Katarzyna Chałubińska-Jentkiewicz*

Dezinformacja jako akt agresji w cyberprzestrzeni

Streszczenie

Fundamentalnym elementem bezpieczeństwa oraz poczucia braku zagrożenia jest ich społeczne komunikowanie. Wraz z rozwojem społeczeństw, postępem związanym z procesami cyfrowymi i informatyzacją w obszarze komunikowania oraz łatwością przekazywania informacji i danych, personalizacją przekazu, która prowadzi jednocześnie do zupełnie nowych form aktywności, coraz większą rolę zaczęły odgrywać media społecznościowe oraz przekazy, które nie mają charakteru powszechnego odbioru. Dotyczy to wszelkich zdarzeń i zjawisk związanych ze sferą publiczną i oddziaływaniem na sferę publiczną, sposobów oceny przez określone grupy społeczne lub społeczeństwa jako prawdziwe, z którymi mogą się utożsamiać.

Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo, dezinformacja, media

* Dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj, Instytut Prawa, Akademia Sztuki Wojennej w Warszawie, kierownik Katedry Prawa Mediów, Własności Intelektualnej i Nowych Technologii, e-mail: kasiachalubinska@gmail.com.

Media i bezpieczeństwo

Można powiedzieć, iż rola mediów przy definiowaniu kwestii bezpieczeństwa jest powiązana ze społecznym wymiarem definiowania zagrożeń, ich identyfikowaniem i neutralizowaniem. Poszerzenie sfery bezpieczeństwa państwa i obywateli o obszar przestrzeni wirtualnej oraz odniesienie do cyberbezpieczeństwa jest naturalną konsekwencją rozwoju technologii komunikacyjnych i sprzężonych z nimi zjawisk społecznych skupionych wokół pozyskiwania, przetwarzania i dystrybuowania informacji. Taki schemat z reguły prowadzi do określonych potrzeb zmian prawnych i redefinicji celów interesu publicznego, które realizuje się m.in. przy pomocy instrumentów normatywnych. Media się przeobrażają i powstaje problem ich definiowania. Według D. Merscha „odpowiednio wieloznaczna jest lista tego, co zostało określone mianem »media« – są to klasyczne środki komunikacji, takie jak ciało, głos i pismo; technologie, jak druk książek, drzeworyt, fotografia lub płyta winylowa; środki komunikacji masowej – radio, film, telewizja; albo najogólniej rozumiane instrumenty, jak narzędzia, próbki, preparaty i aparaty". M. McLuhan używa pojęcia mediów dla określenia tak różnorodnych artefaktów, jak broń, odzież, zegarki, pieniądze, okulary, domy lub środki wentylacji (wymienia 26 rodzajów mediów), według J. Beaudrillarda są to dobra konsumpcyjne, a P. Virilio rozumie przez nie wehikuły wszelkiego rodzaju, w tym powozy, samochody i samoloty, z kolei według H. Innisa są one materialnymi nośnikami informacji, a F.A. Knitter ograniczył pojęcie mediów niemal wyłącznie do aparatów technicznych i ich operatorów, takich jak przekaźniki, tranzystory i systemy hardware'owe komputerów różnych generacji[1]. Zdaniem autora media to: „Ni to jednostkowość, ni ogólność, ni forma, ni materia, ni postać, ni treść, ni figura, ni tło – zajmuje przestrzeń nieokreśloną, wymykającą się zwykłym podziałom"[2]. Ze względu na powszechność internetu i cyfrowego przekazywania informacji – klasyczne media takie jak prasa, radio i telewizja zostały rozszerzone o portale informacyjne, społecznościowe, blogi, platform do umieszczania materiałów video umożliwiających jednocześnie wymianę opinii, odczuć i spostrzeżeń – informacji. Internet stał się miejscem do tworzenia własnych przestrzeni informacyjnych, jednocześnie nowych form mediów i nowej sfery publicznej, nie znającej granic terytorialnych, przeszkód językowych czy narodowych. Taki wymiar często

