ARTYKUŁY

„Polityka i Społeczeństwo" 1(18) / 2020
DOI: 10.15584/polispol.2020.1.2

Agnieszka Demczuk*

WOLNOŚĆ WYPOWIEDZI I PRAWO DO PRYWATNOŚCI W SPOŁECZEŃSTWIE INFORMACYJNYM – WYBRANE AKTUALNE REFLEKSJE

FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY IN THE INFORMATION SOCIETY – SELECTED CURRENT REFLECTIONS

Abstract

The measure of civilizational progress is not only economic development, which for several years has been determined by the development of computer science, but also an increase in the level of respect for human rights and freedoms guaranteed in various international legal documents. The Internet is increasingly determining the use of personal, political, social, and economic rights. Public authorities, as part of positive obligations, should be more actively involved in the protection of human rights, especially the freedom of expression and the right to privacy, which are currently being violated quite widely and especially in the horizontal dimension in cyberspace.

Keywords: freedom of expression, right to privacy, protection of human rights, information society, internet, ICT, human rights violations, human rights abuse

[…] *cechą charakterystyczną naszego przeobrażonego świata*
jest zewnętrzne łączenie wirtualnego z fizycznym
w wyniku zdarzeń i zjawisk,
które określam wspólną nazwą 'masowa migracja i Internet'

T.G. Ash

Wstęp

Rewolucja informacyjna, która dokonuje się od blisko dwóch dekad, wynikająca z gwałtownego rozwoju sieci komputerowych, przebudowu-

* Katedra Systemów Politycznych i Praw Człowieka, Instytut Nauk o Polityce i Administracji, Wydział Politologii i Dziennikarstwa, Uniwersytet Marii Curie-Skłodowskiej, pl. Marii Curie-Skłodowskiej 5, 20-400 Lublin, e-mail: ademczuk@hektor.umcs.lublin.pl, ORCID ID: 0000-0003-2691-2043

je i zmienia społeczeństwo w informacyjne, coraz bardziej zglobalizowane i usieciowione. Samo jednak określenie „społeczeństwo informacyjne" budzi coraz więcej wątpliwości, gdyż wszechogarniający szum informacyjny, *fake news* i zalew dezinformacji powodują, iż na obecnym etapie jego rozwoju właściwiej należałoby je określić mianem „społeczeństwa (dez)informacyjnego".

W tym swoistym „potopie informacyjnym" zatracają się granice pomiędzy prawdą i fałszem, informacją i dezinformacją, a debata publiczna, będąca centralnym miejscem społeczeństwa demokratycznego, ustępuje miejsca populistycznym sporom oraz rankingom popularności liderów politycznych i post-ekspertów. Post-prawdzie i dezinformacji w sieci towarzyszy zalew mowy nienawiści na niespotykaną dotąd skalę. Powszechna staje się praktyka naruszająca własność intelektualną w cyberprzestrzeni, zagrożone jest prawo do prywatności i tajemnica elektronicznej korespondencji. Powstają nowe sieciowe ruchy społeczne, będące tradycyjnym wyrazem niepokojów społecznych i zarazem nową formą mobilizacji obywatelskiej na początku XXI w. (Castells, 2013). Coraz lepszy dostęp do nowych technologii i powszechna obecność jednostek w mediach społecznościowych (*social media*) umożliwiają organizację „twitterowych rewolucji" oraz „sieci oburzonych".

Wolność wyrażania opinii, prawo do informacji, edukacji, prywatności, zakaz dyskryminacji i inne prawa i wolności są gwarantowane przez podstawowe dokumenty prawne z zakresu ochrony praw człowieka. Jednak ich faktyczna realizacja w ramach komunikacji elektronicznej daleka jest od założonych standardów „zaprojektowanych" w traktatach międzynarodowych po II wojnie światowej dla wzmocnienia i utrwalenia społeczeństwa demokratycznego.

Na początku XXI w. przed władzami stoją nowe wyzwania w zakresie przyjęcia nowych regulacji prawnych i realizacji praktyki skuteczniejszej ochrony praw człowieka w cyberprzestrzeni w ramach pozytywnych obowiązków, coraz powszechniej naruszanych przez innych użytkowników. Omówione zostaną zagadnienia związane z naruszeniami praw człowieka zgodnie z powszechnie uznaną, w literaturze fachowej, koncepcją triady ochrony praw człowieka, tj. ochroną normatywną, instytucjonalną i proceduralną (środków prawnych).

Autorka scharakteryzuje zachodzące zjawiska zachodzących za sprawą rozwoju ICT zmian we współczesnym społeczeństwie informacyjnym, mających wpływ na praktykę naruszającą w zakresie praw człowieka. Przy czym należy na wstępie zauważyć, iż do naruszenia różnych praw człowieka, a w szczególności wolności wypowiedzi i prawa do prywatności, coraz częściej dochodzi w relacjach horyzontalnych. To użytkownicy (internauci) i inne podmioty niepaństwowe (np. firmy informatycz-

ne) dopuszczają się naruszeń prawa ochrony wizerunku, danych osobowych, ochrony dobrego imienia, godności i innych. Tym samym tradycyjne rozumienie działania praw człowieka w wymiarze wertykalnym (pomiędzy władzą a jednostką), ze względu na specyfikę elektronicznej komunikacji, jak się wydaje, nie jest już wystarczające do opisania i wyjaśnienia nowych form naruszenia i nadużywania praw człowieka w społeczeństwie informacyjnym. Należy bowiem zauważyć, iż deficyty legislacyjne w zakresie prawa sieci, jak np. te dotyczące rozpowszechniania fałszywych wiadomości (*fake news*) czy obecności w cyberprzestrzeni „armii trolli i botów" i ich szkodliwego wpływu na debatę publiczną, czy wreszcie luki prawne dotyczące do niedawna jeszcze możliwości domagania się od administratora platformy realizacji prawa do zapomnienia, generowały i wciąż generują nowe formy nadużywania starych przepisów prawnych, niedostosowanych do aktualnych wyzwań postępu technologicznego. Konieczne są działania ze strony władz publicznych, mające na celu wypracowanie nowego, wieloaspektowego instrumentarium przeciwdziałania tym naruszeniom i nadużywaniu praw i wolności człowieka w cyberprzestrzeni.

Sama koncepcja praw człowieka, mimo iż jest przede wszystkim przedmiotem zainteresowania nauki prawa, ma jednak charakter interdyscyplinarny. Prawa człowieka są przedmiotem badania różnych dyscyplin naukowych, np. filozofii, teologii, historii, psychologii społecznej, socjologii, politologii czy nauki stosunków międzynarodowych. Ze względu na szybki rozwój nowych mediów elektronicznych prawa i wolności człowieka stały się także w większym zakresie przedmiotem zainteresowania nauki o mediach, komunikacji społecznej czy informatyki.

Z powodu ograniczonych ram objętościowych niniejszej analizy autorka ograniczy się w swoich refleksjach przede wszystkim do wybranych dwóch praw i wolności człowieka, tj. wolności wypowiedzi i prawa do prywatności. Zostaną przeanalizowane zagadnienia związane z nowymi zjawiskami towarzyszącymi społeczeństwu informacyjnemu i rozwojowi nowoczesnych technologii: propaganda polaryzacyjna, komputacyjna (obliczeniowa), które są formą nowej manipulacji w cyberprzestrzeni opartej na nowych technikach obliczeniowych (boty, trolle, *fake news*), a także mowie nienawiści. Scharakteryzowane zostaną negatywne skutki propagandy polaryzacyjnej i komputacyjnej, które przede wszystkim mogą zagrażać debacie publicznej i mieć destrukcyjny wpływ na procesy demokratyczne. Autorka podda analizie także kwestie związane z naruszaniem prawa do prywatności, gdyż rozwój prawa do prywatności dowodzi, iż to właśnie jego poszczególne elementy są niezwykle wrażliwe na zmiany wynikające z przeobrażeń warunków cywilizacyjnych związanych z szybkim postępem technologicznym. Warto wreszcie zauwa-

żyć, iż analiza problematyki praw człowieka byłaby niepełna z perspektywy jurydycznej i politologicznej, gdyby nie zawierała także praktycznego wymiaru praw człowieka. Stąd w tekście omówione zostanie wybrane orzecznictwo międzynarodowe, w tym szczególnie strasburskie.

