Eunika BARON-POLAŃCZYK

Algorytmy vs prawo – uważaj, jak się uczysz!

Algorithms vs law – watch out how you learn!

Słowa kluczowe: ICT, edukacja, manipulowanie informacją, profilowanie osobowości, źródła wiedzy.

Key words: ICT, education, manipulation of information, profiling personality, sources of knowledge.

Abstract. The article presents an overview of the latest foreign and national media reports on research of the Internet, and especially social media. It addresses the problems of manipulation of information, user profiling and the propagation of untruthful and socially harmful content. In the face of the threats described, it indicates the necessity for the owners of portals to accept responsibility for the presented content and not only for the technical and functional aspects of the operation of these portals. Imposing appropriate legal regulations may enforce this process, but at the same time limit the freedom of the Internet. The text emphasizes the importance of shaping conscious and responsible attitudes of all participants in the education process towards new technologies. Well-established axiological competencies are a necessary complement to instrumental competences, and their combination is a guarantee of valuable use of ICT in lifelong learning.

Wprowadzenie. Początek 2018 roku przyniósł wiele nowych medialnych doniesień, które obnażają skalę społecznych nadużyć w Internecie, a zwłaszcza mediach społecznościowych. Udowodniono manipulowanie za pomocą mediów społecznościowych elektoratem i wpływanie na wyniki referendum w sprawie Brexitu, wyborów prezydenckich w USA w roku 2016, wyborów prezydenckich we Francji i parlamentarnych w Niemczech w 2017. Dużą rolę odegrały w tym procederze tak zwane boty, specjalizowane aplikacje, która wykonują zautomatyzowane zadania 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. „Boty społecznościowe" – zautomatyzowane konta, które umożliwiają publikowanie treści lub interakcje z innymi użytkownikami bez bezpośredniego zaangażowania ludzi – były przedmiotem wielu analiz i uwagi w ostatnich latach. Konta te mogą odgrywać cenną rolę w ekosystemie mediów społecznościowych, odpowiadając na pytania

dotyczące różnych tematów w czasie rzeczywistym lub dostarczając automatyczne aktualizacje wiadomości lub wydarzeń. Jednocześnie można je również wykorzystać do próby zmiany sposobu postrzegania dyskursu politycznego w mediach społecznościowych, rozpowszechniania dezinformacji lub manipulowania systemami ocen online. Badania przeprowadzone przez zespół z Oxford Internet Institute[1], 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 kandydata republikanów, porównując z tymi popierającymi kandydatkę demokratów. Naukowcy z Uniwersytetu Południowej Kalifornii i Uniwersytetu Indiany opracowali i przetestowali platformę wykrywania botów na Twitterze. Sklasyfikowali 14 mln kont aktywnej anglojęzycznej populacji Twittera, ustalając optymalne wyniki progowe, które dzielą konta ludzi i botów dla kilku modeli prostych i wyrafinowanych botów. Uzyskane wyniki badań pozwalają oszacować udział bota na od 9% do 15% całej populacji. Udział w procederze manipulowania użytkownikami portali społecznościowych miały również fałszywe konta należące do internetowych trolli, działających często w większych, sterowanych z zewnątrz strukturach nazywanych farmami trolli.

Boty odgrywają bardzo istotną rolę w rozsyłaniu tak zwanych *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. Raport z projektu badawczego prowadzonego przez MIT (Massachusetts Institute of Technology)[2] – podczas którego naukowcy prześledzili kaskady wiadomości rozsiewanych na Twitterze – udowodnił, że to ludzie, a nie boty, są głównie odpowiedzialni za rozpowszechnianie wprowadzających w błąd informacji.

