenneth Cukier, Cathy O'Neil, Michael Miller, John Brockman, Nick Bostrom, Alex Pentland, Stephen Wolfram i innych. Problemy te dotyczą kwestii dominacji superinteligencji nad człowiekiem i oceny realności zaistnienia opisanej sytuacji w przyszłości oraz konsekwencji wynikających z takiej przewagi. Wizjonerzy i naukowcy rozważają możliwość kresu naszego gatunku podporządkowanego i kontrolowanego przez sztuczną inteligencję[25], a co najmniej kresu tego, co nazywamy człowieczeństwem. Dostrzegają także rozwiązania, które być może uchronią ludzkość przed samozagładą, ale wymagać będą od nas znalezienia odpowiedzi na pytania, a następnie dokonania dobrych wyborów.

Jednak sformułowanie dobrych pytań o sposób funkcjonowania człowieka w przyszłości, jak unaocznia to Kevin Kelly, nie będzie łatwe, ponieważ powinny one tworzyć nowy obszar refleksji oraz zmuszać do przeformułowania własnych odpowiedzi i generowania wielu innych dobrych pytań. Cenne pytania to te, które przesuwają granice pomiędzy tym, co znane, a tym, co nieznane, dlatego zadawanie

24 M. Wójcik, *Rozszerzona rzeczywistość w usługach informacyjnych bibliotek*, Kraków 2018, s. 119–120.

25 N. Bostrom, *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016.

pytań ma według Kevina Kelly'ego większą moc niż szukanie odpowiedzi[26]. Warto przywołać kilka z nich autorstwa wyżej wymienionych ekspertów, aby ukazać stopień skomplikowania problemów związanych z cywilizacją technologiczną:

1) Czy potrafimy żyć dla przyszłości, nawet jeżeli nie jest to już nasza przyszłość[27]?
2) Czy potrafimy chronić zmarginalizowanych i tych, których sprofilowano jako osoby podejrzane, nie lękając się tego, co może nas spotkać z powodu naszych działań[28]?
3) Czy inwazyjność dragnetu jest dopasowana do celu, jakiemu służy, i czy przynosi on korzyści społeczeństwu[29]?
4) Czy bycie obserwowanym i oglądanym może być antidotum na toksyczność wykluczenia i przestaje być zagrożeniem[30]?
5) Czy powszechne śledzenie powinniśmy uznać za normę, gdy wszystko, co kiedyś było mierzalne, zostanie skwantyfikowane, zamienione na postać cyfrową i przeznaczone do monitorowania[31]?
6) Czy potrafimy ucywilizować i zagospodarować monitorowanie tak, aby było produktywne i korzystne dla obu stron inwigilacji[32]?
7) Czy w społeczeństwie opartym na współmonitorowaniu może zaistnieć świadomość swoich praw[33]?
8) W jakim stopniu etyka normatywna może sprawdzać się w warunkach współczesnej inwigilacji?
9) Czy potrzebujemy sztucznej inteligencji, aby dowiedzieć się od niej, czym jest człowiek[34]?
10) Czy w świecie *big data* potrafimy chronić najbardziej ludzkie cechy, takie jak kreatywność, intuicję i ambicje intelektualne, aby nie zdominowały człowieka odpowiedzi wygenerowane przez maszyny na podstawie eksploracji danych[35]?
11) Czy zdołamy oprzeć się pokusie osądzania ludzi za posiadane przez nich predyspozycje, które wywnioskujemy z danych, naruszając w ten sposób zasadę sprawiedliwości i wolnej woli[36]?
12) Czy potrafimy oprzeć się pauperyzacji intelektualnej polegającej na osłabieniu potencjału intelektualnego ludzi i w konsekwencji zastąpienia pewnych czynności przez technologie, co doprowadzi do zaniku zdolności analitycznych, skłonności do podejmowania ryzyka i zdominowania jednostki przez dyktat danych[37]?