Rozwój społeczeństwa informacyjnego w II dekadzie XXI w.

W dobie intensywnego rozwoju nowych technologii, coraz szybszego obiegu informacji oraz powszechnego dostępu do niej kształtuje się nowy typ społeczeństwa – społeczeństwo informacyjne. Cywilizacja u progu XXI w., jak pisał Yoneji Maruda, jeden z japońskich prekursorów koncepcji nowego społeczeństwa, nie będzie cywilizacją materialną, symbolizowaną przez ogromne konstrukcje, ale będzie cywilizacją niewidoczną – informacyjną (za: Goban-Klas, 1999, s. 9).

Przedstawiciele nauk społecznych proponują dziesiątki różnych definicji społeczeństwa informacyjnego. Zawsze jednak ich wspólnym mianownikiem jest informacja i dostęp do niej. Społeczeństwo informacyjne jest z pewnością rzeczywistością wielowarstwową, można więc przyjąć, za Agnieszką Pawłowską, iż składają się na nią: substrat technologiczny, ekonomiczny, społeczny i kulturowy. Substrat technologiczny to rozwijająca się infrastruktura informatyczna, czyli dostępność urządzeń służących gromadzeniu, przetwarzaniu, przechowywaniu i udostępnianiu informacji, mnogość kanałów przesyłania danych oraz możliwość łączenia ich w rozmaite konfiguracje. Substrat ekonomiczny obejmuje intensywnie rozwijający się informacyjny sektor gospodarki, czyli rozwijają się te gałęzie produkcji i usługi, które zajmują się wytwarzaniem informacji oraz technikami informacyjnymi (ICT), a także ich dystrybucją. Substrat społeczny stanowi wysoki odsetek osób korzystających w pracy, szkole i gospodarstwie domowym z ICT, co odpowiada wysokiemu poziomowi wykształcenia społeczeństwa, natomiast substrat kulturowy oznacza wysoki poziom kultury informacyjnej, tj. stopień akceptacji dla informacji jako dobra strategicznego oraz towaru, a także odpowiedni poziom kultury informatycznej, czyli umiejętności związanych z obsługą urządzeń informatycznych (Pawłowska, 2002, s. 33–34).

Nowy raport *Global Electronic 2018* z *We Are Social* i *Hootsuite* ujawnił, że w 2018 r. z Internetu korzystało już ponad 4 mld ludzi na całym świecie. Ponad połowa populacji na świecie była *online*, a prawie jedna czwarta miliarda nowych użytkowników pojawiła się *online* po raz pierwszy w 2017 r. Afryka odnotowała najszybsze tempo wzrostu, a liczba użytkowników Internetu na całym kontynencie rosła o ponad

20% z roku na rok. Znaczna część wzrostu liczby użytkowników Internetu w 2018 r. wynika z bardziej przystępnych cenowo smartfonów. Dwie trzecie ludzkości, tj. 5,135 mld z 7,6 mld mieszkańców na świecie posiada telefon komórkowy, a ponad połowa używanych telefonów to urządzenia „inteligentne", coraz więc łatwiej jest ludziom korzystać z Internetu. Popularność mediów społecznościowych (*social media*) wciąż nadal szybko rośnie, a liczba osób odwiedzających platformę w każdym kraju wzrosła o prawie milion nowych użytkowników każdego dnia w ciągu ostatnich 12 miesięcy. Ponad 3 mld ludzi na całym świecie korzysta obecnie z mediów społecznościowych co miesiąc (*Global Digital Report*, 2018). W 2019 r. odnotowano kolejny wzrost cyfrowy w skali całego świata, i tak z Internetem łączyło się już więcej ludzi niż mieszkało w miastach, tj. blisko 2/3 globalnej populacji – 4 mld 390 mln osób. Warto odnotować, że w 2018 r. około 367 mln internautów po raz pierwszy połączyło się z siecią. Ponad połowa ludzkości, czyli 57%, łączyło się z siecią, a 52% robiło to przez smartfony i tablety (*Global Digital Report*, 2019*).*

Powyższe dane wskazują zatem na coraz intensywniejszy rozwój infrastruktury i skłaniają do sformułowania wniosku, iż rzeczywiście ludzkość wkroczyła w nowy – drugi etap rozwoju społeczeństwa globalnie informacyjnego i usieciowionego. W pierwszym etapie rozwoju społeczeństwa na przełomie XX/XXI w. zasadniczym problemem była dostępność do infrastruktury informatycznej. Stąd eksperci i decydenci polityczni na szczeblu krajowym i międzynarodowym postulowali konieczność rozbudowy i upowszechnienia infrastruktury teleinformatycznej (prawo do usług ICT, Demczuk i Pawłowska, 2009, s. 133–147). W ramach polityki krajowej i międzynarodowej prowadzonej na forum przede wszystkim Unii Europejskiej (w ramach strategii lizbońskiej) i ONZ (w ramach organizowanych światowych szczytów społeczeństwa informacyjnego) decydenci polityczni podjęli się opracowania politycznych strategii rozwoju społeczeństwa informacyjnego (np. *Information Society For All*). Podjęto szereg działań mających na celu wsparcie finansowe projektów badawczych z zakresu rozwoju sieci infrastruktury technicznej.

W kolejnym etapie rozwoju społeczeństwa informacyjnego, jednocześnie poddawanego od lat procesom globalizacyjnym, do kluczowych spraw należy zaliczyć obecność nowych bądź starych – ale zwielokrotnionych – społecznych zjawisk towarzyszących korzystaniu z Internetu. Powszechne stały się: zalew informacyjny, naruszenia prywatności, sieciowe ruchy społeczne, mowa nienawiści, rozpowszechnianie fałszywych wiadomości *(fake news)*, hejting. Internet, jak zauważył M. Ca-

stells, stał się techniczną bazą dla struktury organizacyjnej współczesnej epoki informacji – sieci, które mają wiele zalet ze względu na typową dla nich naturalną elastyczność i łatwość dostosowania do bieżących wymogów, a które to cechy decydują o przetrwaniu w szybko zmieniającym się świecie (Castells, 2003, s. 11). Dziesięć lat później Castells podkreślał, iż obserwowany jest rozwój masowej komunikacji zindywidualizowanej stanowiącej platformę technologiczną, która pozwala konstruować autonomię aktora społecznego, i to zarówno jednostki, jak i zbiorowości (Castells, 2013, s. 19). Aktorzy ci realizują i zaspokajają swoje potrzeby, pragnienia i emocje głównie w mediach społecznościowych. Obserwowany jest masowy proces profilowania danych osobowych użytkowników sieci. Podmioty komercyjne od kilku lat stosują powszechnie psychografię konsumentów i wykorzystują w tym celu algorytmy prognostyczne[1].

