©Wydawnictwo UR 2019 „Edukacja – Technika – Informatyka" nr 2/28/2019
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2019.2.32

EUNIKA BARON-POLAŃCZYK

Boty, trolle i fake news – uważaj, kto cię uczy!

Bots, Trolls and Fakenews – Watch Out Hho Teaches You!

ORCID: 0000-0002-8163-5491, doktor habilitowany profesor UZ, Uniwersytet Zielonogórski, Wydział Mechaniczny, Zakład Profesjologii, Polska

Streszczenie

Artykuł prezentuje wyniki badań internetu, a szczególnie mediów społecznościowych, dotyczących manipulowania informacją, wpływania na podejmowanie decyzji oraz propagowania nieprawdziwych i społecznie szkodliwych treści. Opisuje sposoby wykorzystywania internetowych botów i trolli oraz ich hybrydowych połączeń do celowego kształtowania dyskursu społecznego. Kolejny omawiany problem to bardzo łatwe i szybkie szerzenie nieprawdy w postaci propagowania *fake news* w internecie. W procederze tym bardzo istotną rolę odgrywa czynnik ludzki. Biorąc pod uwagę nierozerwalne osadzenie współczesnej edukacji rozumianej jako proces permanentny i całożyciowy w ICT, podkreśla znaczenie kształtowania świadomych i odpowiedzialnych postaw wszystkich uczestników tego procesu wobec nowych technologii.

Słowa kluczowe: ICT, edukacja, manipulowanie informacją, fałszywe wiadomości

Abstract

The article presents the results of research of the Internet and especially social media, concerning the manipulation of information, influencing decision-making and the propagation of untruthful and socially harmful content. Describes how online bots and trolls, and their hybrid connections are used to deliberately shape social discourse. The next discussed problem is very easy and quick spreading untruth in the form of propagating fake news on the Internet. Human factor plays a very important role in this proceder. Considering the inseparable embedding of modern education – understood as a permanent and lifelong process – in ICT, it underlines the importance of shaping conscious and responsible attitudes of all participants in this process towards new technologies.

Keywords: ICT, education, information manipulation, fake news

Wstęp

Trudno wyobrazić sobie współczesną edukację bez różnorodnych form wykorzystania ICT (*Information and Communication Technologies*). Stanowią one bez wątpienia wartościowe narzędzie poznawcze, które towarzyszy nam w cza-

sie nauki, pracy i zabawy. Można nawet stwierdzić, że przenikając przez wszystkie formy aktywności człowieka, jest ono immanentne dla zachodzących obecnie procesów edukacyjnych. Znajduje to bezpośrednie odzwierciedlenie we współczesnych teoriach formowania wiedzy, szczególnie w kognitywizmie, konstruktywizmie i konektywizmie. Zwłaszcza ta ostatnia, wciąż budząca kontrowersje teoria wydaje się najlepiej opisywać proces uczenia się w środowisku sieciowym. W dokumencie *Connectivism: A Learning Theory for the Digital Age* Siemens (2008) nakreślił główne tezy konektywizmu: 1) uczenie się i wiedza opierają się na różnorodności opinii; 2) uczenie się jest procesem łączenia z określonymi węzłami lub zasobami informacji; 3) wiedza może być gromadzona poza człowiekiem, w różnych urządzeniach; 4) zdolność, by wiedzieć więcej, jest ważniejsza niż to, co aktualnie wiemy; 5) tworzenie i utrzymywanie połączeń jest niezbędnym elementem ułatwiającym proces ustawicznego uczenia się; 6) zdolność do dostrzegania połączeń pomiędzy obszarami, ideami i koncepcjami jest umiejętnością krytyczną; 7) wiedza, która potrzebna jest w danym momencie (dokładna i aktualna), leży u podstaw konektywnej czynności uczenia się; 8) proces podejmowania decyzji sam w sobie jest już procesem uczenia się; 9) wybór, czego się uczyć, i znaczenie napływających informacji jest postrzegane przez pryzmat zmieniającej się rzeczywistości; 10) odpowiedź poprawna dzisiaj może być błędna jutro w wyniku zmian środowiska informacyjnego wpływającego na decyzję.