---

26 K. Kelly, *Nieuniknione. Jak inteligentne technologie zmienią naszą przyszłość*, Warszawa 2017, s. 399–401.

27 Z. Bauman, D. Lyon, *Płynna inwigilacja. Rozmowy*, Kraków 2013, s. 219.

28 Tamże.

29 J. Angwin, *Społeczeństwo inwigilowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, Warszawa 2017, s. 332.

30 Z. Bauman, D. Lyon, dz. cyt., s. 30, 40.

31 K. Kelly, dz. cyt., s. 357.

32 Tamże.

33 K. Kelly, dz. cyt., s. 363.

34 Tamże, s. 74.

35 V. Mayer-Schönberger, K. Cukier, dz. cyt., s. 256.

36 Tamże, s. 252.

37 K. Leśniak-Moczuk, *Społeczeństwo równości czy zniewolone danetyzacją*, „Nierówności Społeczne a Wzrost Gospodarczy" 2017, nr 52 (4), s. 234.

13) Czy potrafimy ustrzec ludzkość przed skutkami ubocznymi rozwoju technologicznego?
14) Czy potrafimy zadbać o opłacalność, medialność i społeczną akceptację naszego bezpieczeństwa i czy opłaca się bronić wszystkich ludzi i wszystkich wartości[38]?

W odpowiedziach na powyższe pytania uzewnętrznia się siła informacji pozyskiwanej w procesach monitorowania, śledzenia, obserwowania, podsłuchiwania, przechwytywania, filtrowania, skanowania, wykorzystywanej do uzyskiwania przewagi nad podmiotem obranym jako cel inwigilacji. Oznacza to koniec ery zaufania do drugiego człowieka, jeżeli nie prześwietli się jego życia, nie przeskanuje wszystkich dostępnych informacji na jego temat, nie „przesłucha" znajomych naszego kontrahenta i osób z jego otoczenia, nie stworzy jego profilu w oparciu o dane z różnych źródeł, przetwarzane w sposób wielostrumieniowy. Bardziej będziemy skłonni zawierzać bazom i silosom danych kolekcjonującym informacje według niezrozumiałych dla nas algorytmów niż zaryzykować i polegać na doświadczeniu, intuicji i mądrości pozwalającej odróżnić fikcję od rzeczywistości i zdemaskować proceder sterowania przekazem medialnym przez programy generujące fałszywą aktywność w sieci. W świecie postprawdy i kłamstwa coraz trudniej będzie znaleźć punkt odniesienia, na którym można budować bezpieczeństwo.

Tym punktem odniesienia dla Kevina Kelly'ego może być holos, czyli „zbiorowa inteligencja wszystkich ludzi połączona z grupowym działaniem wszystkich maszyn, razem z inteligencją natury oraz wszelkimi interakcjami, które powstaną w tym środowisku"[39], tworzące globalną matrycę, formę kształtującą złożone współzależności występujące pomiędzy elementami tego holos. W takiej konwergentnej strukturze będą zachodzić zjawiska w skali, której nie jesteśmy sobie dzisiaj w stanie wyobrazić. Ma to być „nowy reżim, w którym dzięki naszym wytworom staniemy się lepszymi ludźmi". Według Kevina Kelly'ego zmierzamy w kierunku coraz większej płynności, coraz intensywniejszego udostępniania i szerszego dostępu, bardziej rozbudowanego monitorowania i śledzenia, liczniejszych interakcji, nieograniczonego remiksowania i kopiowania, filtrowania, permanentnego korzystania z ekranów i totalnej kognifikacji przejawiającej się w wyposażeniu wszystkich przedmiotów w sztuczną inteligencję, co pozwoli człowiekowi stawać się innym człowiekiem w innym świecie[40]. Stephen Wolfram, brytyjski naukowiec specjalizujący się w fizyce cząstek elementarnych, automatach komórkowych i algebrze komputerowej, dostrzega nawet możliwość osiągnięcia przez człowieka w środowisku holos „efektywnej ludzkiej nieśmiertelności", która „nie wiadomo, czy osiągnięta zostanie biologicznie, czy cyfrowo, ale nastąpi nieuchronnie[41]. Podążając tokiem rozumowania wynalazcy, zastanowić się należy nad jego wizją, w której