Kolejny rozwój systemu horyzontalnych sieci komunikacyjnych i informacyjnych (era Web 2.0) uruchomił nowy system horyzontalnego rozpowszechniania wszelkich wypowiedzi na niespotykaną skalę, w którym każdy użytkownik Internetu stał się zarówno ich nadawcą, jak i odbiorcą, bez granic i bez kontroli władz publicznych. Futurystyczna fraza ochrony wolności wypowiedzi „ponad granicami" pochodząca z międzynarodowych dokumentów prawnych z zakresu praw człowieka (międzynarodowy pakt praw obywatelskich i politycznych, art. 19, czy europejska konwencja o ochronie praw człowieka i podstawowych wolności, art. 10) zmaterializowała się na początku XXI w. Komercjalizacja i w konsekwencji pauperyzacja mobilnych technologii informacyjnych i komunikacyjnych, gwałtowny rozwój i upowszechnienie mediów społecznych (*social media*), proces uniwersalizacji i globalizacji wolności wypowiedzi w ramach międzynarodowych praw człowieka (ONZ, Rada Europy, Unia Europejska), czy wreszcie dominacja na rynku informatycznym wielkich koncernów technologicznych, funkcjonujących na podstawie amerykańskiej koncepcji ochrony wolności wypowiedzi (I Poprawka i orzecznictwo Sądu Najwyższego Stanów Zjednoczonych) stworzyły dogodną sytuację społeczną i polityczną dla współczesnych trendów we współczesnym sieciowym społeczeństwie informacyjnym.

[1] Algorytmy – informatyczne procedury kontrolujące, jakie treści użytkownicy publikują i „lajkują", aby w ten sposób najlepiej dotrzeć do nich z nowymi ofertami reklamowymi i tym samym zwiększyć zainteresowanie kupnem nowych produktów w sieci. Proces przygotowania i doskonalenia algorytmów jest coraz bardziej zautomatyzowany i w coraz większym stopniu odwołuje się do narzędzi sztucznej inteligencji i uczenia maszynowego. Złożoność systemu, jak zauważa Edwin Bendyk, zarówno ze względu na skomplikowanie rozwiązań informatycznych, jak i skalę tego procesu, wzrasta w tempie szybszym niż zdolność do efektywnej kontroli przez twórców tego systemu (Bendyk, 2018, s. 71).

Wpływ nowoczesnych technologii na kondycję wolności wypowiedzi i prawo do prywatności

W 2016 r. i kolejnych latach ujawniono, iż platformy komunikacyjne, jak Facebook i Twitter, są wykorzystywane do prowadzenia tzw. wojny hybrydowej, umożliwiając wpływ na procesy polityczne i funkcjonowanie dojrzałych demokracji liberalnych. Światowe media (np. *The Guardian*) doniosły o tzw. aferze Cambridge Analytica, wiążącej się z wykorzystaniem danych około 50 mln użytkowników Facebooka. Dane miały być wykorzystane m.in. po to, by wpłynąć na wyniki wyborów w Stanach Zjednoczonych Ameryki Północnej. Wiele dostępnych informacji wskazuje, że firma Cambridge Analytica tworzyła psychologiczne profile użytkowników, aby następnie kierować do tych osób przekazy o określonej, dopasowanej treści, które mogły oddziaływać na ich wybory, w tym wybory polityczne[2]. Cambridge Analytica mogła prowadzić działania, które w efekcie wpłynęły także na wyniki referendum w sprawie *brexitu* czy też na wybory w Kenii. Tym samym powszechnie analizowana i komentowana stała się kwestia udostępniania danych osobowych oraz wykorzystywania ich do wpływania na wybory i decyzje użytkownika. Jak zauważył Adam Bodnar, Rzecznik Praw Obywatelskich w latach 2015–2020, w piśmie do Generalnego Inspektora Ochrony Danych Osobowych w marcu 2018 r. (wystosowanym w związku z wątpliwościami, czy sprawa wykorzystania w ten sposób danych dotyczyć mogła także obywateli polskich), proceder ten mógł stwarzać zagrożenie nie tylko dla prawa do prywatności użytkownika sieci internetowej, ale również dla szeroko pojętych procesów demokratycznych i ochrony praw obywatelskich w państwie[3]. Brytyjski organ, Komisarz ds. Informacji, rozpoczął również sprawdzanie okoliczności, w jakich dane pozyskane z Facebooka mogły zostać wykorzystane, w szczególności do tzw. mikrotargetowania *(microtargeting),* czyli techniki znanej w kampaniach wyborczych na świecie i wykorzystywanej przez partie polityczne. Istotne jednak jest to, aby wyborcy byli świadomi metod, za pomocą których informacje są wykorzystywane w nowoczesnych kampaniach politycznych oraz jaki

[2] Firma Cambridge Analytica sięgała przy tym do danych nie tylko tych osób, które instalowały określoną aplikację, ale również do danych powiązanych z nią użytkowników i na takie działania miał się zgadzać Mark Zuckerberg, założyciel *Facebooka* (wydał także stosowne oświadczenie w tej sprawie w marcu 2018 r.)

[3] W sprawie Cambridge Analytica szczególne działania podjął także brytyjski Komisarz ds. Informacji *(Information Commissioner*), wszczynając postępowanie dotyczące wykorzystania danych osobowych i ich analizy przez Cambridge Analytica do celów kampanii politycznych, dla celów partii i podmiotów komercyjnych.

jest ich potencjalny wpływ na prawo do prywatności (Pismo RPO do GIODO, 2018).

W cyberprzestrzeni zauważalny jest także od kilku lat zalew nadmiarowości informacji, w tym także fałszywych wiadomości (*fake news*), dezinformacji oraz agresywnej i niejednokrotnie prymitywnej mowy nienawiści. Z wykorzystaniem algorytmów stwarzane są tzw. bańki informacyjne, a „zamknięci" w nich internauci mają podobne preferencje, poglądy i zainteresowania, które utrudniają prowadzenie demokratycznego sporu w ramach elektronicznej agory. Tym samym Internet, który miał umożliwić odrodzenie się autonomicznej, otwartej, krytycznej i racjonalnej debaty publicznej, stał się w ostatnich latach głównie przestrzenią dla lawinowo rozprzestrzeniającej się mowy szerzącej nienawiść, hejtu oraz całych narracji nienawiści. Stał się także przestrzenią dla informacji nieprawdziwych, wiadomości fałszywych i „zabarwionych" skrajnie negatywnymi emocjami, stereotypami i uprzedzeniami. Cyberprzestrzeń stała się miejscem kreowania postprawdy (d'Ancona, 2018). Postprawda (*post-truth*), w której fakty są mniej ważne w kształtowaniu opinii publicznej, a istotniejszą rolę odgrywają emocje i osobiste przekonania czy poglądy narratora, jest, zdaniem Timothy'ego Syndera, „przedfaszyzmem" (Synder, 2018, s. 71). Należy się zgodzić z wybranymi autorami (np. T. Synder, Matthew d'Ancona, Ralph Keyes, Timothy Garton Ash), iż postprawda nie jest czymś nowym, skoro już George Orwell kilkadziesiąt lat temu wspominał o „dwójmyśleniu", jednak Internet wzmocnił, utrwalił i „rozsławił" to zjawisko. We współczesnych, zarówno „starych", jak i „młodych" demokracjach obserwowany jest także silny trend odradzających się ekstremistycznych ideologii. Fenomen Facebooka czy Twittera powoduje, że każdy użytkownik może być źródłem informacji, stąd każdy może udostępniać wszelkie posty zawierające fałszywe i nienawistne informacje. Większość dostawców usług internetowych ma swoje siedziby w Stanach Zjednoczonych Ameryki Północnej, gdzie obowiązuje I Poprawka i doktryna tzw. wolnego rynku idei[4].

[4] Coraz częściej jednak ostatnio dochodzi do uwzględniania krajowych przepisów, szczególnie dotyczących szerzenia mowy rasistowskiej czy antysemickiej, która zgodnie z tradycją europejską jest penalizowana w krajowych systemach prawnych. Warto także wspomnieć o stronie internetowej *Redwatch Polska*, której celem było „monitorowanie czerwonych", tj. zbieranie i publikacja wszelkich możliwych informacji na temat osób trudniących się działalnością antyfaszystowską, antyrasistowską, kolorowych imigrantów, działaczy lewicowych stowarzyszeń i sympatyków oraz aktywistów LGBT. Ostatecznie autorzy treści (administratorzy) zostali skazani przez SO we Wrocławiu w 2010 r., jednak sama strona nadal była dostępna na liście w wyszukiwarce internetowej *Google*.