Badania dostarczyły różnych sposobów kwantyfikacji tego zjawiska: np. prawdopodobieństwo ponownego wysłania fałszywych wiadomości jest o 70% wyższe niż prawdziwych. Czas potrzebny na dotarcie prawdziwych historii do określonej grupy odbiorców jest ok. sześć razy dłuższy niż w przypadku fałszywych. Fałsz rozprzestrzenia się znacznie dalej, szybciej, głębiej i szerzej niż prawda we wszystkich kategoriach informacji, a w wielu przypadkach o rząd wielkości. Naukowcy z MIT twierdzą, że jest wysoce prawdopodobne, że to samo zjawisko występuje na innych platformach mediów społecznościowych, w tym na FB, ale podkreślają, że potrzebne są dokładne badania. Tak więc za szerzenie fałszu i propagandy w dużej mierze odpowiada czynnik ludzki, a nie tylko technologia, która dostarczyła narzędzia umożliwiające manipulowanie społeczeństwem na wielką skalę. Zagadnienia te stanowią istotne wyzwanie dla nauk społecznych, a zwłaszcza edukacji zarówno dzieci, jak i dorosłych. Umiejętność oceny wartości i wiarygodności informacji oraz źródła jej pocho-

[1] S.C. Woolley, P.N. Howard, *Political Communication, Computational Propaganda, and Autonomous Agents – Introduction*, "International Journal of Communication" 2016, No. 10, s. 4882–4890.

[2] S. Vosoughi, D. Roy, S. Aral, *The spread of true and false news online*, „Science" 2018, Vol. 359, Issue 6380, s. 1146–1151.

dzenia jest warunkiem koniecznym bezpiecznego funkcjonowania w świecie ICT (*Information and Communication Technologies*)[3].

Algorytmy – jak skutecznie profilować użytkownika? Masowe rozpowszechnianie fałszywych informacji to jednak nie największy kłopot Marka Zuckerberga, twórcy i Generalnego Dyrektora (*CEO*) Facebooka. W marcu 2018 roku Christopher Wylie, dyrektor ds. badań w brytyjskiej firmie Cambridge Analytica ujawnił redaktorom Guardiana i Observera szokujące informacje na temat wykorzystywania przez tę firmę danych nielegalnie pozyskiwanych z FB. Cambridge Analytica we współpracy z FB przeprowadzała testy oraz quizy, które posłużyły do zgromadzenia danych, w celu stworzenia profili psychologicznych[4]. Cambridge Analytica to spółka, która pracowała zarówno przy kampanii promującej Brexit przed referendum w Wielkiej Brytanii, jak i przy kampanii prezydenckiej Donalda Trumpa w 2016 roku. Jak twierdzi sam Christopher Wylie, użytkownik serwisów społecznościowych pozostawia w jednym miejscu mnóstwo informacji o tym, kim jest zarówno w życiu prywatnym, jak i zawodowym (np. lajkując coś). Informacje te mogą być w prosty sposób wyłapane i przepuszczone przez algorytm, który uczy się, kim jest ta osoba. Analizuje jej zachowania przez cały czas i w wielu aspektach. Tak zbudowany system może być lepszy od człowieka w przewidywaniu zachowań ludzi. Stąd mocne przesłanki, by stwierdzić, że dzięki Facebookowi w pośredni sposób można wpływać na to, co jego użytkownicy myślą o zjawiskach, problemach czy politykach. FB buduje im profil klienta, wzmacnia zainteresowania jakimiś zagadnieniami, po to, by później podsunąć rozwiązania. Osoby biorące udział w testach wyrażały zgodę na przetwarzanie swoich danych, ale, jak się okazało, system gromadził także informacje o wszystkich znajomych użytkownika bez ich zezwolenia. Szczegółowe dane o 87 mln osób były uzyskane dzięki bezpośredniej zgodzie jedynie 300 tys. z nich. Zrobili to, klikając bezrefleksyjnie „Akceptuję" pod długim, niezrozumiałym i nieprzeczytanym regulaminem. Dane tych milionów użytkowników portalu społecznościowego miały zostać użyte przez sztaby kampanii prezydenckiej Donalda Trumpa w USA oraz nawołującej do Brexitu w Wielkiej Brytanii.