Jednym z najważniejszych aspektów konektywizmu jest wykorzystanie sieci z jej różnymi węzłami (węzeł oznacza tu coś więcej niż zasób, źródło) i połączeniami jako centralnej metafory procesu uczenia się. Uczenie się jest procesem tworzenia połączeń pomiędzy różnymi węzłami i rozwijania sieci. Oczywiście nie wszystkie połączenia mają jednakową moc w uczeniu się i w rzeczywistości wiele z nich ma charakter luźny, słaby. W epoce cyfrowej proces uczenia się nie może być w pełni kontrolowany. Istotne znaczenie ma tutaj nieformalne uczenie się – wykonywanie zadań związanych z pracą, uczestnictwo w społecznościach, rozwijanie sieci kontaktów osobistych. Istotę stanowi społeczno-kulturowy kontekst poznania, gdzie podstawową jednostką jest nie indywidualny podmiot, lecz wspólnota poznająca (Baron-Polańczyk, 2015, s. 33–41).

Z punktu widzenia nauk kognitywnych procesy edukacyjne wspierane przez ICT są ze swej natury samoregulujące, permanentne, całożyciowe, ale także przypadkowe i płytkie. Jednocześnie edukacyjne zastosowania ICT niosą ze sobą wiele zagrożeń. Nie chodzi tu wyłącznie o szeroko rozumianą cyberprzestępczość. Równie groźne jest szerzenie fałszu i socjotechniczna manipulacja służąca wywieraniu wpływu na podejmowane decyzje oraz propagowaniu szkodliwych społecznie idei (np. nacjonalizmu, ksenofobii, rasizmu, faszyzmu). Nadużycia te są często robione w „białych rękawiczkach", przez co trudniejsze

do zidentyfikowania i prawidłowej oceny. Stąd tak istotne jest formowanie świadomej i odpowiedzialnej postawy uczestników procesu całożyciowej edukacji wobec nowych technologii (Baron-Polańczyk, 2018, s. 72–88).

To ja, bot – skąd się wziąłem?

Początek 2018 r. przyniósł wiele nowych faktów, które wydają się potwierdzać do niedawna mało wiarygodne opinie zwolenników teorii spiskowych mediów cyfrowych. Jedną z głównych głoszonych przez nich tez było manipulowanie za pomocą mediów społecznościowych elektoratem i wpływanie na wyniki referendum w sprawie Brexitu, wyborów prezydenckich w Stanach Zjednoczonych w 2016 r., wyborów prezydenckich we Francji i parlamentarnych w Niemczech w 2017 r. Badacze z Oxford Internet Institute podkreślają, że internet z pewnością zakłócił nasze rozumienie, czym może być komunikacja, kto ją prowadzi i w jakim celu (Woolley, Howard, 2016, s. 4882–4890). Większość komunikacji cyfrowej nie przebiega już między ludźmi, ale między urządzeniami wokół ludzi poprzez tzw. internet rzeczy (IoT – *Internet of Things*). Jak potwierdzają publikowane corocznie raporty zespołu CERT (Computer Emergency Response Team) działającego w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej), prognozowane zagrożenia ze strony internetu rzeczy stały się faktem. Okazało się, że nie trzeba mieć komputera, aby stać się ofiarą cyberprzestępcy lub narzędziem w jego rękach. Największe w historii ataki paraliżujące działanie globalnych korporacji (np. Reddit, Spotify czy „The New York Times") zostały dokonane przy użyciu tysięcy zwykłych kamer internetowych, domowych nagrywarek DVR (*Digital Video Recorder*) lub routerów należących do nieświadomych użytkowników. Wykorzystując przy tym słabe zabezpieczenia urządzeń lub jego zupełny brak. Ataków paraliżujących internet (DDoS – *Distributed Denial of Service*) poprzez rekordowy poziom generowanego ruchu dokonywały tzw. boty (*Krajobraz*…, 2018). Nazywają tak swoje produkty, które służą do automatyzacji działań w sieciach społecznościowych lub urządzeniach sieciowych, programiści i zaawansowani użytkownicy systemów sieciowych oraz hakerzy i cyberprzestępcy.