1 M. Mersch, *Teorie mediów*, Warszawa 2010, s. 8.
2 Ibidem, s. 27.

niekontrolowanego rozszerzenia przestrzeni medialnej wymaga nowego podejścia regulacyjnego pod względem nowych metod i technik zapewniania bezpieczeństwa. Nowe formy zagrożeń wynikających ze złośliwego oprogramowania, kradzieży tożsamości w sieci, podszywania się pod oficjalne strony internetowe czy *phishing'u* tworzą całkiem nowe sposoby pozyskiwania informacji, także nielegalnego, w tym do kreowania nowych sytuacji sprzyjających konkretnym grupom interesu – również aktorom państwowym w kontekście relacji międzynarodowych. Siły zbrojne poszczególnych państw zaczynają organizować wojska zajmujące się ochroną cyberprzestrzeni – zwłaszcza powiązanej z klasycznymi instytucjami bezpieczeństwa państwa i innych jego sfer wpływających na codzienne życie obywateli. Odnosi się to również do negatywnego wykorzystania mediów cyfrowych i ich użytkowników. W socjologii podkreśla się znaczenie twierdzenia W.I. Thomasa, które wskazuje, że „jeśli ludzie definiują sytuacje jako rzeczywiste, to stają się one sytuacjami rzeczywistymi"[3]. M. Castells nową internetową rzeczywistość medialną nazywa: „masową komunikacją zindywidualizowaną, która w znaczny sposób zwiększyła autonomię komunikowania podmiotów wobec korporacji komunikacyjnych, ponieważ użytkownicy stali się jednocześnie nadawcami i odbiorcami przekazów"[4]. W obszarze kwestii bezpieczeństwa, jeżeli dane zagrożenie jest źle zidentyfikowane od samego początki, np. pod wpływem przedstawiania różnych domniemań jako fakty, wówczas przedsięwzięte środki, które mają konkretny wymiar obiektywny, nie są adekwatne do realnego zagrożenia. Jeżeli dochodzi do jakiegokolwiek zdarzenia, w którym giną ludzie, jak katastrofy budowlane, wypadki samochodowe, zbiorowe morderstwa dokonywane przez osoby chore psychicznie, wówczas pierwsze pytanie lub hipoteza dziennikarza z reguły dotyczy możliwości ataku terrorystycznego[5]. Zagadnienie bezpieczeństwa jako pojęcia niedookreślonego jest bardzo szerokie i stanowi wypadkową szerszych procesów, w ramach których media cyfrowe tworzą platformę wymiany informacji, poglądów i odczuć pomiędzy wszystkimi uczestnikami rynku cyfrowego i cyberprzestrzeni. Niezwykle ważne jest koordynowanie przekazów medialnych w sytuacjach kryzysowych z oficjalnymi komunikatami administracji publicznej zajmującej się bezpieczeństwem państwa i obywateli. Koordynacja ta przede wszystkim powinna polegać na wzmacnianiu zasięgów oficjalnych

3 R.K. Merton, *Samospełniające się proroctwo* [w:] red. P. Sztompka, M. Kucia, *Socjologia*, Kraków 2006, s. 361.
4 M. Castells, *Władza komunikacji*, Warszawa 2013, s. 16.
5 M. Ciesielski, *Terroryzm i media w kontekście paniki moralnej*, „Bellona" 2012, nr 2, s. 176–177.

komunikatów, ale w szczególności na eliminowaniu nieuprawnionych nadinterpretacji ze strony osób niekompetentnych, które mogłyby zdestabilizować poszczególne społeczności lub całe społeczeństwo. Problem z nowoczesnymi mediami polega na tym, że nie wiemy, jak zdefiniować nowoczesność mediów. Według Leszka Kołakowskiego: „Nie wiedząc, czym jest 'nowoczesność', próbujemy ostatnio odejść od naszego pytania i mówić o 'postmodernizmie' (jest przedłużeniem lub imitacją nieco starszych określeń, takich jak 'społeczeństwo postindustrialne', 'postindustrialne' – kapitalizm itp.)"[6]. A. Giddens opisał, że żyjemy w późnej epoce nowożytnej, a to oznacza, że jedną nogą jesteśmy na stałe w środowisku lokalnym, a drugą w świecie globalnym: „Chociaż wszyscy żyjemy w środowiskach lokalnych, światy, których doświadcza większość z nas są naprawdę globalne". Z. Bauman postrzegał globalizację jako zmniejszenie dystansu pod wieloma względami: „To niesamowite poczucie »wypełniania świata« jest powszechnie określane jako »globalizacja«. Gdy prędkości transmisji osiągają wartości graniczne – porównywalne z prędkością światła – (w tym wyzwalacze akcji), niemal równoczesna sekwencja przyczyny i skutku zmniejsza nawet największe odległości i ostatecznie unieważnia rozróżnienie między samą przyczyną a skutkiem. Mimo wszelkich praktycznych intencji i celów, wszyscy żyjemy dziś w bliskiej, wręcz kameralnej okolicy"[7].

Obecnie mamy do czynienia z bardzo różnorodnymi mediami, ale jednocześnie nie da się zweryfikować wszystkich przekazywanych informacji – zwłaszcza na forach internetowych, blogach, w mediach społecznościowych i innych mediach informacyjnych. Skuteczność danej kampanii dezinformacyjnej zależy głównie od kanałów ich transmisji i szybkości, z jaką się rozprzestrzenia, a ta jest niepowtarzalna w przeszłości i niewyobrażalna co do przyszłych możliwości. Anonimowość, jaką daje internet nie pomaga w procesie dławienia cyberzagrożeń.

Wojna hybrydowa – obszar odziaływania mediów cyfrowych

Specyfika wojny hybrydowej powoduje, że stroną konfliktu zbrojnego może być nie tylko państwo, ale również organizacja nieposiadająca podmiotowości prawnej, a także korporacja – przedsiębiorca. Jednym z podstawowych celów ataków w cyberprzestrzeni jest dezinformacja, która stanowi stary temat,

6 L. Kołakowski, *Cywilizacja na ławie oskarżonych*, Warszawa 1990, s. 201.
7 Z. Bauman, *Społeczeństwo w stanie oblężenia*, Warszawa 2007, s. 18.

który teraz przyjmuje zupełnie nowe oblicze. Właśnie przy wykorzystaniu instrumentów służących do cyberataków dezinformacja i wojna informacyjna stały się nowym obszarem działań nie tylko pomiędzy państwami, ale też bardzo często ta wojna cyfrowa ma charakter rywalizacji pomiędzy przedsiębiorstwami, a także pomiędzy korporacjami a państwami. Dokonując próby zdefiniowania takiego incydentu, można sięgnąć jako wzoru do definicji zdarzenia o charakterze terrorystycznym. Zgodnie z art. 2 pkt 7 ustawy o działaniach antyterrorystycznych[8] należy przez to pojęcie rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub zagrożenie zaistnienia takiego przestępstwa.