Zjawisko upowszechniania fałszywych wiadomości (*fake news*) nie jest niczym nowym, jednak rozwój technologiczny spowodował znaczny wzrost jego popularności[5]. Poprzez dostęp do technologii komputerowej zasięg zjawiska zmienił się z lokalnego na globalny, wzrosła ilość twórców i odbiorców, zmieniły się w jego następstwie także skutki ich działania w różnych obszarach życia publicznego: politycznym, społecznym czy gospodarczym. Należy zauważyć, iż fałszywe wiadomości stały się nieodłącznym elementem nowej formy manipulacji, tj. propagandy komputacyjnej. Zgodnie z ustaleniami Samuela C. Woolleya i Philipa N. Howarda, ten rodzaj propagandy oparty jest na nowoczesnych technikach obliczeniowych, jak: automatyczne boty, kampanie internetowe koordynowane przez trolle i ustrukturyzowane sieci fałszywych wiadomości (Woolley i Howard, 2019, s. 4).

Zjawiska te zbiegają się z innymi zjawiskami politycznymi i społecznymi, jak np. ze wzrostem populizmu w wielu państwach. Do władzy dochodzą politycy posługujący się retoryką ksenofobiczną, mizoginiczną, antyuchodźczą, antymigracyjną. Atrakcyjny dla wielu polityków i wyborców populizm, który zdaniem Jana Wernera Müllera jest nieodłącznym cieniem polityki przedstawicielskiej i niedostatków reprezentacji wyborców, stanowi jednak poważne zagrożenie zarówno dla liberalizmu, jak i samej demokracji. Politycy populistyczni odwołujący się do „mitycznego" ludu odrzucają jednocześnie jakiekolwiek inne poglądy. Przekaz populistyczny w szerokim zakresie wykorzystuje zarówno *fake news*, jak i narracje nienawistne. Populizm stanowi zagrożenie dla pluralizmu, który jest podstawą demokratycznego sporu (Müller, 2018, s. 141–145), bo stara się uprościć i zdominować inne narracje, odrzucając je jako nieuprawnione, czy wręcz szkodliwe dla „homogenicznego suwerena". Współczesne społeczeństwo, z jednej strony – jest zglobalizowanym i usieciowionym społeczeństwem informacyjnym, z drugiej zaś – społeczeństwem niepewności i ryzyka (Beck, 2012).

W latach sześćdziesiątych XX w. Marshall McLuhan twierdził, że na świecie tworzy się za sprawą mediów elektronicznych tzw. globalna wioska, kilka dekad później T.G. Ash polemizując z nim, stwierdził, że:

[5] Aby uwiarygodnić *fake news*, potrzebna jest duża liczba osób, które w niego „uwierzą" i przekażą go dalej. Między innymi z tego powodu zaczęły powstawać firmy oferujące powiększenie swojego zasięgu w Internecie. Firmy te oferują określoną ilość *followers* („zwolenników-wyznawców" danego posta), „lajków", komentarzy (zarówno negatywnych, jak i pozytywnych), a nawet rozpowszechnienie fali hejtu lub poparcia innym użytkownikom. Według Raportu Trend Micro, kupno *fake news* od firm specjalizujących się w tym np. w Rosji czy Chinach kosztuje 30 dolarów, a np. kampania dyskredytująca dziennikarza 55 tys. dolarów (*Trend Micro*, 2017, s. 58–60).

McLuhanowskie porównanie świata do 'globalnej wioski' nie jest trafne, ani jako opis, ani jako przepowiednia. Wioski to małe, zwykle jednorodne i konformistyczne miejsca. Tolerancja nie jest ich znakiem rozpoznawczym. […] Ani nie jesteśmy w 'globalnej wiosce', ani nie powinniśmy chcieć w niej być. Jako elektroniczni sąsiedzi żyjemy raczej w globalnym mieście. Z ludźmi pochodzącymi z innych krajów i kultur spotykamy się przez większość czasu tylko powierzchownie (w mieście). […] Podobnie jest w sieci. Oto świat-miasto (Ash, 2018, s. 35).

W tym „globalnym mieście" dochodzi coraz częściej do naruszeń praw podmiotowych jednych użytkowników przez drugich. Przede wszystkim najczęściej dochodzi do naruszenia prawa do prywatności. Powszechna staje się praktyka naruszająca własność intelektualną w cyberprzestrzeni, naruszana jest tajemnica elektronicznej korespondencji, stosowane są *phishing, cyberstalking, sniffing*[6], prowadzona jest inwigilacja[7], zakładane są fałszywe konta, przywłaszczane są cudze dobra osobiste. Powszechna jest w cyberprzestrzeni mowa rasistowska, antysemicka i inne rodzaje mowy nienawiści, w sposób nieuprawniony publikowane są fotografie bez zgody osób, których dotyczą. Pojawiły się pierwsze sprawy sądowe przeciwko portalom społecznościowym, w których użytkownicy domagali się usunięcia niezgodnych z prawdą treści na swój temat. Głośna stała się sprawa Anasa Modamaniego, który zrobił sobie selfie z Angelą Merkel w ośrodku dla uchodźców, a następnie stał się adresatem hejtu wśród użytkowników, którzy uznali, iż zdjęcie to jest przykładem „polityki zapraszania" terrorystów przez kanclerz do Niemiec[8]. Selfie z kanclerz Merkel posłużyło do rozpowszechniania tym samym *fake newsów* na temat samego Modamaniego. W wyroku sąd w Wuerzburgu (2017) stwierdził jednak, że Facebook nie był ani sprawcą, ani uczestnikiem „niekwestionowanego oczerniania", a portal służy wyłącznie jako narzędzie w rękach internautów, które samo w sobie nie ma obowiązku blokowania określonych treści.

[6] *Phishing* jest metodą oszustwa polegającą na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia informacji lub nakłonienia do określonych działań; *cyberstalking* jest formą elektronicznego nękania innej osoby; *sniffing* zaś to podsłuchiwanie w sieci tego, co jest publikowane w sieci, a co nie jest adresowane do podmiotu, który podsłuchuje.

[7] W 2013 r. skalę inwigilacji prowadzonej w Internecie przez amerykańskie służby ujawnił Edward Snowden, były współpracownik Agencji Bezpieczeństwa Narodowego USA. Stwierdził on, iż władze amerykańskie stworzyły programy, np. PRISM, które umożliwiają monitorowanie ruchu w sieci na całym świecie. Ponadto służby bezpośrednio podłączały się do kanałów komunikacyjnych największych firm teleinformatycznych. Po tych doniesieniach na nowo odżyły debaty o granicach praw człowieka w społeczeństwie informacyjnym, szczególnie o ochronie prywatności w cyberprzestrzeni.

[8] Modamani skasował konto na Facebooku i skierował sprawę do sądu w Wuerzburgu.

W poszukiwaniu nowego instrumentarium ochrony praw i wolności człowieka

W 2012 r. Rada Praw Człowieka ONZ wydała swoją pierwszą w historii rezolucję dotyczącą wolności w Internecie, uznając, że prawa i wolności człowieka powinny podlegać takiej samej ochronie zarówno *offline,* jak i *online*. Rada uznała też „globalną i otwartą naturę Internetu" oraz ochronę prawa dostępu do Internetu. Rezolucja została zainspirowana przez wydarzenia podczas tzw. Arabskiej Wiosny („twitterowe rewolucje"). W rezolucji Rada potwierdziła także, iż wolność słowa powinna być chroniona bez względu na granice i używane do tego celu media (zgodnie z art. 19 międzynarodowego paktu praw obywatelskich i politycznych), a państwa powinny promować i ułatwiać dostęp do Internetu oraz dążyć do współpracy mającej na celu rozwój technologii komunikacyjnych na całym świecie. Istotą tej rezolucji jest zatem twierdzenie, że prawa człowieka powinny być chronione tak samo w cyberprzestrzeni, jak i poza nią.