Bot internetowy, znany również jako robot sieciowy (*botnet*), robot WWW lub po prostu bot, to aplikacja, która uruchamia zautomatyzowane zadania (skrypty) w internecie. Zazwyczaj boty wykonują zadania, które są zarówno proste, jak i strukturalnie powtarzalne w zastępstwie człowieka i w tempie o wiele wyższym, niż byłoby to możliwe dla człowieka. Czasem ich funkcją jest udawanie ludzkiego zachowania. Największe wykorzystanie botów występuje w tzw. *web spidering* (*web crawler*), w którym zautomatyzowany skrypt pobiera, analizuje i zapisuje informacje z serwerów sieciowych wielokrotnie szybciej od człowieka. Ponad połowa całego ruchu internetowego jest generowana przez boty, które żmudnie zbierają informacje w internecie, monitorują witryny cza-

tów, wychwytując przypadki niewłaściwego użycia, i indeksują finansowe bazy danych, śledząc rynkowe trendy (*Internet bot*…, 2018). Wykonują również przydatne społecznie funkcje, takie jak rozpowszechnianie wiadomości i publikacji czy koordynowanie działań wolontariuszy – ale jest też ciemna strona, ponieważ mogą wspierać „złośliwe" zastosowania, takie jak np. promowanie propagandy terrorystycznej, rasistowskiej, faszystowskiej oraz rekrutacja do tych działań. Istnieją także interaktywne boty „zorientowane politycznie". Gracze polityczni wykorzystują technologicznych reprezentantów w postaci zastrzeżonych algorytmów i półautomatycznych graczy społecznych – politycznych botów – w subtelnych próbach manipulowania opinią publiczną. Narzędzia te mogą być również wykorzystywane do sterowania społeczeństwem, ale sposób, w jaki działają, by zapewnić sobie kontrolę nad interakcją i organizacją, może być nieprzewidywalny nawet dla ich twórców. Iteracyjna budowa skryptów komputerowych oraz olbrzymia liczba możliwych iteracji oraz wielość ścieżek przebiegu w grafie sieci sprawia, że wyniki działania algorytmu mogą być nieprzewidywalne zarówno dla programistów, jak i odbiorców. Jak piszą Woolley i Howard (2016, s. 4882–4890), „autonomiczne programy są często wykorzystywane jako przedstawiciele graczy politycznych, którzy chcą mieć wpływ na opinię publiczną poprzez szerzenie propagandy i dezinformacji. Badanie, w jaki sposób algorytmy i automatyzacja porządkują nasze życie, jest kolejnym wielkim wyzwaniem dla nauk społecznych, ponieważ takie badania obejmują oszałamiającą grupę graczy, artefaktów i kodu w złożonych sieciach przyczynowości". Wspomniana kampania prezydencka za oceanem pokazała, że boty stają się nową, nietypową bronią w politycznej rozgrywce. Trudno znaleźć je wśród prawdziwych użytkowników, ponieważ wyrafinowane boty świetnie imitują ludzkie zachowania, używając językowych algorytmów w rozmowach z innymi użytkownikami, komentując posty i odpowiadając na pytania.

Badania przeprowadzone przez zespół cytowanego już profesora Howarda z Uniwersytetu w Oxfordzie w ramach szerszego projektu odkrywającego „obliczeniową propagandę" (*computational propaganda*) wykazały, że podczas pierwszej amerykańskiej debaty prezydenckiej ponad cztery razy więcej tweetów zostało wygenerowanych przez zautomatyzowane konta na korzyść Donalda Trumpa, porównując z tymi popierającymi Hillary Clinton (Silva, 2018). Konto na Twitterze zostawało uznane za bota, jeśli tweetowało ponad 50 razy dziennie przez cztery dni. Badacze twierdzą, że większość prawdziwych użytkowników nie dochodzi do liczby 50 tweetów dziennie. Przeprowadzona analiza wykazała, że boty stały za około 580 tys. z blisko 1,8 mln tweetów opowiadających się za Trumpem. W przypadku Clinton proporcje wynosiły 123 tys. botowych tweetów spośród blisko 613 tys. Liczba tweetów jest jednak tylko jednym ze sposobów na identyfikację botów i nie wszyscy badacze podzielają adekwatność tej metody, zważywszy na fakt, że granica między ludzkim a botowym zachowaniem jest coraz bardziej rozmyta.