> ludzką świadomość będzie się dało zamienić w postać cyfrową, w pełni zwirtualizowaną. Wkrótce będziemy mieli skrzynkę z bilionem dusz. Bilion dusz w skrzynce, wszystkie zwirtualizowane. W skrzynce będzie zachodziła komputacja molekularna – może

38 P. Polko, R. Polko, *Bezpiecznie już było. Jak żyć w świecie sieci, terrorystów i ciągłej niepewności*, Gliwice 2018, s. 126.
39 K. Kelly, dz. cyt., s. 404.
40 Tamże, s. 410.
41 S. Wolfram, *Sztuczna inteligencja i przyszłość cywilizacji*, [w:] *Człowiek na rozdrożu. Sztuczna inteligencja – 25 punktów widzenia*, red. J. Brockman, Gliwice 2020, s. 290.

> bazująca na biologii, może nie. Ale skrzynka będzie w stanie wykonywać wszelkiego rodzaju skomplikowane procesy (…) Uświadomienie sobie, że nie istnieje realna różnica między inteligencją a zwykłą komputacją prowadzi nas wizji takiej przyszłości – zwieńczenia naszej cywilizacji w postaci skrzynki z bilionem dusz (…) Jaki to będzie miało „cel"?[42].

Bezrefleksyjne podążanie w kierunku sztucznej inteligencji, zauroczenie jej możliwościami, nieprecyzyjne wyznaczenie celów dla superinteligentnych maszyn, które to cele stoją w konflikcie z naszymi, nieuchronnie mogą prowadzić do zagłady ludzkości. Stąd pytanie Alexa „Sandy" Pentlanda, profesora sztuk i nauk medialnych, jak chcemy wykorzystać nowe możliwości, które dostarcza nam analiza *big data*: czy dla dobra ludzkości czy przeciw niej? czy stworzymy nową, lepszą cywilizację, czy zniszczymy starą i nic nie zbudujemy? *Big data* pozwala człowiekowi po raz pierwszy w historii jego rozwoju zobaczyć szczegóły rynku i rewolucji politycznych oraz na ich podstawie przewidywać i kontrolować przebieg wydarzeń politycznych, ekonomicznych, społecznych itp. Pentland porównuje siłę możliwości wynikających z analizy *big data* do siły ognia prometejskiego, który można wykorzystać dla czynienia dobra lub zła. Wskazuje na potencjalne „zagrożenia ze strony systemów decyzyjnych, w których dane efektywnie przejmują władzę, a ludzka kreatywność zostanie zepchnięta na dalszy plan"[43]. W sytuacji tej postrzega konieczność tworzenia wielkich ekosystemów złożonych z ludzi i sztucznej inteligencji, opartych na modelach systemów stworzonych przez ludzi, w których powstała cyberkultura będzie sprawiała wrażenie ludzkiej i zapewni możliwość funkcjonowania nam jako ludziom. Stworzenie ludzkiej sztucznej inteligencji jest propozycją zespołu badawczego kierowanego przez Alexa Pentlanda obrony przed skutkami ubocznymi sztucznej inteligencji. W tym celu poszukuje on odpowiedzi na pytania: „w jaki sposób wybiera się kulturę w ewolucji, skoro reprodukują się jednostki? na jakiej podstawie wybierane są najlepsze kultury, najlepsze grupy, najlepsze jednostki, które przekazują geny? Odpowiedź na te pytania wymagała posiłkowania się tzw. próbkowaniem społecznym połączonym z osobistym osądem"[44]. Analiza zachowań ludzkich, sprawdzenie, które z nich są popularne w grupie osób do nas podobnych, oparte muszą być na wiarygodnych informacjach zwrotnych uzyskanych od przedstawicieli tej grupy, a te najczęściej obarczone są błędem wynikającym z wywierania wpływu przez dysponentów informacji (np. w formie reklamy, działań propagandowych, manipulacji, namnażania *fake news*). Niemniej metoda ta zasługuje na uwagę ze względu na możliwość podniesienia sprawności i inteligencji społeczeństwa dzięki stworzeniu „ludzko-sztucznej inteligencji" opartej na wiarygodnych danych i sprawiedliwej ocenie wynikającej z nich, nadzorowanej przez „ramy matematyczne, które są w stanie wykorzenić zjawiska radykalizacji poglądów i prób manipulowania nami"[45]. W konkluzji Pentland stwierdza, że mając kontrolę nad danymi, można kontrolować sztuczną inteligencję, ponieważ widoczne są dane wejściowe wykorzystywane przez AI i wyjściowe, co pozwala właściwie ocenić, jak postępuje sztuczna inteligencja. Podobnie można postępować w sytuacji kontroli społecznej