Na gruncie doktryny praw człowieka powszechny jest tradycyjny pogląd, iż prawa człowieka mają charakter wertykalny, bo występują wyłącznie w relacjach jednostki z państwem. Próby opisu stosunków pomiędzy ludźmi, opierające się na metodyce i terminologii praw człowieka, czyli tzw. horyzontalne działanie tych praw, zdaniem Marka Nowickiego, nie powiodły się, w związku z tym, gdy mowa jest o prawach człowieka, to chodzi zawsze o opis stosunków między człowiekiem a państwem (Nowicki, 1998, s. 8). Jak pisze Wiktor Osiatyński, przede wszystkim anglo-amerykańska doktryna liberalna z zasady odrzuca stosowanie praw człowieka w relacjach prywatnych, dopuszcza ją natomiast niemiecka teoria konstytucyjna (*Drittwirkung)*[9]. Jednakże, jak sam zauważa, coraz trudniej jest chronić czyjeś prawa naruszane przez korporacje transnarodowe, monopole informatyczne, ale i różne instytucje użyteczności publicznej:

[9] Według koncepcji *Drittwirkung* prawa człowieka działają nie tylko w relacji państwo – jednostka, ale także w relacji między jednostkami. Naruszenie praw człowieka może być więc udziałem zarówno państwa jako podmiotu zobowiązanego, jak i jednostek. Na gruncie międzynarodowej ochrony praw człowieka występuje koncepcja pośredniej horyzontalności oddziaływania norm praw człowieka *(indirect Drittwirkung)* i składa się z trzech elementów, tj. naruszenia przez podmiot prywatny normy na poziomie krajowym, następnie możliwości przypisania państwu obowiązku ochrony przed naruszeniem określonych praw człowieka przez inny podmiot prywatny oraz prawo jednostki pokrzywdzonej do zaskarżenia przed odpowiednim trybunałem państwa, które takiemu naruszeniu nie zapobiegło (Balcerzak i Sykuna, 2010, s. 69–70).

Nowe metody nadzoru, specjalne techniki, internetowy dostęp do danych osobowych, i liczne technologie wykorzystywane przez korporacje, media i przestępców stwarzają bezprecedensowe zagrożenie prywatności i innych praw. Powstaje więc pytanie: czy prawa człowieka mają zastosowanie w stosunkach między jednostkami, które nie wykorzystują władzy państwowej? (Osiatyński, 2011, s. 305).

Doktryna *Drittwirkung* jest odpowiedzią na sytuację, w której jednostka nie tylko wymaga ochrony przed działaniami państwa, ale także innych jednostek. Dochodzi do rozszerzenia w tej doktrynie odpowiedzialności państwa na działania innych podmiotów prywatnych (jednostek niepaństwowych – *non state actors*); obecnie mogą to być korporacje transnarodowe, organizacje terrorystyczne, media elektroniczne. Należy jednak zauważyć, iż część autorów twierdzi, iż przypisanie odpowiedzialności państwu za działania innych podmiotów prywatnych może i powinno odbywać się w ramach tzw. jego pozytywnych obowiązków, czyli podjęcia określonych działań przez państwo w celu poszanowania i ochrony praw człowieka. I tak Europejski Trybunał Praw Człowieka w Strasburgu wskazywał, iż na państwie członkowskim spoczywa pozytywny obowiązek stworzenia np. ram prawnych w celu zapewnienia efektywnej ochrony swobody wypowiedzi dziennikarzy, w tym ostatnio także dziennikarzy publikujących w Internecie (sprawa *Editorial Bard of Pravoye Delo i Shtekel przeciwko Ukrainie,* 2011). To bardzo istotne zalecenie sędziów Trybunału, gdyż w okresie tak szybkiego postępu technologicznego, jaki dokonuje się od kilkunastu lat na świecie, i szybkiego upowszechnienia się usług internetowych wciąż brak jest regulacji prawnych wielu zagadnień związanych z jego funkcjonowaniem. Przykładowo, długo oczekiwaną regulacją prawną na poziomie całej Unii Europejskiej w zakresie wzmocnienia ochrony danych osobowych było rozporządzenie z 2016 r. w sprawie ochrony osób fizycznych (RODO)[10].

RODO wprowadziło szereg nowych narzędzi ochrony danych osobowych osób, których informacje te dotyczą. Wprowadzone narzędzia prawne mają na celu wzmocnienie ochrony tych danych poprzez: prawo do usunięcia danych (prawo do bycia zapomnianym – *right to be forgotten)*, łatwiejszy dostęp do danych, gdyż osoby, których dane dotyczą, będą miały dostęp do szerszego zakresu informacji o przetwarzaniu ich danych, a także poprzez obowiązek informowania o naruszeniu danych oraz, co jest szczególnie istotne z punktu widzenia ochrony najmłodszych, silniejszą ochronę praw dzieci. W RODO słusznie przyjęto zało-

[10] Tj. rozporządzenie z 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.

żenie, iż dzieci mogą być w mniejszym stopniu świadome zagrożeń, konsekwencji i gwarancji swoich praw w odniesieniu do przetwarzania danych osobowych. Rozporządzenie przewiduje zgodę rodziców na przetwarzanie danych dziecka, które nie ukończyło 16 lat. Wprowadzono także przepis umożliwiający egzekucję przestrzegania przepisów w ten sposób, że polski organ ochrony danych jest wyposażony w możliwość nakładania administracyjnych kar pieniężnych w wysokości nawet do 20 mln euro lub do 4% całkowitego rocznego światowego obrotu.

Na gruncie prawa europejskiej konwencji praw człowieka i podstawowych wolności w Radzie Europy aktywną rolę w wyznaczaniu nowych standardów pełni Europejski Trybunał Praw Człowieka. Trybunał zadecydował też, że prawa zawarte w konwencji z 1950 r. nakładają na państwa obowiązek podjęcia „kroków zmierzających do zagwarantowania poszanowania prywatności także w stosunkach między osobami prywatnymi" (Osiatyński, 2011, s. 308). Podobnie problematykę „prawa poszanowania prawa do prywatności" w relacjach horyzontalnych szczegółowo opisuje Monika Florczak-Wątor. Wprawdzie europejska konwencja z 1950 r. miała być instrumentem ochrony praw i wolności w stosunkach wertykalnych (co potwierdzał jej art. 1)[11], jednak obowiązek zapewnienia przez państwo poszanowania prywatności w stosunkach horyzontalnych był jednym z pierwszych obowiązków pozytywnych o charakterze ochronnym sformułowanych przez Trybunał. Wynika to zresztą *expressis verbis* z orzecznictwa Trybunału, który twierdzi, iż konwencja określana jest mianem „żywego instrumentu" (*living instrument*), który powinien dostosowywać się do zmian zachodzących we współczesnym świecie niezależnie od tego, czy były one przewidywane w okresie, gdy konwencję w obecnym brzmieniu przyjmowano. Wydaje się więc, że tego rodzaju zmianą, która wymagała uwzględnienia w stosowaniu konwencji, jest właśnie ta dotycząca źródła zagrożeń dla praw człowieka, czyli obecnie Internetu. Prawo do poszanowania prywatności, co jest bezsprzeczne, coraz częściej jest naruszane przez podmioty prywatne, a to po stronie państwa rodzi obowiązek zapewnienia rzeczywistej i skutecznej ich ochrony. Stąd też w orzecznictwie ETPC została sformułowana koncepcja obowiązków pozytywnych państwa jako tych, które uzupełniają obowiązki o charakterze negatywnym. Spostrzeżenie, że prawa chronione konwencją mogą zostać naruszone przez podmioty prywatne, miało kluczowe znaczenie dla rozwoju koncepcji obowiązków ochronnych państwa.

[11] Art. 1 zobowiązuje państwa jako „Wysokie Układające się Strony" do zapewnienia każdemu człowiekowi praw i wolności określonych w konwencji.