Dowiedli tego w swoich badaniach naukowcy z Uniwersytetu Południowej Kalifornii i Uniwersytetu Indiany. Opracowali i przetestowali platformę wykrywania botów na Twitterze, wprowadzili system uczenia maszynowego, który wyodrębnia ponad tysiąc funkcji w sześciu różnych klasach z publicznych danych i metadanych o użytkownikach: znajomi, treść i zabarwienie światopoglądowe tweetów, szablony (wzorce) sieciowe i przebieg czasów aktywności. Sklasyfikowali 14 mln kont aktywnej anglojęzycznej populacji na Twitterze, ustalając optymalne wyniki progowe, które dzielą konta ludzi i botów dla kilku modeli z różnymi mieszankami prostych i wyrafinowanych botów. Uzyskane wyniki badań pozwalają oszacować udział bota na 9–15% całej populacji. Badacze wskazują również na znaczenie śledzenia coraz bardziej wyrafinowanych botów, ponieważ technologie oszustwa i wykrywania są niekończącym się wyścigiem zbrojeń (Varol, Ferrara, Davis, Menczer, Flammini, 2017). Przyjmując te szacunki za wiarygodne, można stwierdzić, że spośród około 319 mln aktywnych użytkowników Twittera nawet 48 mln kont może należeć do botów zdolnych do interakcji (*like, retweet, follow*).

Z pewnością boty stają się coraz bardziej znaczącą częścią mediów społecznościowych. W politycznej sferze boty nadają kształt opinii publicznej – często prowadząc do błędów i dysproporcji. Niezależni badacze zaczynają obnażać warstwy ingerencji politycznych. Według Ferrara, uczestnika badań z Uniwersytetu Południowej Kalifornii, około 400 tys. botów zamieszczało wiadomości polityczne podczas wyborów prezydenckich w Stanach Zjednoczonych na Twitterze. Ta sama grupa 1600 botów tweetujących ekstremistyczne prawicowe treści w wyborach w USA również ujawniła nastroje „anty-Macron" podczas wyborów prezydenckich we Francji i głosiła ekstremistyczne prawicowe treści podczas wyborów niemieckich w 2017 r. (Wang, 2018).

Pomimo zwrócenia bacznej uwagi dokładne rozmiary społeczności botów na Twitterze pozostają nieprzejrzyste. Naukowcy bezskutecznie prosili firmę Twitter o współpracę przy badaniach, ponieważ bez wewnętrznych danych Twittera nie są w stanie ustalić pochodzenia i kontrolowania ujawnionych botów, które rozsyłają tweety motywowane politycznie. Stworzenie algorytmów pozwalających wyszukać złośliwe tweety jest bardzo trudne. Manipulatorzy stosują działania hybrydowe, uzupełniają swoje sieci botów ludźmi, którym płacą za skoordynowane rozsyłanie wiadomości w tym samym czasie. Algorytmy Twittera mogą mieć wówczas trudności z wykryciem różnic. Ostateczne rozprawienie się z botami oraz współpraca w tym celu z naukowcami może nie do końca leżeć w interesie Twittera, gdyż postawi go w trudnej sytuacji na Wall Street. Inwestorzy wyceniają firmę na podstawie miesięcznej bazy aktywnych użytkowników, a pozbycie się fałszywych kont i botów z pewnością znacznie ją zmniejszy.

W kontekście toczących się dyskusji na temat roli i natury botów ośrodek Pew Research Center postanowił zbadać, jak wiele linków udostępnianych na Twitterze – z których większość odnosi się do strony spoza samej platformy – jest promowanych przez boty zamiast ludzi. W tym celu Centrum wykorzystało listę 2315 najpopularniejszych stron internetowych i zbadało około 1,2 mln tweetów (wysłanych przez użytkowników w języku angielskim), które zawierały linki do tych witryn w okresie około 6 tygodni latem 2017 r. Wyniki ilustrują wszechobecność automatycznych kont w rozpowszechnianiu linków do wielu popularnych stron na Twitterze (Wojcik, Messing, Smith, Rainie, Hitlin, 2018). Badacze szacują, że 2/3 linków z tweetem do popularnych stron internetowych jest publikowanych przez konta automatyczne – a nie ludzi.

Fake news – dlaczego prawda jest nudna?