42 Tamże, s. 304.
43 A. Pentland, *Ludzka strategia*, [w:] *Człowiek na rozdrożu…*, s. 217.
44 Tamże, s. 219–220.
45 Tamże, s. 221.

w celu zmuszenia decydentów do odpowiedzialności. Potrzebujemy w tym celu wiarygodnych danych wejściowych dotyczących danej decyzji i wyników uzyskanych na ich podstawie umożliwiających wydanie obiektywnego sądu na temat podejmowanych przez nich aktywności. Jakość danych, ich wiarygodność, inteligentna analiza służy do demaskowania faktycznych celów stawianych sobie przez ludzi i sztuczną inteligencję oraz zapobiegania zagrożeniom, które mogą generować.

Bezpieczeństwo człowieka w środowisku ekstrakcji wielkich danych

Michael Miller bezpieczeństwo człowieka w czasach *big data* łączy z bezpieczeństwem osobistych danych pozyskiwanych przez Internet rzeczy i algorytmy służące do inwigilacji społeczeństwa oraz z bezpieczeństwem Internetu rzeczy jako całości[46]. Szczególnie ta druga sfera wymaga lepszych zabezpieczeń, aby każdy punkt sieci był godny zaufania. Najsłabiej chronione inteligentne urządzenia mogą stać się potencjalnym celem ataków i spowodować niewyobrażalne szkody. A takich słabych punktów wraz z rozwojem Internetu rzeczy będzie przybywać.

Bezpieczeństwo człowieka w środowisku ekstrakcji wielkich danych można sprowadzić za Katarzyną Jasińską do problemów związanych z:

1) nieuprawnionym wykorzystywaniem informacji, które związane jest ze zbieraniem i przetwarzaniem na masową skalę danych o osobach indywidualnych,
2) nadmierną komercjalizacją, która polega na intensyfikacji przekazu marketingowego we wszystkich dostępnych kanałach informacyjnych,
3) cyberzagrożeniami infrastruktury krytycznej, które obecnie utożsamiane są głównie z atakami hakerów,
4) kreowaniem fikcji, które sprowadza się do sterowania przekazem medialnym przez wszechobecne algorytmy decydujące, które informacje wyświetlić w sieci dla określonego użytkownika, i do przekazywania nieprawdziwych, szokujących informacji w celu wygenerowania fałszywego ruchu w sieci,
5) dyktaturą danych, czyli zjawiskiem, które pozwala korzystać z potencjału ukrytego w olbrzymich bazach danych do realizacji celów związanych z ugruntowaniem pozycji monopolowej lub władzy,
6) naruszaniem zasady sprawiedliwości i wolnej woli polegającym na możliwości stosowania zasady karania za określone skłonności,
7) przekazywaniem danych przez nieświadomych użytkowników, co jest konsekwencją małej wiedzy na temat wartości tych danych,
8) naruszaniem neutralności sieci, czyli traktowaniem użytkowników w różny sposób,
9) naruszaniem neutralności technologicznej polegającym na możliwości wykupienia priorytetowego trybu udostępnienia infrastruktury; informacyjny blackout, który stanowi przeciążenie urządzeń i łączy nadmierną ilością danych, i grozi zaburzeniem systemu, jeżeli infrastruktura danego państwa nie będzie w stanie obsłużyć krytycznego przepływu informacji,