Przez pojęcie „akt agresji w cyberprzestrzeni" należy rozumieć incydent w rozumieniu art. 2 pkt 5 ustawy o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020, poz. 369), co do którego istnieje podejrzenie, że wypełnia znamiona czynu zabronionego z art. 131 § 3, art 165 § 1 pkt 4, art. 267 § 1, § 2, albo § 3, art. 268a § 1 albo § 2, art. 269 § 1 lub 2, art. 269a albo art. 269b § 1, ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, popełnionym przez siły obcego państwa lub przez podmioty działające na zlecenie lub w interesie takiego państwa, jak również aktów podejmowanych przez te siły lub podmioty, polegających na tworzeniu i rozpowszechnianiu informacji w celu osiągnięcia strategicznych celów.

Pierwszym istotnym zagadnieniem, pojawiającym się przy budowie definicji, jest kwestia nazwy incydentu będącego aktem wojny informacyjnej. Ostatecznie sformułowanie „akt agresji w cyberprzestrzeni" może oznaczać działanie lub zaniechanie, którego sprawcą może być każdy podmiot (a nie tylko człowiek, co ma znaczenie w wypadku posłużenia się przez wrogie państwo sztuczną inteligencją), a także nie wiąże się z sytuacją klasycznej wojny konwencjonalnej. Definicja ta w istotnym stopniu nawiązuje do pojęcia „incydent" do art. 2 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020, poz. 369 ze zm.), zgodnie z którym jest to „zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo". Samo cyberbezpieczeństwo można zdefiniować jako wszelkie działania – metody, procedury, rozwiązania prawne – podejmowane przez właściwe w tym względzie podmioty, które to zmierzają do integralności zgromadzonych,

8 Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. 2016, poz. 904 ze zm.

przechowywanych i przetwarzanych zasobów informacyjnych, zmierzające do ich ochrony przed niepożądanym, nieuprawnionym ujawnieniem, zmianą lub zniszczeniem[9]. Zabieg polegający na odwołaniu się do niej oznacza możliwość przy dokonywaniu wykładni sięgania do tejże ustawy oraz orzecznictwa i poglądów doktryny jej dotyczących. Kluczowe może mieć też tu znaczenie definicja bezpieczeństwa informacyjnego, którym jest również każde działanie, system lub metoda, które zmierzają do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przekazywanych, przechowywanych w pamięci komputerów oraz sieci teleinformatycznych[10]. Jednak, wydawać się może, że definicja ta jest zawężona do kwestii ochrony informacji, a nie odnosi się do wielu innych zagrożeń, które nie muszą być związane bezpośrednio z jakimkolwiek nielegalnym wykorzystaniem informacji, a mogą dotyczyć działań wykorzystujących narzędzia informatyczne lub samą informację – tak jak w przypadku dezinformacji.

Dezinformacja jako akt agresji

Rozwój internetu umożliwił w praktyce nieskrępowany dostęp nie tylko do korzystania z informacji, ale także do ich tworzenia i rozpowszechniania z pominięciem, zazwyczaj regulowanych, tradycyjnych dostawców informacji, takich jak prasa, radio i telewizja, których sfera została poddana regulacji prawnej. Za pomocą sztucznej inteligencji i gotowych cyfrowych narzędzi każdy ma możliwość stworzenia tzw. *deepfakes*, czyli zmanipulowanych materiałów audiowizualnych. Technologia ta działa w oparciu o algorytm, który najpierw uczy się tzw. cech dystynktywnych danej osoby, tj. jej mimiki, barwy głosu itd., a następnie synchronizuje je z dowolnie wybranym przez twórcę materiałem tak, aby stworzyć iluzję wskazującą, że osoba przedstawiona na filmie faktycznie wypowiada słowa stanowiące podkład dźwiękowy. Innymi słowy jest to technologia umożliwiająca stworzenie realistycznych fałszerstw przedstawiających wypowiedzi i działania, do których nigdy nie doszło. Wraz z rozwojem technologii deepfake w relatywnie prosty sposób powstaje możliwość stworzenia

9 P. Potejko, *Bezpieczeństwo informacyjne* [w:] red. K.A. Wojtaszczyk, A. Materska-Sosnowska, *Bezpieczeństwo państwa*, Warszawa 2009, s. 194.

10 M. Kaliski, A. Kierkowska, G. Tomaszewski, *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] red. J. Kaczmarek, M. Kwieciński, *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010, s. 34.

poligonu do rozprzestrzeniania dezinformacji w sferze politycznej i wpływu na opinię publiczną w zakresie konkretnych osób pełniących funkcje publiczne. Fałszywe informacje mogą być obecnie wykorzystywane do wywierania wpływu na proces wyborczy, jakość mediów, napięcia społeczne, a także, w świecie korporacyjnym, w celu wywierania wpływu na konkurencję na rynku.