Okazało się, że już w 2016 roku FB wiedział o wycieku danych i zażądał ich usunięcia przez CA, niestety FB nawet nie sprawdził, czy faktycznie dane pozyskane nielegalnie zostały skasowane oraz nie poinformował użytkowników o wycieku ich danych. Mimo oficjalnych przeprosin M. Zuckerberga za „naruszenie zaufania", opublikowanych w całostronicowych ogłoszeniach zamieszczonych w największych brytyjskich i amerykańskich gazetach, akcje portalu tąpnęły, a samego dyrektora zaprowadziły na przesłuchania przed komisje senackie Stanów Zjednoczonych. M. Zuckerberg udzielił pozytywnej odpowiedzi na to pytanie, stwierdzając, że w tej chwili w FB

[3] Zob. więcej: rozważania nt. „Nowe technologie – nowe zagrożenia wyzwaniem dla edukacji" w monografii: E. Baron-Polańczyk, *My i Oni. Uczniowie wobec nowych trendów ICT*, Oficyna Wyd. UZ, Zielona Góra 2018 (w druku).

[4] C. Cadwalladr, *I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, The Guardian, 17.03.2018, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump [22.04.2018].

jest zespół liczący 20 tys. osób, które zajmują się każdego dnia wykrywaniem i usuwaniem nieodpowiednich treści z serwisu. Dodał, że jego zdaniem za 5–10 lat algorytmy sztucznej inteligencji będą w stanie wychwytywać nawet mowę nienawiści i FB nad tym pracuje, ale chwilowo jeszcze muszą się tym zajmować ludzie[5]. Drugi istotny problem poruszony podczas przesłuchania to kwestia stworzenia odpowiednich regulacji dla sektora technologii, który jak widać nie może regulować się sam.

Giganci Internetu – kto odpowiada za treść? Widać więc wyraźnie, że dyskusja o roli ICT w codziennym funkcjonowaniu społeczeństw musi zmierzyć się z podstawowym pytaniem o formy i zakres odpowiedzialności portali i ich użytkowników za upowszechnianą treść. Jak podkreśla w swojej nowej książce brytyjski historyk Timothy Garton Ash, dzięki dostępowi do Internetu wolność słowa nabrała nowego wyrazu. Każdy może publikować niemal wszystko i docierać do milionów odbiorców. Równie łatwo jest propagować treści wartościowe jak szerzyć fałsz czy mowę nienawiści. Giganci Internetu – koncerny takie jak Facebook, Google czy Amazon dysponują potęgą w kreowaniu dyskursu społecznego. Często za tą potęgą nie stoi człowiek, a wyrafinowane algorytmy sztucznej inteligencji. Zasady funkcjonowania, na których w większości opierają się te algorytmy, premiują zaangażowanie, dążą do tego, by użytkownicy spędzali na portalach jak najwięcej czasu. Koncentrują w jednym miejscu wiele usług i sprzyjają wszystkiemu, co jest ekscytujące i może przyciągnąć uwagę, a *fake news* wpisuje się w ten model idealnie. Ma on więcej odsłon, a odpowiedni algorytm pozycjonuje go jeszcze wyżej. W rezultacie fałsz ma zdecydowanie większe szanse, by stać się hitem Internetu niż prawdziwa informacja. Im słabiej jesteśmy wykształceni i bardziej ukierunkowani ideologicznie, tym większe dla nas zagrożenie stanowi Internet[6]. Problemem współczesnego świata jest pogłębiająca się radykalizacja, która jest następstwem polaryzacji dyskusji opartej na wydawaniu opinii bez odniesienia się do faktów. Zarówno w USA, jak i w Polsce, osoby, które oglądają tylko jeden kanał telewizyjny i czytają jedną gazetę, nie sięgają po inne tytuły, które są źródłem odmiennej opinii. W efekcie osoby z takich „baniek informacyjnych" żyją w kompletnie osobnych światach. Zatem, jak stwierdza T.G. Ash „z jednej strony mamy więc do czynienia z efektem pogłosu, czyli wsłuchiwania się w opinie, które pozwolą nam utwierdzić się w przekonaniu o swoich racjach, z drugiej strony coraz mniej jesteśmy świadomi tego, co konsumujemy w Internecie. Badania na Oksfordzie pokazały, że nawet wyedukowani i inteligentni studenci nie wiedzieli, skąd pochodzą informacje, które przeczytali na Facebooku – czy z CNN, czy z BBC, czy z Kremla"[7].