46 M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016, s. 349.

10) pauperyzacją intelektualną, która polega na obniżeniu możliwości intelektualnych ludzi i w konsekwencji zastąpieniu pewnych czynności przez technologię, co prowadzi do zaniku zdolności analitycznych, skłonności do podejmowania ryzyka i zdominowania jednostki przez dyktat danych[47].

Słusznie zatem Cathy O'Neil stwierdza, że aby podjąć wyzwanie i zacząć rozwiązywać wymienione problemy, i przystąpić do działań naprawczych, „niezbędna jest wyobraźnia moralna oraz to coś, co posiadają jedynie istoty ludzkie. Musimy wprost umieszczać w naszych algorytmach wyższe wartości, tworząc w ten sposób modele *big data* wyczulone na kwestie etyczne"[48].

Jest to szczególnie ważne, w sytuacji gdy panuje przekonanie, jakoby formuły algorytmiczne były w pełni neutralne. Tymczasem każdy algorytm charakteryzuje się uprzedzeniami i błędami myślowymi ich twórców. Oznacza to, że te algorytmy mogą rządzić naszym życiem zgodnie z zamierzeniami ich autorów. Kto kontroluje algorytmy, ten ma władzę, ale kto to konkretnie jest, tego nie wiemy, gdyż stanowi to sekret firmy, państwa i innych podmiotów, które wykorzystują technologię opartą na algorytmach. Za Markiem Goodmanem warto sobie uświadomić, że algorytmy komputerowe rządzą światem i mamy z nimi kontakt podczas: algorytmicznego inwestowania na giełdzie, algorytmicznego wymiaru sprawiedliwości, algorytmicznej kontroli granicznej, algorytmicznej oceny wiarygodności kredytowej, algorytmicznej inwigilacji, algorytmicznej opieki zdrowotnej, algorytmicznej sztuki wojennej, a nawet algorytmicznego randkowania[49].

W tworzeniu prognoz rozwoju człowieka w cywilizacji technologicznej autorzy piszący o różnych wymienionych tu zagrożeniach pomijają fakt, że zwieńczeniem ich wszystkich jest uwikłanie człowieka w niekończącą się wojnę informacyjną, w której staje się on głównym celem wszelkich działań destrukcyjnych, manipulacyjnych, inwigilacyjnych, dezinformacyjnych. W wojnie tej gra toczy się o jego duszę, o zniewolenie umysłu niezdolnego do obrony przed agresorem wykorzystującym technologie *big data*, Internetu rzeczy, sztucznej inteligencji[50]. Jak więc przeciwstawić się dominacji inteligentnych technologii, jeżeli niszczona jest świadomość i psychika ludzi przez ludzi. Istnieje bardziej konkretny wróg, z którym należy podjąć walkę, niż sztuczna inteligencja. Są nim ludzie wykorzystujący technologię w celach niemających nic wspólnego z dobrem ludzkości. Marc Goodman, mając tego świadomość, uważa, że najlepszym sposobem przewidywania przyszłości jest jej wymyślanie i umieszczanie w modelach naprawczych elementów optymistycznych. Jego myśl końcowa zawiera przesłanie, że jeżeli

> uda nam się zmobilizować zwykłych obywateli i odzyskać pełnię kontroli nad naszymi urządzeniami i technologiami, będziemy mogli korzystać z tych narzędzi dla jak największego dobra wspólnego. (…) Lepsza wersja naszej przyszłości – ta której wszyscy

47 K. Jasińska, *Big data – wielkie perspektywy i wielkie problemy*, [w:] *Megatrendy i ich wpływ na rozwój sektorów infrastrukturalnych*, red. J. Gajewski, W. Paprocki, J. Pieriegud, Gdańsk 2015, s. 73–78.

