Jacek Sobczak*

Przestępczość w cyberprzestrzeni między przepisami polskimi a międzynarodowymi

Streszczenie

W artykule podjęta jest problematyka przestępczości w cyberprzestrzeni, regulowanej za pośrednictwem przepisów krajowych oraz prawa międzynarodowego. W dobie społeczeństwa informacyjnego, gdzie internet posiada niezwykle duże znaczenie, a jego użytkowników ciągle przybywa, dochodzi do szeregu naruszeń prawa, które często stanowią przestępstwa. Przestępstwa w cyberprzestrzeni, rozumianej jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych, stają się coraz groźniejsze i bywają coraz trudniejsze do wykrycia i ścigania.

Regulacje krajowe, jak też i międzynarodowe nie zawsze nadążają za dynamicznym postępem techniki, rozwojem sieci oraz wyzwaniami, które niesie ona za sobą. Nadal pojawiają się nowe czyny zabronione, popełniane w cyberprzestrzeni, w większym lub mniejszym stopniu sprzeczne z obowiązującym prawem, obnażające jednocześnie niedoskonałość przyjętych regulacji.

Słowa kluczowe: przestępczość, cyberprzestrzeń, społeczeństwo informacyjne, prawo krajowe, prawo międzynarodowe, zagrożenie, cyberterroryzm, cyberatak, system bezpieczeństwa

* Prof. dr hab. Jacek Sobczak, SWPS Uniwersytet Humanistycznospołeczny.

Zjawisko internetu

Pojawienie się internetu i objęcie siecią praktycznie całego świata nastąpiło stosunkowo niedawno, choć wyrosło już i nawet studiuje na wyższych uczelniach pokolenie, które ze zdziwieniem dowiaduje się, że były czasy, kiedy nie istniała sieć, podobnie jak kserokopiarki, skanery, ebooki itd. Założenia, które legły u podstaw internetu, będącego w istocie rzeczy zdecentralizowanym środkiem przekazu opartym na globalnej sieci połączeń, który składa się z wielu systemów komunikacyjnych, wykorzystywanych przez użytkowników, były wysoce idealistyczne. Stanowiły one bowiem próbę zbudowania nowego społeczeństwa o charakterze liberalnym, cieszącym się wolnością słowa – nieskomercjonalizowanego i niezależnego politycznie[1]. Wszelkie reguły działania internetu miały być oparte o *Netykietę* – dobrowolnie przyjmowaną i przestrzeganą przez użytkowników sieci[2]. Wróżby prawników, że prędzej czy później internet będzie musiał zostać poddany regulacjom prawnym większość internautów, w szczególności pochodzących ze środowisk informatyków przyjmowała je z niedowierzaniem i kwitowała pogardliwym wzruszeniem ra-

1 L.W. Zacher, *Etykietowanie przyszłych społeczeństw – kryteria, określenia, ewaluacje* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005, s. 23–34; Z. Łęski, Z. Wieczorek, *Społeczeństwo wirtualne – czy mamy jakiś wybór?* [w:] M. Sokołowski, M. Furmanek (red.) *Oblicza Internetu. Internet a globalne społeczeństwo informacyjne*, Elbląg 2005, s. 13–28, I. Korcz, *Internet a człowiek w kontekście globalizującego się świata?* [w:] M. Sokołowski, M. Furmanek (red.) *Oblicza…*, s. 29–34.

2 Eksploatowanie sieci komputerowych (w pierwszym rzędzie internetu) doprowadziło do wykształcenia się wielu swoistych zasad i zwyczajów, które nie zostały skodyfikowane i nie wszystkie są w jednakowej mierze aprobowane i przestrzegane. Mimo to jednak wiele z nich zyskało rangę szczególnych norm etycznych, składających się na to, co określa się jako „etyka sieci" (*Netiquette, Nethic, Cybermanners* – w języku polskim: *Netykieta).* Zob. A.H. Rinaldi, *Internationale Netze und das Wettberbstrecht* [w:] J. Becker (red.), *Rechtsprobleme internationalen Dattenetze*, Baden-Baden 1996, s. 13–35 i n. Tak więc, *Netykieta* to zasady etyczne regulujące zachowanie się w sieci. Nie ma ona jednak charakteru zbioru norm prawnych, gdyż nie formułuje jakichkolwiek sankcji za nieprzestrzeganie przyjętych zasad oprócz ostracyzmu użytkowników internetu. Najczęściej przyjmowana jest angielska wersja *Netykiety*, znana jako dokument RFC 1855 (*Netiquette Guidelines).* Znana jest w wielu innych wersjach i odmianach. Wskazać należy wśród nich dokument napisany przez Arlene H. Rinaldi z Florida Atlantic University w 1992 r. Zob. http://tools.ietf.org/html/rfc1855; http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/10.Commandments.html. W odniesieniu do działalności reklamowej w internecie Międzynarodowa Izba Handlowa wypracowała szczególne zasady postępowania, mające jednak również charakter norm etycznych, a mianowicie *Guidelines on Interactive Marketing Communications*, zob. T. Hoeren, *Werberecht im Internet am Beispiel der ICC Guidelines on Interactive Marketing Communications* [w:] M. Lehmann (red.), *Internet – und Multimediarecht (Cyberlaw)*, Stuttgart 1997, s. 112 i n.