Boty odgrywają również bardzo istotną rolę w rozsyłaniu tzw. *fake news*, nieprawdziwych lub niesprawdzonych informacji wprowadzających w błąd odbiorców. Termin *fake news* to neologizm w języku angielskim dosłownie znaczący fałszywe wiadomości. Odnosi się on do informacji, które nie mają pokrycia w rzeczywistości, jednak mimo to są przedstawiane jako prawdziwe w wiadomościach bądź portalach społecznościowych (Allcott, Gentzkow, 2017, s. 211–236). Jak pokazują jednak najnowsze badania, boty nie są największym nosicielem *fake news* w internecie.

Raport z projektu badawczego prowadzonego przez MIT (Massachusetts Institute of Technology) (Vosoughi, Roy, Aral, 2018, s. 1146–1151) – podczas którego naukowcy prześledzili około 126 tys. kaskad wiadomości rozsiewanych na Twitterze, które zostały w sposób skumulowany przekazane ponad 4,5 mln razy przez około 3 mln osób w latach 2006–2017 – udowodnił, że to ludzie, a nie boty są głównie odpowiedzialni za rozpowszechnianie wprowadzających w błąd informacji. Badania ustaliły również, że fałszywe wiadomości rozprzestrzeniają się zdecydowanie szybciej na portalu społecznościowym Twitter niż wiadomości prawdziwe. Fałsz rozprzestrzenia się znacznie dalej, szybciej, głębiej i szerzej niż prawda we wszystkich kategoriach informacji, a w wielu przypadkach o rząd wielkości. Badanie dostarcza różnych sposobów kwantyfikacji tego zjawiska: np. prawdopodobieństwo ponownego wysłania fałszywych wiadomości jest o 70% wyższe niż prawdziwych. Czas potrzebny na dotarcie prawdziwych historii do 1500 osób jest około sześć razy dłuższy niż w przypadku fałszywych. Jeśli chodzi o „kaskady" na Twitterze lub nieprzerwane łańcuchy *retweet*, fałsz osiąga kaskadową głębokość od około 10 do 20 razy szybciej niż fakt. Kłamstwa przekazywane są przez unikatowych użytkowników szerzej niż prawdziwe stwierdzenia na każdej głębokości kaskady (Dizikes, 2018).

Nasuwa się podstawowe pytanie: dlaczego fałsz rozprzestrzenia się szybciej niż prawda? Badacze sugerują, że odpowiedź może tkwić w ludzkiej psychice:

lubimy nowe rzeczy. Fałszywe wiadomości są bardziej nowatorskie, a ludzie częściej dzielą się nowymi informacjami. W sieciach społecznościowych osoby, które dzielą się nowymi informacjami, są postrzegane jako lepiej poinformowane. Problem z pewnością jest bardziej złożony, ponieważ niektórzy ludzie celowo rozpowszechniają fałszywe wiadomości, podczas gdy inni robią to zupełnie nieświadomie. Teraz pojawia się kolejny ważne zadanie dla nauk społecznych i edukacji – to walka z rozpowszechnianiem fałszu. Gdyby robiły to wyłącznie boty, być może wystarczyłaby w tym celu jedynie technologia. Naukowcy z MIT twierdzą, że jest możliwe, że to samo zjawisko występuje na innych platformach mediów społecznościowych, w tym na Facebooku (FB), ale podkreślają, że potrzebne są dokładne badania dotyczące tego i innych powiązanych pytań.

To ja, troll – zgadnij kim jestem?