48 C. O'Neil, dz. cyt., s. 275–276.

49 M. Goodman, *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, Gliwice 2016, s. 357–358.

50 H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Kraków 2019, s. 232–233.

pragniemy – nie pojawi się magicznie sama z siebie. Do jej wykreowania potrzebne są zamiar, wysiłek i walka[51].

Siłę przeciwdziałania niekorzystnym konsekwencjom oddziaływania cyfrowej cywilizacji na podmiot bezpieczeństwa dostrzeżono w informacyjnych komponentach kultury bezpieczeństwa, które opisano z perspektywy nauk o informacji i nauk o bezpieczeństwie[52]. Ich kształtowanie wymaga od człowieka świadomości, wysiłku i podjęcia walki o ich ukonstytuowanie się w społeczeństwie. Konieczność podjęcia systemowych działań związanych z zabezpieczeniem, ochroną i obroną człowieka zmuszonego żyć w środowisku nadmiaru informacji i niezrozumiałych algorytmów wymaga włączenia do tych działań komponentów kultury bezpieczeństwa, takich jak: kultura informacyjna, ekologia informacji, polityka informacyjna, kultura organizacyjna, kultura bezpieczeństwa informacyjnego. W przypadku kultury informacyjnej jej znaczącymi komponentami w budowie społecznego ładu informacyjnego są kompetencje informacyjne i medialne, edukacja informacyjna, dojrzałość informacyjna, wychowanie do informacji. Wszystkie one użyte w obronie człowieka przed negatywnymi skutkami nadmiarowości informacji wymagają aktywności człowieka i wysiłku potrzebnego na zapoznanie się z nimi oraz chęci i zrozumienia celu ich zastosowania. Świadomość podmiotowości bezpieczeństwa w obszarze zagrożeń cywilizacyjnych i możliwości ograniczenia ich wpływu jest ściśle związana z kulturą bezpieczeństwa. A ta wymaga od obywatela dojrzałości, czyli odpowiedzialności za siebie i innych. W środowisku informacyjnym jest to odpowiedzialność za:

1) jakość tworzonych i udostępnianych informacji,
2) zarządzanie informacją w zakresie indywidualnym i organizacyjnym,
3) podnoszenie swoich kompetencji informacyjnych, medialnych i technologicznych,
4) działania powstrzymujące powstawanie barier informacyjnych,
5) rozwój kultury dzielenia się informacją i wiedzą,
6) rozwój kompetencji komunikacyjnych,
7) rozwój Internetu jako dobra wspólnego,
8) rozwój świadomości informacyjnej,
9) rozwój ekoinfosystemu człowieka,
10) zrównoważony rozwój człowieka w sferach techniki i kultury,
11) przeciwdziałanie wykluczeniu cyfrowemu, technologicznemu, informacyjnemu,
12) budowę społecznego ładu informacyjnego,
13) ochronę infosfery jako środowiska życia człowieka,
14) kształtowanie postaw obywatelskich, partycypacyjnych, współuczestniczących,
15) bezpieczeństwo informacyjne w wymiarach osobistym, lokalnym i globalnym,
16) bezpieczeństwo medialne,
17) zwalczanie cyberzagrożeń i chorób informacyjnych,
18) walkę ze świadomym zniekształcaniem informacji i tworzeniem patogenów informacyjnych oraz celowym namnażaniem informacji[53].