Trzeba podkreślić, iż obecne ataki mają charakter zorganizowany i masowy, głównie nastawiony na ingerencję w działaniach samych systemów. Obecna forma ataku na system komputerowy lub usługę sieciową przybiera formę uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów[11]. W atakach tego typu wykorzystuje się jednocześnie bardzo wiele komputerów. Coraz częściej ataki tego typu są wykorzystywane także dla celów politycznych. Przestępczość związana z wykorzystaniem komputerów i sieci teleinformatycznych określana jest jako „przestępczość komputerowa", „high-tech przestępczości" i „cyberprzestępczość". Te pojęcia są często używane zamiennie. Jednak różnice, które odnoszą się zarówno do celu przestępstwa, jego skutków i zakresu oddziaływania mogą mieć wpływ na potrzebę kategoryzacji takich czynów dokonywanych przy pomocy technologii teleinformatycznych. Rozwój przestępczości w sieci teleinformatycznej, gdzie z wykorzystaniem podstawowych cech samej sieci, jak i urządzeń mobilnych zmienia się myślenie o tradycyjnym przestępstwie, wymaga aktualizacji definicji w krajowych kodeksach karnych, uwzględnienia ulepszonych środków współpracy oraz wprowadzenia odpowiednich procedur. Nowoczesne systemy informatyczne i nowe rodzaje komunikacji umożliwiają wykonywanie nielegalnej działalności z dowolnego miejsca na świecie w każdym czasie. Z powodu ograniczonej świadomości i doświadczenia administratorów sieci oraz użytkowników systemu, wiele czynów przestępczych nie jest wykrywanych. Również same ofiary nie są skłonne do zgłaszania przypadków wykorzystywania technik komputerowo-sieciowych ze względu na obawę co do ponownych ataków oraz własną renomę, zwłaszcza w zakresie bezpieczeństwa zawieranych transakcji czy świadczenia usług. Większość ataków odnosi się jednak do sytuacji dostępności sieci informatycznych i komunikacyjnych oraz zawartych w nich danych, których wartość jest istotna, nawet jeśli nie mają one charakteru materialnego. Zagadnienie to dotyczy w szczególności ochrony prywatności w sieci.

11 A. Završnik, *Cybercrime definitional challenges and criminological particularities*, http://www.inst–krim.si/upload/izdajanje/AZavrsnikcybercrime.pdf.

Jednak obecnie powstaje zupełnie nowy poziom zagrożeń związanych z rozpowszechnianiem nieprawdziwych informacji. Ta sytuacja wymaga nowego podejścia do definiowania cyberprzestępczości, a tym samym cyberbezpieczeństwa przez pryzmat zagrożeń dla bezpieczeństwa i porządku publicznego w strefie komunikacji społecznej.

Dezinformacja to proces, który polega na celowym, błędnym informowaniu[12], to pojęcie definiuje również S. Dubisz jako nieprawdziwą, mylącą informację ale także sytuację, w której brakuje rzetelnych informacji[13]. Dezinformacja to celowe działanie, które zmierza do wywołania zmian w świadomości odbiorców, zmian postaw wobec zjawisk i wywołania określonej reakcji gospodarczej, społecznej albo politycznej. Postęp technologiczny sprawia, że zjawisko to w ostatnich latach nabrało na sile i w łatwy sposób rozprzestrzenia się globalnie[14]. Oficjalną unijną definicję dezinformacji opracował zespół ekspertów z krajów członkowskich Unii Europejskiej. Zgodnie z tą definicją, dezinformacja to „fałszywa, niedokładna lub wprowadzająca w błąd informacja, stworzona, zaprezentowana i rozpowszechniana dla zysku lub rozmyślnego spowodowania szkody publicznej"[15]. Zgodnie z powyższą definicją, dezinformacja jest działaniem celowym, zmierzającym do wywołania określanej reakcji społecznej, politycznej czy też gospodarczej. Dezinformacja podważa zaufanie do instytucji publicznych oraz szkodzi demokracjom przez utrudnianie obywatelom podejmowania świadomych decyzji. Nieprawdziwe informacje sieją niepewność oraz przyczyniają się do napięć społecznych, co może mieć poważne konsekwencje szczególne dla bezpieczeństwa obywateli. Rozwój nowoczesnych technologii sprawił, że takie nieprawdziwe informacje z łatwością rozprzestrzeniają się na skalę globalną[16].

Problem ten towarzyszy człowiekowi od lat, związany jest on bezpośrednio z przekazywaniem informacji, a w szerszym rozumowaniu z komunikacją, która składa się z kilku elementów m.in. uczestników, przekazu, kanałów

12 A. Markowski, *Wielki słownik poprawnej polszczyzny*, Warszawa 2004, s. 172.

13 S. Dubisz, *Uniwersalny słownik języka polskiego*, Warszawa 2003, s. 60.

14 A. Ogrodowczyk, M. Borkowska, E. Murawska-Najmiec, K. Twardowska, *Fake news – dezinformacja online próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2020, s. 5.

15 https://www.cyberdefence24.pl/ue-unijna-definicja-dezinformacji-i-nowy-kodeks-postepowania-dla-mediow.