Opracowanie i wdrożenie stosownych ram prawnych dla nowych technologii jest trudnym, ale wydaje się, że koniecznym wyzwaniem współczesności. Tym bardziej że

[5] M. Wąsowski, *Oto najważniejsze wątki z przesłuchania Marka Zuckerberga przed komisjami Senatu USA*, Business Insider, 10.04.2018, https://businessinsider.com.pl/firmy/zarzadzanie/zeznanie-marka-zuckerberga-w-senacie-usa-przesluchanie-10-kwietnia/dr8f4ye [28.04.2018].

[6] Zob.: T.G. Ash, *Wolne słowo. Dziesięć zasad dla połączonego świata*, Wyd. Znak, Kraków 2018.

[7] *Po co nam wolna prasa?* Wywiad z prof. Timothy Garton Ash, http://www.newsweek.pl/wideo/tomasz-lis-wydanie-specjalne-po-co-nam-wolna-prasa-,film,426539.html [03.05.2018].

wielu użytkowników Internetu nadal lekceważy ochronę własnej prywatności i danych osobowych. Zapominają, że co raz trafi do Internetu, na zawsze tam zostaje. Takie niefrasobliwe zachowanie w połączeniu z deficytem wiedzy informatycznej często umożliwia cyberprzestępcom kradzież tożsamości.

Przykładem regulacji, która właśnie wchodzi w życie i ma zwiększyć bezpieczeństwo użytkowników, chronić ich prywatność oraz harmonizować prawo w ramach UE jest „Ogólne rozporządzenie o ochronie danych" – RODO (GDPR – *General Data Protection Act*). Dyrektywa została przyjęta 27 kwietnia 2016 i po dwuletnim okresie przejściowym od 25 maja 2018 zaczyna obowiązywać w krajach członkowskich UE[8]. Nowe prawo ma m.in. zapewnić: łatwiejszy dostęp do danych (zapewnienie większej liczby informacji na temat sposobu przetwarzania danych i zapewnienie, aby informacje te były dostępne w przejrzysty i zrozumiały sposób), nowe prawo do przenoszenia danych (ułatwia przesyłanie danych osobowych pomiędzy dostawcami usług), jaśniejsze prawo do usunięcia danych („prawo do bycia zapomnianym"), prawo do bycia niezwłocznie poinformowanym w razie ataku hakerskiego na dane (firmy będą także zobligowane zawiadomić odpowiednie organy nadzorcze ds. ochrony danych), technologie takie jak pseudonimizacja oraz szyfrowanie. Rozporządzenie reguluje również ogólne warunki nakładania administracyjnych kar pieniężnych oraz wprowadza dwa bardzo dotkliwe przedziały kar dla administratorów danych.

Mark Zuckerberg już oświadczył, że choć zasadniczo zgadza się z restrykcyjną reformą prawa ochrony danych osobowych, którą w UE wprowadza RODO, to jego koncern nie zamierza stosować się do zasad przez nie narzucanych poza obszarem UE. W firmie trwają prace nad własnymi zasadami dotyczącymi ochrony danych, które zostaną wdrożone na całym świecie[9]. Facebook rozpoczął kampanię edukacyjną, która w możliwie przystępny sposób tłumaczy kwestie bezpieczeństwa danych i zarządzania prywatnością[10]. FB wprowadził również nowe globalne centrum prywatności danych, które pozwala użytkownikom organizować, kto widzi ich posty i jakie typy reklam są wyświetlane. Wytłumaczony został też model biznesowy FB, oparty na wykorzystywaniu zebranych informacji do sprzedawania treści reklamowych. Sposób, w jaki największe firmy technologiczne poradzą sobie z regulacjami, najprawdopodobniej wpłynie na funkcjonowanie całego rynku nowych technologii, gdyż mniejsze firmy często na nich się wzorują. Idąc za przykładem UE, inne państwa mogą również zacząć domagać się podobnych środków prawnych ochrony danych dla swoich obywateli. Być może nieco utopijna wizja „wolnego Internetu" przechodzi na naszych oczach do historii.