51 M. Goodman, dz. cyt., s. 436.

52 H. Batorowska, *Przeciążenie informacyjne wyzwaniem dla kształtowania kultury bezpieczeństwa*, [w:] *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*, red. H. Batorowska, P. Motylińska, Warszawa 2020, s. 15–36.

53 H. Batorowska, *Nowe obszary badawcze w domenie kultury bezpieczeństwa z perspektywy nauki o informacji* [w:] *Bezpieczeństwo informacyjne…*, s. 61.

Względną wolność będą mogli zachować w tych nadchodzących czasach jedynie przedstawiciele wyspecjalizowanej technicznie elity, potrafiący unikać zastawionych na każdego obywatela sieci inwigilacji, potrafiący zarządzać swoją wiedzą dzięki wysublimowanym sprawnościom informacyjno-technologicznym oraz osoby o dużej inteligencji i wysokiej kulturze bezpieczeństwa informacyjnego[54].

Zakończenie

Odpowiedzi na postawione w artykule pytania nie są proste. Pomimo ogromnego zagrożenia ze strony przywołanych technologii i powszechnej zgody światowych ekspertów, że w starciu z niekontrolowaną sztuczną inteligencją inteligencja człowieka może przegrać, każda z przytoczonych książek nie kończy się pesymistycznie, dając czytelnikowi nadzieję na możliwość korzystania ze zdobyczy cywilizacji technologicznej zgodnie z celami stawianymi przez człowieka, a nie maszyny. Wszystko zależy od dokonanych przez nas wyborów i wykorzystania zdobyczy AI, *big data* i Internetu rzeczy dla dobra ludzkości. Wszyscy zaprezentowani autorzy prognoz pokładają wiarę w mądrość naszego gatunku i wybór jasnej strony cywilizacji technicznej, nie lekceważąc jej ciemnej strony. Wszyscy też wybór ten wiążą z edukacją ludzkości i rozwojem jej świadomości i dojrzałości. Według większości przewidywań ludzkość przetrwa, jeżeli znajdzie w sobie siłę do podejmowania działań chroniących prawo człowieka do prywatności, do równości, transparentności, jeżeli poczuje się współodpowiedzialne za jakość danych wprowadzanych do obiegu, będzie umiało nimi zarządzać, analizować je i wyciągać wnioski z tych analiz wolne od uprzedzeń, błędów, manipulacji, ignorancji i bylejakości. Do tej pory znajdowaliśmy taką siłę, ponieważ poza „złymi ludźmi" nikt nie mógł nam zagrozić. „Sztuczni ludzie" – superinteligentne roboty – mogą zmienić rozkład sił. A przecież nie potrzebujemy inteligentnych robotów, tylko sprawnych narzędzi ułatwiających pracę człowieka i wykorzystywanych do zwiększenia własnych możliwości intelektualnych oraz likwidacji nierówności, biedy, analfabetyzmu technologicznego. Dążmy do tego, aby osiągnąć stan inteligencji powszechnej, globalnej dla ludzi, a nie sztucznej inteligencji dla robotów. Nie obdarzajmy ich inteligencją, skoro tylu jeszcze ludzi jej nie posiada w wystarczającym stopniu. Starajmy się zapewnić całej populacji możliwość przejścia na wyższy poziom rozwoju cywilizacji ludzkiej inteligencji odpowiedzialnej za bezpieczeństwo Ziemi i jej mieszkańców.

Bibliografia

Angwin J., *Społeczeństwo inwigilowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, Warszawa 2017.

Assange J., Appelbaum J., Müller-Maguhn, Zimmermann J., *Cypherpunks. Wolność i przyszłość internetu*, Gliwice 2013.

54 J. Assange, J. Appelbaum, Müller-Maguhn, J. Zimmermann, *Cypherpunks. Wolność i przyszłość internetu*, Gliwice 2013, s. 164.