16 Krajowa Rada Radiofonii i Telewizji, *Fake news – dezinformacja online. Próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2020, s. 7.

komunikacji oraz sprzężenia zwrotnego[17]. Zjawisko dezinformacji często podważa zaufanie do instytucji, tradycyjnych i cyfrowych mediów oraz szkodzi obywatelom w podejmowaniu świadomych decyzji. Nasilenie i rozprzestrzenienie się tego zjawiska wynika z rozwoju nowoczesnych mediów i portali społecznościowych, a co za tym idzie, powiązane jest także z szumem informacyjnym spowodowanym wielkością informacji, które docierają do nas z różnych kanałów komunikacyjnych. W praktyce tak zwane fake newsy posiadają tendencję do znacznie szybszego rozpowszechniania się w porównaniu do wiarygodnych i rzetelnych informacji[18].

Na podstawie raportu przeprowadzonego przez Radę Europy w 2017 r. rozróżniamy trzy kategorie nieładu informacyjnego: „Mis" – informacja występuje kiedy rozpowszechniane informacje są nieprawdziwe, lecz nie zostały utworzone z zamiarem wymierzenia szkody. Wspomniana wcześniej dezinformacja – fałszywe informacje są tworzone oraz rozpowszechniane w sposób świadomy z zamiarem wyrządzenia szkody lub krzywdy. Pojęcie „Mal" – informacja, czyli rozpowszechnianie informacji jest oparte na faktach lecz powstały w celu wyrządzenia szkody lub krzywdy, przykładem jest upublicznienie informacji prywatnych[19]. Demokracja jest oparta na wolności słowa, środków przekazu i zależy od swobodnego przepływu informacji. Pod tym względem możemy powiedzieć, że dezinformacja podważa reguły demokracji, a nawet wykorzystuje jej atrybuty i system wartości w działaniach skutkujących agresją wobec jednostki, poszczególnych grup społecznych, a nawet państw. Dezinformacja to w rzeczywistości atak w samo serce demokracji. Opowieść o dezinformacji dotyczy informacji, które są celowo fałszywe, aby manipulować ludźmi i wprowadzać w błąd. Żyjemy w świecie, w którym nie ma uzgodnionej definicji języka, którym opisujemy to zjawisko, także w przepisach prawa. Dezinformacja – celowe tworzenie i rozpowszechnianie informacji, które są fałszywe i zwodnicze w celu wprowadzenia odbiorców w błąd, to przestępstwo, mieszanka prawdy i fałszu, a zasady państwa demokratycznego stoją w opozycji do potrzeb związanych z zapewnieniem bezpieczeństwa i porządku w świecie cyfrowym. Podstawową zasadą demokracji jest wolność słowa, prawo do prywatności i te właśnie wartości kluczowe dla państw demokratycznych, są wykorzystywane przez inne państwa, dla których takie wartości nie stanowią istoty funkcjonowania.

17 https://mfiles.pl/pl/index.php/Dezinformacja.
18 A. Ogrodowczyk, M. Borkowska, E. Murawska-Najmiec, K. Twardowska, *Fake*…, s. 5–6.
19 Ibidem, s. 7.

Dezinformacja tworzona jest przez podmioty, które zainteresowane są wprowadzeniem do obiegu fałszywych informacji i chcą wywrzeć określony efekt, wpłynąć na decyzję lub postawę użytkownika posługując się często informacją, która istnieje albo wyrażając opinię na jakiś temat[20]. Często dezinformacja jest elementem wojny informacyjnej, gdyż dysponuje szeregiem narzędzi, które wykorzystują błędy poznawcze oraz specyfikę środowiska informacyjnego. W zależności od grupy docelowej oraz kanału dystrybucji używane techniki będą się od siebie nieco różniły[21]. Takie informacje mają często negatywny wpływ na poczucie bezpieczeństwa, ponieważ nie tylko powielanie fake newsów niesie społecznie negatywne konsekwencje ale i rozpoznanie elementów dezinformacji może skutkować podchodzeniem w przyszłości z dystansem do informacji prawdziwych przedstawianych w mediach, a nawet podważanie słów prawdziwych ekspertów czy autorytetu władz publicznych[22]. Szczególnie podatność na dezinformację można zauważyć w przypadku zjawisk skomplikowanych, mało znanych oraz budzących emocje wśród ludzi. W ostatnich latach okazało się, że profilowanie i sieci społecznościowe mogą być wykorzystywane także do wpływania na opinię publiczną i proces wyborczy w poszczególnych krajach demokratycznych. Jednocześnie łatwość tworzenia treści i ich udostępniania utrudnia cenzurę i kontrolę nad mediami w państwach niedemokratycznych i autorytarnych.

Wskazany powyżej ostatni fragment definicji aktu agresji w cyberprzestrzeni dotyczy dezinformacji, która obecnie jest uważana za jedną z form cyberwojny oraz wojny hybrydowej (tzw. wojna informacyjna). Podczas prób definiowania aktu agresji w cyberprzestrzeni rezygnuje się ze wskazania celu działań sprawcy agresji w przypadku zachowań z pierwszej grupy (tj. czynów o znamionach przestępstw z kodeksu karnego), co jest częstym elementem definicji „cyberwojny", jak to ma miejsce np. w sformułowanej przez Susan W. Brenner, która przyjęła, że są to „działania podejmowane przez państwa za pomocą technologii informatycznej ukierunkowane na osiągnięcie militarnych czy innych, strategicznych celów"[23]. Uznano bowiem, że utrudni to stosowanie definicji – w momencie cyberataku nie wiadomo zwykle, kto go przeprowadza

20 Ibidem, s. 9.

21 https://warsawinstitute.org/pl/dezinformacja-jako-zagrozenie-dla-prywatnych-publicznych-przedsiebiorstw/.