---

8 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32016R0679 [03.05.2018].

9 *Facebook nie będzie stosować RODO poza Unią Europejską*, PAP, https://businessinsider.com.pl/firmy/strategie/rodo-stanowisko-facebooka-poza-ue/hwhty4y [03.05.2018].

10 *Giving You More Control of Your Privacy on Facebook*, Facebook Newsroom, https://newsroom.fb.com/news/2018/01/control-privacy-principles/ [05.05.2018].

Patostreamy – dlaczego zło jest atrakcyjne? Kolejnym problemem jest również bardzo łatwa dostępność w Internecie nieodpowiednich treści propagujących niemoralne, patologiczne czy wręcz kryminalne zachowania. Dużą popularnością cieszą się szczególnie wśród młodych odbiorców tak zwane „patostreamy". Jak wskazuje sama nazwa, będąca zlepkiem słów patologia i stream (czyli transmisja strumieniowa), jest to przekaz na żywo zawierający patologiczne treści. To zjawisko społeczne występuje głównie na YouTubie i pokazuje, że również ten największy na świecie portal wideo, należący do Google, ma problem z prezentowanymi treściami, a mechanizmy ich propagacji są tożsame z tymi FB czy Twittera. Kiedy platforma była jeszcze małym serwisem, rekomendacje podlegały żywym osobom, które proponowały, jakie kolejne wideo będzie nam wyświetlać się w polecanych. Gdy użytkowników i filmów zaczęło przybywać w postępie geometrycznym, serwis podjął decyzję o zastąpieniu ludzi algorytmami, które dopasowują, co nam się wyświetli na podstawie naszej historii przeglądania. Google jest brokerem reklamowym, sprzedającym naszą uwagę firmom, które za to zapłacą. Im dłużej ludzie pozostają na YouTube, tym więcej pieniędzy zarabia Google – bot musi więc zasugerować takie treści, które będą chętniej oglądane przez danego widza. Treść nie ma znaczenia, o ile nie zawiera elementów niezgodnych z polityką serwisu.

Używając wyszukiwanych przez użytkownika haseł, bot indeksuje wszystkie najlepsze polecane filmy i śledzi te, które są najczęściej polecane. Działanie tego algorytmu, które zaobserwowała dziennikarka NYT („The New York Times") przy tematach politycznych, skłoniło ją do przeprowadzenia kilku eksperymentów z tematami niepolitycznymi. Pojawił się ten sam podstawowy mechanizm: filmy o wegetarianizmie prowadziły do filmów o weganizmie, filmy o joggingu prowadziły do filmów o uprawianiu ultramaratonu. Autorka stwierdza, że „nigdy nie jesteś dość 'hard coreowy' dla algorytmu rekomendacji YouTube. Promuje, rekomenduje i rozpowszechnia filmy wideo w sposób, który wydaje się stale podnosić stawkę. Mając ok. miliarda użytkowników, YouTube może być jednym z najpotężniejszych instrumentów radykalizujących w XXI wieku"[11]. Potwierdza to projekt Algotransparency[12], za którym stoi Guillaume Chaslot, były pracownik YouTube. Demonstruje on, jak potencjalnie działa bot serwisu odpowiedzialny za rekomendacje i stwierdza: „po obejrzeniu 20 filmów o tym, że Ziemia jest płaska, niektórzy w to uwierzą". W podobny sposób wzrasta zainteresowanie teoriami spiskowymi, kwitną ruchy antyszczepionkowe czy negujące teorię ewolucji – algorytm serwisu wpycha użytkowników w bańki informacyjne. Ta sytuacja jest szczególnie niebezpieczna, biorąc pod uwagę, jak wielu ludzi wykorzystuje YouTube w celu uzyskania informacji.