Batorowska H., Klepka R., Wasiuta O., *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Kraków 2019.
Bauman Z., Lyon D., *Płynna inwigilacja. Rozmowy*, Kraków 2013.
Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji, red. H. Batorowska, P. Motylińska, Warszawa 2020.
Bostrom N., *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016.
Carr N., *Płytki umysł. Jak Internet wpływa na nasz mózg*, Gliwice 2012.
Człowiek na rozdrożu, Sztuczna inteligencja – 25 punktów widzenia, red. J. Brockman, Gliwice 2020.
Gołębiewski Ł., *Książka/book. Szerokopasmowa kultura*, Warszawa 2009.
Gołębiewski Ł., *Śmierć książki. No future book*, Warszawa 2008.
Goodman M., *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, Gliwice 2016.
Jasińska K., *Big data – wielkie perspektywy i wielkie problemy*, [w:] *Megatrendy i ich wpływ na rozwój sektorów infrastrukturalnych*, red. J. Gajewski, W. Paprocki, J. Pieriegud, Gdańsk 2015, s. 56–81.
Jenkins H., *Kultura konwergencji. Zderzenie starych i nowych mediów*, Warszawa 2007.
Kelly K., *Nieuniknione. Jak inteligentne technologie zmienią naszą przyszłość*, Warszawa 2017.
Kerckhove D., *Inteligencja otwarta. Narodziny społeczeństwa sieciowego*, Warszawa 2001.
Leśniak-Moczuk K., *Społeczeństwo równości czy zniewolone danetyzacją*, „Nierówności Społeczne a Wzrost Gospodarczy" 2017, nr 52 (4).
Materska K., *Zarządzanie informacją w warunkach wiedzy niedoskonałej*, [w:] *Zarządzanie informacją*, red. W. Babik, Warszawa 2019, s. 338–354.
Mayer-Schönberger V., Cukier K., *Big data efektywna analiza danych. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa 2017.
Miller M., *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016.
O'Neil C., *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówność i zagrażają demokracji*, Warszawa 2017.
Polko P., Polko R., *Bezpiecznie już było. Jak żyć w świecie sieci, terrorystów i ciągłej niepewności*, Gliwice 2018.
Schneier B., *Dane i Goliat. Ukryta bitwa o Twoje dane i kontrolę nad światem*, Gliwice 2017.
Silver N., *Sygnał i szum. Sztuka prognozowania w erze technologii*, Gliwice 2014.
Wolfram S., *Sztuczna inteligencja i przyszłość cywilizacji*, [w:] *Człowiek na rozdrożu. Sztuczna inteligencja – 25 punktów widzenia*, red. J. Brockman, Gliwice 2020.
Wójcik M., *Rozszerzona rzeczywistość w usługach informacyjnych bibliotek*, Kraków 2018.
Zych J., *Teleinformatyka dla bezpieczeństwa 2.0*, Poznań 2019.

An overview of researchers' visions for human security and survival in the age of big data and artificial intelligence

Abstract

Big Data is the subject of research of many specialists, including IT specialists, data librarians and data researchers, data brokers, analytical and information services, and even artists. This new method of data mining causes changes in all areas of human life; thus, we have on our hands a tool that can be used for people's good and security, but which can also destroy

our civilization. These two possibilities inspire researchers to make predictions about a future dominated by artificial intelligence, the Internet of Things, and new ways of extracting data from Big Data that allows them to predict and control these objects by seeing correlations between them. This gives unlimited power to data silo holders and algorithms. The article presents scientists' fears about the threats generated by these technologies and formulates them as questions about the condition of humanity in the future. The consequences of creating forecasts without considering human deficiencies in analyzing data and the perils of creating incomplete knowledge are also presented. Forecasting requires the ability to analyze and conduct intelligent interpretation through people, not just artificial intelligence systems. Forecasting also requires the ability to ask questions, which is clearly the domain of man.

Keywords: Big data, forecasting, data management, artificial intelligence, Internet of Things, security, information security culture.