22 https://mfiles.pl/pl/index.php/Dezinformacja.

23 *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, red. R.D. Clifford, Durham 2011, s. 17–20; J. Clough, *Principles of cybercrime*, Nowy Jork 2013, s. 10; P. Grabosky, *Electronic crime*, New Jersey 2006, s. 11.

i w jakim celu, choć czasami istnieje możliwość wskazania sprawcy i motywów, jakie jego działaniom przyświecają. Inaczej jest w przypadku dezinformacji – jest to rozsiewanie fałszywych informacji, mających na celu osiągnięcie pewnych strategicznych celów, np. szkody w wizerunku państwa czy dezorientacji społeczeństwa, podważania autorytetu władz publicznych. Jeszcze kila lat temu szczytem dezinformacji było rozpowszechniane fałszywych zdjęć i tekstów. Jednak wraz z rozwojem nowoczesnych technologii, powstały również nowe formy rozpowszechniania nieprawdziwych informacji. W dzisiejszych czasach, przy pomocy sztucznej inteligencji można wykreować również sztuczne wideo, tzw. „deepfake". Wideo to polega na podmienieniu twarzy albo ciała konkretnej osoby na dowolną inną postać. Dzięki temu, można zmienić wypowiedź osoby, a także jej ruchy ciała. Po raz pierwszy sformułowaniem „deepfake", pojawiło się w 2017 r. Był to pseudonim użytkownika, który przy pomocy sztucznej inteligencji, tworzył i publikował filmy pornograficzne z wykorzystaniem wizerunków znanych gwiazd. Deepfake polega nie tylko na podmianie obrazu, może być również podłożony dźwięk, naśladujący głos konkretnej osoby[24]. W 2018 r. eksperci, stworzyli przykładowe polityczne wideo, w którym to Barack Obama nazywał prezydenta Donalda Trumpa „głupkiem". Jednak w rzeczywistości słowa te wypowiedział reżyser Jordan Peele, a postać Obamy została wygenerowana na podstawie innych istniejących już nagrań. Doświadczenie to miało pokazać, jak sztuczna inteligencja może namieszać w polityce[25]. Technologia deepfake niesie za sobą wiele zagrożeń, gdyż może być ona wykorzystywana do manipulowania opinią publiczną. Wraz z rozwojem tej technologii, takie fałszywe filmy stają się coraz trudniejsze do wykrycia[26].

Przyszłość regulacji

Media cyfrowe stanowią obecnie główne źródło informacji. Od 2015 r. instytucje europejskie, podejmują działania na rzecz przeciwdziałania zjawisku dezinformacji, a poszczególne państwa wprowadzają regulacje i samoregulacje. W kwietniu 2018 r. nastąpił przełomowy moment, został wtedy opublikowany Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego

24 https://miroslawmamczur.pl/deepfake-co-to-takiego-i-jak-go-zrobic/.
25 https://tvn24.pl/magazyn-tvn24/slowa-ktore-nie-padly-twarze-ktorych-nie-bylo,224,3867.
26 https://miroslawmamczur.pl/deepfake-co-to-takiego-i-jak-go-zrobic/.

Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, pt. „Zwalczanie dezinformacji w internecie: podejście europejskie". W dokumencie tym zaprezentowano różne narzędzia do walki z dezinformacją w internecie, m.in. komisja wsparła tworzenie kodeksu postępowania w sprawie dezinformacji online, którego głównym zadaniem jest: kontrola reklam; zwiększanie przejrzystości treści; blokowanie fałszywych kont oraz wprowadzanie mechanizmów zabezpieczających przed dezinformacją. W związku z powyższym Komisja Europejska stale wzywa platformy internetowe, aby bardziej zaangażowały się w zwalczanie dezinformacji, tak aby informacje w internecie były ze sprawdzonych źródeł. Kodeks postępowania dotyczący dezinformacji online, został podpisany 16 października 2018 r. przez najważniejsze przedsiębiorstwa internetowe, tj. Facebook, Google, Twitter oraz TikTok. Platformy internetowe, które podpisały kodeks, zobowiązały się również do comiesięcznego raportowania Komisji Europejskiej realizacji zobowiązań, które podejmują w celu zwalczania dezinformacji[27].

W polskim systemie prawnym nie ma jednorodnej regulacji dotyczącej problematyki dezinformacji. Zagadnienia związane z rozpowszechnianiem takich informacji w przestrzeni publicznej, są uregulowane w różnych aktach prawnych, przede wszystkim w ustawie z dnia 26 stycznia 1984 r. Prawo prasowe, w której zostały uregulowane zagadnienia związane z prasową działalnością wydawniczą i dziennikarską. Art. 6 ust. 1 wyżej wymienionej ustawy, stanowi o tym, że prasa zobowiązana jest do prawdziwego przedstawiania omawianych zjawisk. Dziennikarz natomiast jest zobowiązany do starannego i rzetelnego zbierania oraz wykorzystywania materiałów prasowych, w szczególności powinien sprawdzać czy uzyskane wiadomości są zgodne z prawdą lub podać ich źródło (art. 12 ust. 1). Publikowanie w prasie nieprawdziwych informacji nie podlega, co do zasady, karze. Redaktor, autor albo inna osoba, która opublikowała materiał prasowy, ponosi natomiast odpowiedzialność cywilną za naruszenie praw wynikające z opublikowania materiału prasowego. Publikacja materiału prasowego, nawet wtedy gdy jest prawdziwa, może naruszać dobra osobiste osoby fizycznej lub prawnej. W momencie, gdy okaże się, że opublikowane informacje są nieprawdziwe, to odpowiedzialność dziennikarza będzie zależała od ustalenia, czy przy zbieraniu materiału, zachował należytą staranność oraz rzetelność i czy mógł powziąć wątpliwość co do wiarygodności