Wreszcie, art. 17 Konwencji (koncepcja zakazu nadużywania prawa) stanowi, iż żadne z jej postanowień nie może być interpretowane jako przyznanie jakiemukolwiek państwu, grupie lub osobie prawa do podjęcia działań lub dokonania aktu zmierzającego do zniweczenia praw i wolności wymienionych w niniejszej konwencji albo ich ograniczenia w większym stopniu niż to przewiduje konwencja. Tym samym, przepis ten *expressis verbis* wymienia, obok państwa, także osoby i grupy osób jako podmioty, które swoim działaniem mogą niweczyć prawa i wolności konwencyjne albo ograniczać je w niedopuszczalnym stopniu (Florczak-Wąter, 2015, s. 188–189). I tak, należy się spodziewać, iż skargi, w których skarżący domagają się ochrony wypowiedzi ksenofobicznych, rasistowskich czy innych propagujących nienawiść, będą odrzucane przez Trybunał jako niedopuszczalne. Dzieje się tak od lat, jednakże w ostatnich latach takich skarg jest więcej w związku z upowszechnieniem się elektronicznej komunikacji *via* Internet. Kancelaria Europejskiego Trybunału Praw Człowieka we wrześniu 2019 r. opublikowała przewodnik ilustrujący orzecznictwo z art. 17 Konwencji (*Guide on Article 17 of the European Conventionon Human Rights. Prohibition of abuse of rights*, 2019*)*.

Znany jest również pogląd (Lecha Garlickiego), zgodnie z którym tekst europejskiej konwencji daje możliwość interpretacji niektórych jej postanowień w sposób nakładający obowiązki nie tylko na państwa członkowskie, ale również, pośrednio, na osoby prywatne, co nie oznacza, że niedopełnienie tych obowiązków przez podmiot prywatny i tym samym naruszenie praw człowieka innego podmiotu może być dochodzone w postępowaniu przed Trybunałem. Jedynym sposobem zaskarżenia naruszenia jest wtedy powiązanie go z działaniem (zaniechaniem) państwa i przypisanie odpowiedzialności za nie państwu, czyli w praktyce jest to koncepcja obowiązków pozytywnych państwa (Florczak-Wąter, 2015, s. 191–192). Innym natomiast argumentem, który może przemawiać za horyzontalnym działaniem praw człowieka, jest ich cel (Andrzejczuk, 2006, s. 74). Ochrona praw człowieka jest sprawą fundamentalną, podstawową dla każdego człowieka, ale także warunkiem koniecznym dla funkcjonowania demokratycznego państwa prawa.

Przed sądami i trybunałami (ETPCz, TSUE) coraz więcej pojawia się więc skarg na naruszenie praw człowieka w cyberprzestrzeni. Sprawy te przede wszystkim występują w kontekście ochrony prywatności i ochrony wolności wypowiedzi. Omówienie albo próba zasygnalizowania różnorodności spraw, jakie wpływają do europejskich trybunałów, znacznie wykracza poza ramy tego artykułu. Zasygnalizowane będą jedynie niektóre z nich. Na uwagę zasługuje wyrok w sprawie *Centrum*

för Rättvisa (2018). W związku z doniesieniami Edwarda Snowdena do ETPC trafiło wiele spraw dotyczących szerokiego stosowania inwigilacji przez władze krajowe. W sprawie *Centrum för Rättvisa* Trybunał stwierdził, iż masowe przechwytywanie komunikacji w Szwecji jest zgodne ze standardami europejskiej konwencji. Skarga dotyczyła naruszenia art. 8 Konwencji (prawo do poszanowania życia prywatnego)[12]. Jak zauważa Dominika Bychawska-Siniarska, sprawa szwedzka jest wyrazem poważnego odejścia od dotychczasowego orzecznictwa. Trybunału uznał, że system pozwalający na masowe gromadzenie danych telekomunikacyjnych przez służby stanowi naruszenie art. 8 Konwencji (Prosto ze Strasburga, 2019).

W 2014 r. zapadł inny głośny wyrok przed Trybunałem Sprawiedliwości Unii Europejskiej w sprawie *Google Spain SL i Google Inc. Przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González* (*Google v. Agencia Española de Protecc*ón *de Datos (AEPD) i Mario González* (2014). Wyrok TSUE z dnia 13 maja 2014, sygn. C-131/12).

Trybunał wypowiedział się w nim co do nowego, proponowanego rozwiązania, jakim stało się „prawo do bycia zapomnianym"[13]. TSUE orzekł, że Google obowiązany jest usunąć link z informacją dotyczącą obywatela Hiszpanii z list wyników wyszukiwania wszystkich swoich wyszukiwarek na terenie UE. To bardzo ważny wyrok, w którym Trybunał wypowiedział się co do prawa jednostki do kontroli informacji o sobie w cyberprzestrzeni. Jak już wspomniano, od maja 2018 r. obowiązuje regulacja RODO i prawo do usunięcia danych osobowych

[12] *Centrum för Rättvisa*, pozarządowa organizacja prawnicza ze Szwecji, argumentowało, że wprowadzone w 2008 r. prawo umożliwiające przechwytywanie komunikacji elektronicznej na rzecz służb wywiadu stanowi naruszenie prawa do prywatności. Ponadto ETPC uznał, że szwedzka „ustawa inwigilacyjna" wprowadzała adekwatne i wystarczające gwarancje przeciwdziałające arbitralności i ryzyku nadużyć. W związku z przeciwdziałaniem terroryzmowi oraz ponadgranicznej przestępczości zorganizowanej państwo musi dysponować szerokim marginesem uznania przy wprowadzaniu regulacji odnoszących się do kontroli operacyjnej (za: Bychawska-Siniarska, Prosto ze Strasburga, 2018). Trybunał wziął pod uwagę władzę dyskrecjonalną państwa w ochronie bezpieczeństwie narodowego i aktualne zagrożenia globalnym terroryzmem i innymi przestępstwami transgranicznymi.

[13] W 2010 r. obywatel Hiszpanii M.C. González wystąpił do organu ochrony danych ze skargą dotyczącą informacji opublikowanej w 1998 r. przez dziennik *La Vanguardia*, żądając jej usunięcia ze strony internetowej gazety i wyszukiwarki Google. Organ ochrony danych uznał, że gazeta nie musi usuwać pierwotnej publikacji, ponieważ ukazała się zgodnie z prawem, natomiast Google musiał usunąć prowadzące do niej linki. Google odwołał się do hiszpańskiego sądu krajowego najwyższej instancji, który przekazał sprawę do Trybunału Sprawiedliwości UE.

(„prawo do bycia zapomnianym"), wynikające *expressis verbis* z art. 17 RODO. I tak osoba, której dotyczą dane, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe. Obowiązek ten powstaje w wymienionych w RODO sytuacjach[14]. Administrator, który upublicznił dane osobowe, ma także obowiązek poinformować innych administratorów, aby i oni usunęli stosowne linki, kopie i odniesienia do danych, które mają być usunięte.

Trybunał w Strasburgu wielokrotnie wypowiadał się także na temat ochrony wolności słowa w sieci. Po pierwsze – uznał, że na państwach spoczywa pozytywny obowiązek stworzenia ram prawnych w celu efektywnej ochrony swobody wypowiedzi dziennikarzy publikujących w Internecie, po drugie – ochrona publikacji internetowych musi być traktowana na równi z publikacjami w mediach tradycyjnych (*Editorial Board of Pravoye Delo i Shtekel przeciwko Ukraina,* 2011), po trzecie – Trybunał konsekwentnie odmawia przyznania ochrony mowie nienawiści, dopuszczając nawet karę więzienia za jej stosowanie (*Cumpana i Mazare przeciwko Rumunia,* 2004; *Raichinov przeciwko Bułgaria,* 2006). Ponadto stwierdził, że konwencja nie chroni wypowiedzi ksenofobicznych i rasistowskich w Internecie oraz podkreślił potrzebę walki z dyskryminacją rasową i ksenofobią *(Feret przeciwko Belgia,* 2009).