Udział w procederze manipulowania użytkownikami FB mają również fałszywe konta należące do internetowych trolli działających często w większych, sterowanych z zewnątrz strukturach nazywanych farmami trolli. Troll internetowy to osoba, która sieje niezgodę w internecie – wywołuje kłótnie lub denerwuje użytkowników społeczności internetowych (takich jak grupy i fora dyskusyjne, chaty, blogi) – poprzez zamieszczanie treści kontrowersyjnych, napastliwych, obcych, również nieprawdziwych lub nie na temat w celu skłonienia czytelników do emocjonalnych reakcji zakłócających rzeczową dyskusję, często dla zabawy trolla. Istnieje kilka konkurencyjnych teorii wyjaśniających etymologię słowa *troll* w kontekście internetu – od rozpowszechnienia tego słowa przez użytkowników BBS i UseNet we wczesnych latach 80. ubiegłego wieku, poprzez wywodzenie od staronordyckiego słowa *troll* oznaczającego giganta lub demona, a w skandynawskim folklorze i bajkach: antyspołeczne, kłótliwe i powolne stworzenia, które utrudniają życie podróżnikom, do wykorzystania słowa *trolling* we współczesnym języku angielskim opisującego technikę połowu polegającą na powolnym przeciąganiu wabika lub haczyka z przynętą z poruszającej się łodzi (*Internet troll*…, 2018). Zarówno rzeczownik *troll*, jak i pochodzący od niego polski czasownik *trollowanie* (*trolling*) opisujący działania internetowego trolla jest nie tylko związany z dyskursem internetowym, ale w ostatnich latach został przez media upowszechniony i utożsamiony z różnymi formami nękania online.

Aktywność na Facebooku rosyjskiej farmy trolli wyszła na jaw po raz pierwszy we wrześniu 2017 r. To wtedy koncern zdecydował się publicznie poinformować o usunięciu kont należących do zlokalizowanej w Petersburgu w Rosji, działającej na rzecz Kremla organizacji IRA (Internet Research Agency). Farma trolli była domem dla setek pracowników opłacanych za publikowanie komentarzy do artykułów czy postów na blogach, którzy na różne sposoby usiłowali wpływać na polityczne debaty w mediach społecznościowych. W kwiet-

niu 2018 r. szef bezpieczeństwa Facebooka, Alex Stamos, ponownie poinformował, że koncern usunął 70 kont z serwisu i 65 na należącym do firmy Instagramie. Wszystkie usunięte konta wykorzystywane były przez IRA do wywierania wpływu podczas kampanii prezydenckiej w Stanach Zjednoczonych z 2016 r. Internet ResearchAgency wydała około 167 tys. dolarów na reklamę na Facebooku i Instagramie od stycznia 2015 r. Ofiarami kremlowskiej farmy trolli padło ponad milion osób korzystających z Facebooka, które w serwisie stykały się z propagandowymi treściami.

Jak pisze na swoim blogu Stamos (2018), „IRA wielokrotnie używała kompleksowych struktur złożonych z połączonych ze sobą, fałszywych kont, które manipulowały użytkownikami Facebooka przed, podczas i po wyborach prezydenckich z 2016 r. Właśnie dlatego nie chcemy ich w serwisie". Dodał również, że „źli gracze, którzy chcą nadużywać Facebooka – zawsze zmieniają swoją taktykę, aby ukryć się przed zespołem bezpieczeństwa, który będzie nadal z nimi walczył, angażując coraz więcej ludzi i lepszą technologię, aby stale poprawiać bezpieczeństwo na Facebooku" (Stamos, 2018). Fałszywe konta trolli w połączeniu z często wyrafinowanymi algorytmami botów są najczęściej wykorzystywane w zmasowanych atakach socjotechnicznych. Tego typu hybrydy są najtrudniejsze do zidentyfikowania i prawidłowego zakwalifikowania przez badaczy tych zjawisk i specjalistów od bezpieczeństwa.

Podsumowanie

Opisane przykłady obnażają pojawiające się ciągle nowe zagrożenia, które niesie internet, a zwłaszcza media społecznościowe. Wspomniani we wstępie zwolennicy teorii spiskowych polityki i dziejów cywilizacji mogą śmiało stwierdzić: „A nie mówiliśmy!". Z tymi wszystkimi wyzwaniami i zagrożeniami współczesności musi zmierzyć się system edukacji formalnej i pozaformalnej. Na wczesnych etapach życia i kształcenia kluczowa wydaje się rola rodziców i nauczycieli w procesie wychowania do nowych technologii. Muszą oni sami wiedzieć, w jaki sposób kształtować postawy dzieci i młodzieży wobec technologii, które stały się tanie i powszechnie dostępne. Dzieci mają mobilne urządzenia z dostępem do internetu od najmłodszych lat, mogą nie tylko oglądać dowolne treści, ale również je tworzyć i udostępniać. Wielu rodziców swój obowiązek ogranicza do zaspokojenia materialnej potrzeby dziecka – zakupu komputera lub smartfona, lekceważąc fakt, jak potężne i niebezpieczne jest to narzędzie. Być może sami nie mają wystarczającej wiedzy i umiejętności w tym zakresie. Tym ważniejsza jest więc rola nauczycieli, którzy powinni pełnić funkcję przewodników po cyfrowym świecie, a w te kompetencje musi ich wyposażyć współczesny system kształcenia i doskonalenia nauczycieli.