27 Krajowa Rada Radiofonii i Telewizji, *Fake news – dezinformacja online. Próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2020, s. 14–15.

swoich źródeł informacji[28]. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, reguluje natomiast kwestie związane z odpowiedzialnością usługodawców, świadczących usługi na odległość, nie odnosi się jednak do regulacji zjawiska dezinformacji. W tego typu działaniach przestała liczyć się faktyczna siła ofensywna i defensywna sił zbrojnych, została ona zamieniona na efektywność działania na nowych polach ekspansji, takich jak sieć teleinformatyczna[29] i media cyfrowe. Obecnie zjawisko wojny cyfrowej nie dotyczy jedynie działań o charakterze militarnym. Dzieje się tak, dlatego że w działaniach tych większe znaczenie ma umiejętne wykorzystanie zasobów sieciowych i samej informacji, niż posiadana ilość zasobów i kompetencji umożliwiających akty agresji, w tym cyberataki na systemy teleinformatyczne. Kluczowe staje się manipulowanie informacją i wykorzystywanie jej jako elementu aktu agresji.

Obecnie powszechnym tematem jest panująca pandemia wirusa Covid-19, a co za tym idzie w internecie i innych środkach masowego przekazu jest wiele informacji na ten temat zarówno tych rzetelnych, prawdziwych, jak i tych fałszywych. Pandemii towarzyszą zatem zjawiska, takie jak zalew fałszywych i wprowadzających w błąd informacji, żerowanie na ludzkim strachu i masowy napływ informacji, które ulegają szybkim zmianom. Zdaniem WHO dezinformacjami zalewającymi internet są m.in. teorie spiskowe przypisujące powstanie koronawirusa wynalezieniu technologii łączności nowej generacji 5G, wiążące się z chorobą Covid-19 z pochodzeniem etnicznym, a także reklamy produktów, które obiecują dostęp do kuracji lub szczepionek przeciw wirusowi, których nie ma na rynku. Zwalczanie dezinformacji dotyczącej koronawirusa spoczywa przede wszystkim na rządach poszczególnych krajów, platformach internetowych oraz organizacjach międzynarodowych[30]. Fałszywe informację o koronawirusie, które wprowadzają w błąd na tematy związane ze zdrowiem stanowią poważne zagrożenie dla zdrowia publicznego. Szybkie rozprzestrzenianie się dezinformacji w sieci zaburza choćby zaufanie do szczepień, które odgrywają ważną rolę dla zdrowia społeczeństwa. Unia Europejska postanowiła zatem przeciwdziałać działaniom podmiotów, które próbują skorzystać z tego kryzysu zdrowotnego siejąc zamęt, niepokój społeczny i strach. Komisja Europejska proponuje zatem konkretne działania na rzecz silniejszej i odporniejszej Unii Europejskiej, które zostaną uwzględnione w przyszłych pracach

28 Ibidem, s. 30–31.
29 K. Liedel, P. Piasecka, *Pozamilitarne aspekty bezpieczeństwa. Wojna cybernetyczna – wyzwanie XXI wieku*, Warszawa 2011, s. 15.
30 A. Ogrodowczyk, M. Borkowska, E. Murawska-Najmiec, K. Twardowska, *Fake…*, s. 56.

UE dotyczących dezinformacji, w szczególności w akcie prawnym o usługach cyfrowych oraz europejskim planie działania na rzecz demokracji[31]. W związku z wysokim wzrostem dezinformacji związanych z pandemią instytucje UE propagują wiedzę o niebezpieczeństwach dezinformacji oraz zachęcają do korzystania z wiarygodnych źródeł. Światowa Organizacja Zdrowia określiła rozprzestrzeniania się mitów związanych z Covid-19 jako „infodemia". Rozpowszechnianie informacji nieprawdziwych lub niedokładanych o wirusie, jego pochodzeniu, skutkach oraz o działaniu władz w czasie pandemii sprawia, że społeczeństwu trudno jest znaleźć wiarygodne źródła i potrzebne rady. Aby pomóc ludziom odróżniać fakty od fałszywych stwierdzeń Komisja stworzyła stronę faktograficzną, która pomaga również rozpoznać boty internetowe i teorie spiskowe. Według ostatnich badań przeprowadzonych w marcu wśród Europejczyków 50% uważa, że miało do czynienia z dezinformacją w internecie[32].