W jednej z ostatnich spraw z czerwca 2018 r. ETPCz wypowiedział się też w sprawie zakresu ochrony danych osobowych w sieci, a dokładnie w internetowych archiwach gazet. W sprawie *M. L. i M. W. przeciwko Niemcom* (2018) Trybunał nie dopatrzył się naruszenia[15], ale przypo-

[14] Dane osobowe nie są już niezbędne do celów, do których je zebrano, gdy podmiot danych wycofał zgodę i nie istnieje inna podstawa prawna dla przetwarzania tych danych, albo kiedy podmiot danych wniósł sprzeciw do dalszego przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania. Administrator powinien usunąć dane osobowe przetwarzane niezgodnie z prawem oraz kiedy zostały zebrane w celu świadczenia usług internetowych dziecku. Wreszcie, dane osobowe muszą być usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w unijnym bądź krajowym przepisie prawnym

[15] M. L. i M. W. zostali skazani na karę dożywotniego pozbawienia wolności za zabójstwo popularnego aktora W. S., a następnie zwolnieni z zakładu karnego na przełomie 2007 i 2008 r. na okres próby. W 2007 r. wnieśli sprawę przeciwko stacji *Deutschlandradio*, domagając się zanonimizowania archiwalnego materiału na stronie internetowej stacji. Materiał informował o bezskutecznej próbie wznowienia postępowania przez M. L. i M. W. Sądy krajowe uznały, że ze względu na czas, jaki upłynął od skazania, jak również braku interesu społecznego w ujawnieniu ich danych stacja powinna zadbać o ochronę danych osobowych skazanych; jednakże Federalny Sąd Konstytucyjny uchylił decyzję, wskazując, że sąd apelacyjny nie wziął pod uwagę wolności słowa stacji radio-

mniał o obowiązku wyważenia wolności słowa i prawa do poszanowania prywatności. Stwierdził, że media mają prawo do informowania w Internecie o ważnych sprawach społecznych, ale muszą to robić z poszanowaniem prywatności i danych osobowych opisywanych osób.

Zakończenie

Rozwój społeczeństwa informacyjnego stał się nowym wyzwaniem dla poszanowania praw i wolności człowieka, w tym szczególnie dla wolności wypowiedzi i prawa do prywatności. To te dwa prawa stały się szczególnie wrażliwe na oddziaływanie nowoczesnych technologii. Powszechne stało się udostępnianie dezinformacji, fałszywych wiadomości, mowy nienawiści w cyberprzestrzeni. Powszechne także stało się profilowanie danych osobowych internautów, którzy jeszcze do niedawna nie mieli skutecznych instrumentów prawnych przeciwdziałających gromadzeniu i przekazywaniu administratorom własnych danych osobowych i preferencji związanych z dokonywanymi zakupami online. Komercjalizacja i pauperyzacja Internetu przyniosła zarówno pozytywne, jak i negatywne konsekwencje. Do tych drugich przede wszystkim należy zaliczyć coraz powszechniejsze zjawisko naruszania i nadużywania wolności wypowiedzi i prawa do prywatności w wymiarze horyzontalnym. Uzasadniony jest postulat o większej aktywności państwa w ramach pozytywnych obowiązków odnośnie do przeciwdziałania ich naruszaniu w cyberprzestrzeni. Zwraca na to Europejski Trybunał Praw Człowieka w Strasburgu. Warto także zauważyć, iż brak regulacji w wielu kwestiach związanych z nowoczesnymi technologiami sprawia, że na sądach krajowych i międzynarodowych spoczywa obecnie obowiązek kształtowania ram odpowiedzialności prawnej z tytułu naruszenia wolności wypowiedzi czy prawa do prywatności.

Yochai Benkler twierdzi, że wolność jest nierozerwalnie związana z różnorodnością ograniczeń, a nie z optymalną równowagą wolności i ograniczeń, symbolizującą jeden jedyny układ instytucjonalny. To właśnie ta wielorakość ograniczeń umożliwia, jego zdaniem, jednostkom planowanie różnych fragmentów i aspektów życia w różnych kontekstach instytucjonalnych, korzystania z różnego stopnia wolności i bezpieczeństwa, które są w nich możliwe (Benkler, 2008, s. 164). Stąd, w ramach skuteczniejszej ochrony praw człowieka w cyberprzestrzeni powinny być podjęte działania w zakresie wieloaspektowego instrumen-

wej. Podobne postępowania zostały wniesione przeciwko tygodnikowi *Der Spiegel* i dziennikowi *Mannheimer Morgen* (Prosto ze Strasburga, 2018).

tarium prawnego, politycznego, informatycznego (technologicznego) oraz edukacyjnego. Oprócz twardych regulacji prawnych (np. RODO, które jest swoistą „rewolucją" w dziedzinie ochrony danych osobowych w sieci), w Internecie powinny być także upowszechniane instrumenty miękkie (*soft law),* tj. np. etykieta czy regulaminy różnych kanałów komunikacyjnych. W ramach instrumentarium politycznego powinny być podjęte także działania władz publicznych. W kwietniu 2018 r. zorganizowano spotkania z Markiem Zuckerbergiem w Kongresie USA i Parlamencie Europejskim w Brukseli dotyczące wycieku danych osobowych ponad 50 mln użytkowników w latach ubiegłych. Spotkania te dały początek nowemu podejściu w zakresie ochrony praw jednostek przed nieuprawnioną ingerencją zarówno ze strony władz publicznych, ale przede wszystkim podmiotów niepaństwowych, tj. innych internautów, sztucznej inteligencji czy komercyjnych podmiotów. Spotkania Zuckerberga w Waszyngtonie i Brukseli zainicjowały także większe zaangażowanie władz krajowych w kształtowanie nowych regulacji dotyczących nadużyć w Internecie. Warto wspomnieć o nowej inicjatywie Komisji Europejskiej w 2018 r. w celu wypracowania przez grupę wysokiego szczebla ds. *fake news* z udziałem EURACTIV *(HLEG – High Level Export Gropu on Fake News and Online Disinformation)*[16] mechanizmu skuteczniejszego przeciwdziałania fałszywym informacjom w cyberprzestrzeni. W 2016 r. przyjęto kodeks postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w Internecie, a w 2018 r. przyjęto kodeks postępowania w zakresie zwalczania dezinformacji *(Code of Practice on Disinformation).*

Istotne są wreszcie instrumenty technologiczne, w ramach których konieczne jest opracowanie nowych algorytmów, budowanie serwisów *fact-checking* i tzw. *slow news*, za pomocą których użytkownik otrzymuje odnośnik do zweryfikowanej informacji i ocenę stopnia jej wiarygodności. I tak, przykładowo, *The Washington Post* od 2016 r. wprowadził mechanizm *fact-checker*, który na bieżąco weryfikuje wszystkie wypowiedzi publiczne Donalda Trumpa.

[16] Prace HLEG poprzedziły konsultacje publiczne na temat *fake news* i dezinformacji w Internecie przeprowadzone w okresie od listopada 2017 do lutego 2018 r. Grupa 39 ekspertów opracowała wielowymiarowe podejście do przeciwdziałania temu zjawisku poprzez: poprawę przejrzystości wiadomości *online* (z poszanowaniem prywatności), promowanie umiejętności korzystania z mediów i informacji, opracowanie narzędzi umożliwiających użytkownikom i dziennikarzom walkę z dezinformacją i sprzyjanie pozytywnemu zaangażowaniu w szybko rozwijające się technologie informacyjne, zagwarantowanie różnorodności i trwałości europejskiego ekosystemu mediów informacyjnych oraz promowanie ciągłych badań nad wpływem dezinformacji w Europie na ocenę działań podejmowanych przez różne podmioty i stałe dostosowywanie niezbędnych reakcji.