W epoce mediów cyfrowych osoby, które uczą się, pracują lub oddają rozrywce, spędzają godziny przed monitorem komputera i nie rozstają się ze smart-

fonem, tabletem lub notebookiem. Przez to są nieustannie narażone nie tylko na wszystkie przejawy przestępczości komputerowej, ale również na informacyjny fałsz i manipulację. Nieumiejętność lub ignorowanie oceny wartości i źródła pochodzenia informacji wydaje się tu zagadnieniem kluczowym. Konieczne jest wykreowanie szczególnej wrażliwości, gdyż nikt nigdy i nigdzie nie ma pewności, kto kryje się za atrakcyjnie i przyjaźnie brzmiącym nickiem. Może się okazać, że wiedzę czerpiemy z bezmyślnie powielanych *fake news*, a nasze poglądy i postawy kształtuje troll lub bot oparty na wysublimowanym algorytmie. W ten sposób wpadamy w tzw. bańki informacyjne, redukując możliwości własnego poznania.

Literatura

Allcott, H., Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, *31*, 211-236.

Baron-Polańczyk, E. (2015). ICT – kulturowo wartościowe narzędzie kognitywne (w kontekście konstruktywizmu społeczno-kulturowego). *Edukacja – Technika – Informatyka*, *3*(13), 33-41.

Baron-Polańczyk, E. (2018). *My i Oni. Uczniowie wobec nowych trendów ICT*. Zielona Góra: Wyd. UZ.

Dizikes, P. (2018). *Study: On Twitter, False News Travels Faster than True Stories*. Pobrane z: http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 (20.04.2018).

Internet bot. Pobrane z: https://en.wikipedia.org/wiki/Internet_bot (6.04 2018).

Internet troll. Pobrane z: https://en.wikipedia.org/wiki/Internet_troll (28.04.2018).

Krajobraz bezpieczeństwa polskiego Internetu w 2016 roku. Raport roczny z działalności CERT Polska. Pobrane z: https://www.cert.pl/publikacje/ (6.04 2018).

Siemens, G. (2008). Connectivism: A Learning Theory for the Digital Age. *International Journal of Instructional Technology and Distance Learning*, *2*(1). Pobrane z: http://www.elearnspace.org/Articles/connectivism.htm (15.04.2018).

Silva, S. (2018). *Trump's Twitter debate lead was 'Swelled by Bots'*. BBC News. Pobrane z: www.bbc.com/news/technology-37684418 (8.04.2018).

Stamos, A. (2018). *Authenticity Matters. The IRA Has no Place on Facebook*. Pobrane z: https://newsroom.fb.com/news/2018/04/authenticity-matters/ (3.05.2018).

Varol, O., Ferrara, E., Davis, C.A., Menczer, F., Flammini, A. (2018). *Online Human-Bot Interactions: Detection, Estimation, and Characterization*. Accepted paper for ICWSM' 2017. Pobrane z: https://arxiv.org/pdf/1703.03107.pdf (8.04.2018).

Vosoughi, S., Roy, D., Aral, S. (2018). The Spread of True and False News Online. *Science*, *359*(6380), 1146-1151.

Wang, S. (2018). *Twitter Is Crawling with Bots and Lacks Incentive to Expel Them*. Pobrane z: https://www.bloomberg.com/news/articles/2017-10-13/twitter-is-crawling-with-bots-and-lacks--incentive-to-expel-them (8.04 2018).

Wojcik, S., Messing, S., Smith, A., Rainie, L., Hitlin, P. (2018). *Bots in the Twittersphere*. Pew Research Center. Pobrane z: http://www.pewinternet.org/2018/04/09/bots-in-the-twittersphere/ (12.04.2018).

Woolley, S.C., Howard, P.N. (2016). Political Communication, Computational Propaganda, and Autonomous Agents – *Introduction*. *International Journal of Communication*, *10*, 4882-4890.