Podobnie jak w przypadku propagowania *fake news* pojawia się pytanie o odpowiedzialność portalu za treść. YouTube dysponuje tak zwanymi wytycznymi dla społeczności, które są zbiorem zasad, jakich twórcy powinni przestrzegać, wrzucając filmy. To także wskazówki dla samych widzów odnośnie do tego, które treści

[11] Z. Tufekci, *YouTube, the Great Radicalizer*, "The New York Times" 10.03.2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html [05.05.2018].

[12] *Projekt Algotransparency*, https://algotransparency.org [05.05.2018].

„oflagowywać", czyli zgłaszać do sprawdzenia przez pracowników YouTube. Specjalne algorytmy wyłapują też i blokują materiały terrorystyczne czy drastyczne, jednak trudno jest monitorować wszystkie transmisje na żywo. Pomimo podejmowanych przez portal działań wydaje się, że systemy weryfikacji treści nie są wystarczająco skuteczne. Można odnieść wrażenie, że podobnie jak fałsz, zło szerzy się w Internecie szybciej, dalej i głębiej niż dobro. Może jest bardziej atrakcyjne?

Podsumowanie. Używanie prostych i powtarzalnych haseł, klikanie w podejrzane linki i otwieranie załączników do poczty niewiadomego pochodzenia, to najczęstsze przyczyny utraty lub wycieku danych czy zainfekowania systemu informatycznego. Cyberprzestępcy cały czas doskonalą swój warsztat, zaprzęgając sztuczną inteligencję do prowadzenia spersonalizowanych ataków socjotechnicznych z wykorzystaniem złośliwego oprogramowania. Głównym wektorem tych ataków są media społecznościowe. Według Raportu CERT Orange Polska za rok 2017 najczęściej wybieranym przez cyberprzestępców typem ataku w minionym roku były próby infekcji oprogramowaniem typu *ransomware* (szyfruje zawartość dysku twardego i żąda opłacenia okupu, jak pamiętny WannaCry) oraz *phishing* (podszywanie się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji). Obie te formy ataku wymagają dla swej skuteczności określonych zachowań atakowanego użytkownika. Jak słusznie stwierdzają autorzy raportu: „Najlepszą bronią przed niebezpieczeństwami w Internecie jest wiedza, a w razie zaistnienia zagrożenia – odpowiednia reakcja. […] Inicjacja internetowa zaczyna się coraz wcześniej, a wraz z nią pojawia się odpowiedzialność rodziców i wychowawców za przekazanie i dostosowanie tej wiedzy do aktualnych potrzeb. Wprowadzając dziecko w świat Internetu, musimy przekazywać zasady, które w nim panują oraz przygotować środowisko, z którego dzieci korzystają – aby jak najbardziej ograniczyć wpływ szkodliwych treści czy niebezpiecznych zachowań. Niezwykle ważny jest ten pierwszy moment, bo wtedy uczymy dziecko podstawowych zasad, ale musimy też pamiętać o nastolatkach i nie pozostawić ich samym sobie. Z każdym rokiem zmieniają się przecież potrzeby dziecka, mamy do czynienia z ciągle nowymi zjawiskami i zagrożeniami"[13].

Pojawiają się więc pytania o rolę rodziców i domu rodzinnego oraz nauczycieli i całego systemu edukacji w procesie wychowania do nowych technologii. Wielu rodziców kontrolę tego, co ich pociechy oglądają lub transmitują w Internecie[14],

[13] *Raport CERT Orange Polska za rok 2017*, https://www.cert.orange.pl/aktualnosci/przedstawwiamy-raport-cert-orange-polska-za-2017-rok [05.05.2018].