Szczegółowe omówienie podejmowanych coraz aktywniej działań firm informatycznych i władz publicznych związanych z zapewnieniem ochrony wolności wypowiedzi i prawa do prywatności wykracza poza ramy tego artykułu. Zaprezentowane jednak zostały te najważniejsze, aktualne refleksje związane z wpływem rozwoju społeczeństwa informacyjnego na kondycję wybranych praw człowieka.

Bibliografia

Andrzejczuk, R. 2006. Nadużycie prawa w świetle art. 17 europejskiej konwencji praw człowieka. *Roczniki Nauk Prawnych*, *XVI*(1), 69–80.

Balcerzak, M. i Sykuna, S. (2010). *Leksykon ochrony praw człowieka*. Warszawa: C.H. Beck.

Bąk, A. (2016). Serwisy społecznościowe – efekt Facebooka i nie tylko, *Media i Społeczeństwo*, (6), 134–146.

Beck, U. (2012). *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Warszawa: Scholar.

Bednarek, J., Andrzejewska, A., Bąkiewicz, M. i Lizut, J. (red.). (2013). *Zagrożenia cyberprzestrzeni*, Warszawa: Pobrane z: https://cyberprzestrzen.wspkorczak.eu/download/dokumenty/podrecznik_zagrozenia_cyberprzestrzeni.pdf

Bendyk, E. (2018). Nowa republika sieci. *Polityka* (20), s. 71–74.

Benkler, Y. (2008). *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność,* Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Bodnar, A. i Bychawska-Siniarska, D. (2010). *Prawo w sieci – korzyści czy zagrożenia dla wolności słowa?* Warszawa: Helsińska Fundacja Praw Człowieka.

Bodnar, A. i Ziółkowski, M. (2008). Zgromadzenia spontaniczne. *Państwo i Prawo*, (5), 38–50.

Bychawska-Siniarska, D. i Głowacka, D. (red.). (2014). *Wirtualne media – realne problemy*. Warszawa: Helsińska Fundacja Praw Człowieka.

Castells, M. (2003). *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, Poznań: Rebis.

Castells, M. (2013). *Sieci oburzenia i nadziei. Ruchy społeczne w erze Internetu*, Warszawa: Wydawnictwo Naukowe PWN.

Centrum för Rättvisa przeciwko Szwecji. (2018). Wyrok ETPCz z 19 czerwca 2018, skarga nr 35252/08.

Cumpana i Mazare przeciwko Rumunia. (2004). Wyrok ETPCz z 17 grudnia 2004, nr 33348/95.

d'Ancona, M. (2018). *Postprawda*, Warszawa: Wydawnictwo Krytyki Politycznej.

Demczuk, A. i Pawłowska, A. (2009). Prawo dostępu do sieci teleinformatycznej oraz usług świadczonych drogą elektroniczną w międzynarodowym systemie ochrony praw człowieka. W: A. Pawłowska (red.), *Rola Unii Europejskiej i stanów Zjednoczonych w rozwoju międzynarodowych stosunków gospodarczych i politycznych* (s. 133–148). Lublin: Wyższa Szkoła Przedsiębiorczości i Administracji.

Drożdż, M. (2016). Język nienawiści w dyskursie medialnym. *Acta Universitatis Lodziensis. Folia Litteraria Polonica, 31*(1), 21–32.

Editorial Board of Pravoye Delo i Shtekel przeciwko Ukraina. (2011). Wyrok ETPCz z 5 maja 2011, skarga nr 33014/05.

European Commission. (2018). *A multi-dimensional approach to disinformation*. Pobrane z: https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

Feret przeciwko Belgia. (2009). Wyrok ETPCz z 16 lipca 2009, skarga nr 15615/07

Florczak-Wątor, M. (2014). *Horyzontalny wymiar praw konstytucyjnych*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.

Goban-Klas, T. i Sienkiewicz, P. (1999). *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*. Kraków: Wydawnictwo Fundacji Postępu Telekomunikacji.

*Google v. Agencia Española de Protecc*ón *de Datos (AEPD) i Mario González* (2014). Wyrok TSUE z dnia 13 maja 2014, sygn. C-131/12.

Guide on Article 17 of the European Conventionon Human Rights. Prohibition of abuse of rights. (2019). Pobrane z: https://www.echr.coe.int/Documents/Guide_Art 17 _ENG.pdf

Gu L., Kropotov V., Yarochkin F., *The Fake News Machine. How Propagandists Abuse the Internet and Manipulate the Public*, „Raport dla Trend Micro" z 2017. Pobrane z: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf

Habermas, J. (2005). *Filozoficzny dyskurs nowoczesności*. Kraków: Universitas.

Keyes, R. (2018). *Czas postprawdy. Nieszczerość i oszustwa w codziennym życiu*. Warszawa: Wydawnictwo PWN.

Kodeks postępowania w zakresie zwalczania dezinformacji (2018). Digital Single Market. , https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454

Kodeks postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie (2016) Digital Single Market. Pobrane z: https://ec.europa.eu/newsroom/document.cfm?doc_id=42869

Łakomy J. (2010). Prawa człowieka w perspektywie interdyscyplinarnej. *Wrocławskie Studia Erazmiańskie*, *IV*, 131–151.

M. L. i M. W. przeciwko Niemcom (2018). Wyrok ETPCz z 28 czerwca 2018, skarga nr 60798/10 i 65599/10.

McLuhan, M. (1999). *Nowa era komunikacji*. Warszawa: Prószyński i S-ka.

Nowicki, M. (1998). Co to są prawa człowieka*? Szkoła Praw Człowieka HFPC. Teksty wykładów* (1), s. 5–12.

Osiatyński, W. (2011). *Prawa człowieka i ich granice*. Kraków: Społeczny Instytut Wydawniczy Znak.

Pawłowska, A. (2002). *Zasoby informacyjne w administracji publicznej w Polsce. Problemy zarządzania*. Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej.

Pismo Rzecznika Praw Obywatelskich do Generalnego Inspektora Danych Osobowych z 30 marca 2018, nr VII.520.14.2018.AG

Prosto ze Strasburga – omówienie wyroków Europejskiego Trybunału Praw Człowieka. Pobrane 24 kwietnia 2020 z: http://www.wyrokietpc.pl/page/2/

Ptaszek G., *Edukacja medialna 3.0. Krytyczne rozumienie mediów cyfrowych w dobie Big Data i algorytmizacji*, Kraków 2019.

Raichinov przeciwko Bułgaria. (2006). Wyrok ETPCz z 20 kwietnia 2006, skarga nr 47579/99.

Rozporządzenie PE i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobod-

nego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. (Dz. Urz. UE L 119 z 4 maja 2016).

Sprawa *Editorial Bard of Pravoye Delo i Shtekel przeciwko Ukrainie* (2011). Wyrok ETPC z maja 2011, skarga nr 33014/05.

Synder, T. (2017). *O tyranii*. Kraków: Znak Horyzont.

Świeboda, H. (2013). Problem prywatności w społeczeństwie informacyjnym. *Ekonomiczne Problemy Usług* (105), 93–103.

We Are Social, Global Digital Report 2018, 2018, https://digitalreport.wearesocial.com/

We Are Social, Global Digital Report 2019, 2019, https://digitalreport.wearesocial.com/

Wiczanowska, H. (2019). Klauzula zakazu nadużywania praw jako quasi-wyjątek od konieczności ochrony praw jednostki. Rozważania z perspektywy uniwersalnego systemu ochrony praw człowieka. *Polityka i Społeczeństwo*, *17*(1), 56–68.

Woolley, S.C. & Howard, P.N. (Eds.). (2019). *Computational Propaganda. Political parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford Scholarship Online.

Data przekazania tekstu: 19.10.2019 r.; data zaakceptowania tekstu: 12.12.2019 r.