Pandemia i zalew dezinformacji związanych z wirusem popchnął wiele instytucji do walki z fałszywymi informacjami jednym z nich jest Projekt Wzmacniania Zaufania do Szczepień, której eksperci opisują dezinformację w sieci. Specjaliści wyróżniają poziomy dezinformacji, w tym brak zaufania do nauki jest to najbardziej szkodliwa postawa, często osoby powiązane z medycyną podsycają przesadzone albo nieuzasadnione obawy społeczeństwa do szczepień, zachowanie to skutkuje strachem i brakiem zaufania do szczepionek. Następnie można wyróżnić postawę osób, które szerząc antyszczepionkową opinie zarabiają na tym pieniądze lub osoby, które w tej teorii widzą pewne szanse polityczne. Kolejną kategoria równie groźną to „super-rozpowiadacze", którzy fałszywe informacje kierują za pomocą mediów społecznościowych do ludzi podobnie myślących[33].

Trzeba tu podkreślić, iż dezinformacja staje się przyczyną paniki społecznej, a ta z kolei wywołuje panikę moralną, której istota polega na często nieadekwatnej, przesadnej reakcji społecznej, która wyolbrzymia zagrożenie lub straty spowodowane zajściami definiowanymi jako patologiczne[34]. Odnosi się to do oficjalnych reakcji, które są nieproporcjonalne do zagrożenia społecznych wartości i interesów, postrzegane w podobny sposób przez wszystkich

31 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_pl.

32 https://www.consilium.europa.eu/pl/policies/coronavirus/fighting-disinformation/.

33 https://szczepienia.pzh.gov.pl/dezinformacja-w-sieci-moze-stac-sie-jednym-z-najwiekszych-zagrozen-zdrowia-publicznego/.

34 Zob. M. Ciesielski, *Terroryzm…*, s. 176–177.

specjalistów w zakresie przyczyn, prognoz i rozwiązań danego problemu, a środki masowego przekazu prezentują go jako coś nagłego, dramatycznego, często nowego[35]. Warto podkreślić, że panika moralna może być również spowodowana oceną prowadzonej polityki bezpieczeństwa państwa, która polega na ograniczeniu praw i wolności obywatelskich, w celu neutralizacji zagrożenia. Przy czym takie ograniczenia w wymiarze normatywnym, w przypadku Polski, są istotą każdego z trzech stanów nadzwyczajnych możliwych do wprowadzenia przez rządzących w reakcji za powstałe zagrożenie – czy będzie to stan wyjątkowy, klęski żywiołowej, bądź stan wojenny[36]. W kontekście paniki moralnej, podobnie jak w przypadku sekurytyzacji, kluczowe znaczenie mają media, które biorą aktywny udział w definiowaniu sytuacji zagrożenia oraz oceniają celowość prowadzonej polityki bezpieczeństwa.

Dlatego działania związane z przyszłymi regulacjami prawnymi mogą być uzasadniane nie tylko względami zapewnienia porządku i bezpieczeństwa publicznego, ale także celem zapewnienia ochrony tzw. moralności publicznej, uzasadniającej ograniczenie praw i wolności człowieka, w tym tak silnie strzeżone wartości demokratyczne, jak wolność słowa i środków społecznego przekazu w środowisku cyfrowym.

Bibliografia

Bauman Z., *Społeczeństwo w stanie oblężenia*, Warszawa 2007.
Castells M., *Władza komunikacji*, Warszawa 2013.
Ciesielski M., *Terroryzm i media w kontekście paniki moralnej*, „Bellona" 2012, nr 2.
Clough J., *Principles of cybercrime*, Nowy Jork 2013.
Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime, red. R.D. Clifford, Durham 2011.
Dubisz S., *Uniwersalny słownik języka polskiego*, Warszawa 2003.
Grabosky P., *Electronic crime*, New Jersey 2006.
Kaliski M., Kierkowska A., Tomaszewski G., *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] red. J. Kaczmarek, M. Kwieciński, *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, Toruń 2010.
Kołakowski L., *Cywilizacja na ławie oskarżonych*, Warszawa 1990.
Liedel K., Piasecka P., *Pozamilitarne aspekty bezpieczeństwa. Wojna cybernetyczna – wyzwanie XXI wieku*, Warszawa 2001.
Markowski A., *Wielki słownik poprawnej polszczyzny*, Warszawa 2004.
Mersch M., *Teorie mediów*, Warszawa 2010.
Merton R.K., *Samospełniające się proroctwo* [w:] red. P. Sztompka, M. Kucia, *Socjologia*, Kraków 2006.

35 L. Miś, *Problemy społeczne: teoria, metodologia, badania*, Kraków 2007, s. 101.
36 Art. 228–234 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. nr 78, poz. 483.

Miś L., *Problemy społeczne: teoria, metodologia, badania*, Kraków 2007.
Ogrodowczyk A., Borkowska M., Murawska-Najmiec E., Twardowska K., *Fake news – dezinformacja online próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2020.
Potejko P., *Bezpieczeństwo informacyjne* [w:] red. K.A. Wojtaszczyk, A. Materska-Sosnowska, *Bezpieczeństwo państwa*, Warszawa 2009.

Disinformation as an act of aggression in cyberspace

Abstract

The fundamental element of safety, and of a sense of being out of danger, is the social communication of these. As societies continue to develop and progress is being achieved through digital processes and informatisation in communications, and the ease with which information and data can be transmitted, and with communications becoming personalised, engendering entirely new forms of activities, an increasingly prominent role has been played by social media and communications not intended for broad audiences. This is true for all events and phenomena associated with the public sphere and with how it is influenced, as well as for how certain social groups or societies are considered genuine and relatable.

Key words: cyberspace, safety, disinformation, media