[14] Zob.: wyniki badań dot. kontroli rodzicielskiej w użytkowaniu Internetu, wg których ponad połowa badanych nastolatków (55,6%) zadeklarowała, iż ich rodzice nie interesują się tym, co robią w Internecie, a 39,3% stwierdziło, że chociaż rodzice starają się kontrolować, ale nie jest to kontrola pełna lub skuteczna. Tylko co dwudziesty respondent (5,1%) odpowiedział, że rodzice mają pełną kontrolę nad ich aktywnością w sieci. Dominującym sposobem kontroli rodzicielskiej okazuje się być kontrola pośrednia, tzn. rozmowa z dzieckiem (62,3%) lub wgląd do profili na serwisach społecznościowych (17,0%). Stosunkowo nieliczni rodzice stosują kontrolę techniczną bezpośrednią: urządzenia transferujące sygnał (13,2%), filtr rodzicielski (2,3%). Zob.: A. Wrońska, R. Lange, *Nastolatek jako użytkownik Internetu – społeczny wzorzec konsumpcji*, [w:] M. Tanaś (red.), *Nastolatki wobec Internetu*, Wyd. NASK, Warszawa 2017, s. 25–26.

utożsamiają z wyłączeniem Internetu „za karę". W tej sytuacji na systemie edukacji ciąży obowiązek przygotowania i ukształtowania świadomego użytkownika technologii internetowych – ucznia nowej ery. Pojawia się pytanie o przygotowanie do tego obowiązku szkoły i samych nauczycieli. Informatyzacja placówek oświatowych w Polsce jest daleka od doskonałości. Nadal niewiele szkół dysponuje polityką bezpieczeństwa informacji i poprawnie wdrożonymi procedurami bezpiecznej eksploatacji systemów informatycznych czy ochrony danych osobowych. Poprawę tego stanu z pewnością przyniesie wspomniane już wejście w życie przepisów RODO, które wymuszają na organach prowadzących i dyrekcjach szkół podjęcie działań w tym zakresie.

Wartość i wiarygodność źródła pozyskiwania wiedzy i umiejętności przez uczniów w zakresie obsługiwania i wykorzystywania nowych technologii były przedmiotem autorskich badań[15]. Najważniejsze zagregowane rezultaty badań, próby 2510 respondentów z czterech etapów kształcenia (rozkład częstości dla 3585 uczniowskich wskazań), wykazały, że: 1) Dzieci i młodzież zdradzają, że o nowych technologiach uczą się przede wszystkim od swoich nauczycieli, w tym wyróżniając szczególnie nauczycieli zajęć komputerowych i informatyki. Odpowiedzi te zajmują dwa pierwsze miejsca w częstości ich występowania – łącznie stanowiąc prawie trzecią część (31,9%) wskazań. Możemy tu mówić o samoukach i samouctwie, a nawet o samorzutnym rozwoju i stałej potrzebie (samo)kształcenia ustawicznego. Kategoria „SAM się uczę" uplasowała się na trzecim miejscu (w liczbie 14,8%) uczniowskich wskazań; 3) Co dziesiąty badany (tj. ok. 10%) mówił, że wiedzę i umiejętności w zakresie ICT czerpie albo od rodziców (darząc w tym względzie naturalnym zaufaniem i autorytetem matkę i/lub ojca) albo z internetowych zasobów – co stawia na równi te dwa źródła wsparcia w budowaniu uczniowskiej wiedzy; 4) Dalej, jako źródło wiedzy i umiejętności w zakresie ICT (w liczbie mniejszej niż 7,5% wskazań) uczniowie wyliczali kolejno: rodzeństwo, szkołę, znajomych, rówieśników, rodzinę, dom i bibliotekę.

Grupując uzyskane wyniki w szersze znaczeniowo kategorie, możemy uogólniając stwierdzić, że źródła wiedzy i umiejętności w zakresie ICT uczniowie widzą głównie w edukacji nieformalnej. Zaliczając do tego zakresu wypowiedzi zwracające uwagę na rodziców, rodzeństwo, znajomych, bliską i dalszą rodzinę, rówieśników, samouctwo i Internet oraz książki, bibliotekę i „inne" osoby – stanowią one ponad połowę wyliczeń (61,9%). Mimo że wskazania na nauczycieli zajmują pierwsze miejsca, to w sumie dzieci i młodzież mniejsze znaczenie przypisują edukacji formalnej, pomniejszając wagę zorganizowanego procesu kształcenia i oddziaływań placówek oświatowych.

Przytoczone na zakończenie wyniki badań pokazują, że w świecie ICT uczymy się wszyscy, nieustannie i wspólnie w sieci wzajemnych relacji o różnej sile i charakterze. Każdy uczestnik tego procesu powinien posiadać, oprócz koniecznych kompetencji instrumentalnych, ugruntowane kompetencje kierunkowe (aksjologiczne), gdyż tylko ich połączenie daje gwarancję wartościowego wykorzystanie ICT w całożyciowej edukacji.

[15] Zob. rozdział „Źródła wiedzy i umiejętności w zakresie ICT", [w:] E. Baron-Polańczyk, *My i Oni...*, op. cit.

Bibliografia

1. Ash T.G., *Wolne słowo. Dziesięć zasad dla połączonego świata*, Wyd. Znak, Kraków 2018.
2. Baron-Polańczyk E., *My i Oni. Uczniowie wobec nowych trendów ICT*, Oficyna Wyd. UZ, Zielona Góra 2018 (w druku).
3. Cadwalladr C., *I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, The Guardian, 17.03.2018, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump [22.04.2018].
4. *Facebook nie będzie stosować RODO poza Unią Europejską*, PAP, https://businessinsider.com.pl/firmy/strategie/rodo-stanowisko-facebooka-poza-ue/hwhty4y [03.05.2018].
5. *Giving You More Control of Your Privacy on Facebook*, Facebook Newsroom, https://newsroom.fb.com/news/2018/01/control-privacy-principles/ [05.05.2018].
6. Kwiatkowska H., *Pedeutologia*, Wyd. Akademickie i Profesjonalne, Warszawa 2008.
7. *Po co nam wolna prasa?* Wywiad z prof. Timothy Garton Ash, http://www.newsweek.pl/wideo/tomasz-lis-wydanie-specjalne-po-co-nam-wolna-prasa-,film,426539.html [03.05.2018].
8. *Projekt Algotransparency*, https://algotransparency.org [05.05.2018].
9. *Raport CERT Orange Polska za rok 2017*, https://www.cert.orange.pl/aktualnosci/przedstawwiamy-raport-cert-orange-polska-za-2017-rok [05.05.2018].
10. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32016R0679 [03.05.2018].
11. Stamos A., *Authenticity Matters. The IRA Has No Place on Facebook*, https://newsroom.fb.com/news/2018/04/authenticity-matters/ [03.05.2018].
12. Tufekci Z., *YouTube, the Great Radicalizer*, "The New York Times" 10.03.2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html [05.05.2018].
13. Vosoughi S., Roy D., Aral S., *The spread of true and false news online*, „Science" 2018, Vol. 359, Issue 6380.
14. Wąsowski M., *Oto najważniejsze wątki z przesłuchania Marka Zuckerberga przed komisjami Senatu USA*, Business Insider, 10.04.2018, https://businessinsider.com.pl/firmy/zarzadzanie/zeznanie-marka-zuckerberga-w-senacie-usa-przesluchanie-10-kwietnia/dr8f4ye [28.04.2018].
15. Woolley S.C., Howard P.N., *Political Communication, Computational Propaganda, and Autonomous Agents – Introduction*, "International Journal of Communication" 2016, No. 10.
16. Wrońska A., Lange R., *Nastolatek jako użytkownik Internetu – społeczny wzorzec konsumpcji*, [w:] M. Tanaś (red.), *Nastolatki wobec Internetu*, Wyd. NASK, Warszawa 2017.

dr hab. Eunika BARON-POLAŃCZYK, prof. UZ
Uniwersytet Zielonogórski
e-mail: e.baron@iibnp.uz.zgora.pl