mion. Wkrótce jednak okazało się, iż internet, wraz z rozszerzaniem się sieci, powiększaniem się liczby użytkowników, tracił przysłowiową „niewinność". Wśród jego użytkowników miejsce intelektualistów zaczęli zajmować biznesmeni, a w końcu stał się on podstawowym narzędziem, bez którego nie mogą już się obejść miliony, a nawet miliardy zwykłych ludzi. Spowszednienie internetu spowodowało także i to, że zaczęto poszukiwać w jego zasobach treści mniej wysublimowanych, a nawet całkowicie przaśnych, takich jak informacje handlowe, gospodarcze, usługowe[3], polityczne[4], a nawet o charakterze erotycznym.

Rewolucja informacyjna, efektem której był szybki rozwój i upowszechnienie się światowej sieci (efekt informatyczny), zmieniła oblicze współczesnego świata. Wpłynęła na styl życia jednostki, zmieniła sposób funkcjonowania społeczeństwa (efekt socjologiczno-psychologiczny) oraz zredefiniowała rolę państwa (efekt polityczno-prawny). Transformacja stosunków społecznych wpłynęła na zmianę systemów gospodarczych, rozwinęły się nowe wirtualne dziedziny zarówno związane z handlem, jak i finansami. Konsekwencje tych przemian są również widoczne w obszarze bezpieczeństwa.

Możliwość docierania za pośrednictwem internetu do praktycznie nieograniczonej liczby odbiorców zwróciła nań uwagę kół przemysłowo-handlowych, które dostrzegły możliwość wykorzystywania jego potencjału do komunikacji z klientami. Internet okazał się doskonałym narzędziem marketingowym oferującym bogatą gamę usług reklamowych i informacyjnych. Posługiwanie się internetem, w szczególności pocztą elektroniczną przez polityków, przedsiębiorców, handlowców i podmioty świadczące usługi doprowadziło do tego, że odbiorca poczty elektronicznej znalazł się rychło w sytuacji odbiorcy korzystającego z usług poczty tradycyjnej. Podobnie jak ten drugi został zasypany dziesiątkami, potem setkami i tysiącami nigdy niezamawianych reklam, anonsów i ogłoszeń, wśród których ginęły informacje naprawdę dla niego ważne i oczekiwane. Coraz więcej czasu każdy z użytkowników musi poświęcać na segregowanie informacji, na pozbywanie się niechcianej korespondencji. Praktyka taka dotyczy w pierwszym rzędzie reklam o charakterze gospodarczym. Zachęcają mniej lub bardziej nachalnie do nabycia określonych towarów lub skorzystania z określonych usług. Pojawiają się jednak także – i to dość licznie –

3 P. Bickerton, M. Bickerton, U. Pardesi, *Marketing w internecie*, Gdańsk 2006, szczególnie s. 21–151.

4 A. Turska, *Marketing polityczny w Internecie* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006, s. 199–211.

przekazy o charakterze politycznym[5], społecznym bądź religijnym[6], nakłaniające do głosowania na tego czy innego polityka, poparcia partii politycznej[7], określonych idei, czy programów, względnie przyjęcia pewnych dogmatów religijnych[8]. Przyznać jednak należy, że zwłaszcza w rzeczywistości polskiej przekazy internetowe tego ostatniego typu mają charakter marginalny i ich uciążliwość dla odbiorcy jest relatywnie mniejsza. Oczywiście, wspominając o dolegliwości należy mieć na względzie przeciętnego odbiorcę treści reklamowych, skoncentrowanego na własnych problemach i niezainteresowanego informacjami, których w danym momencie nie poszukuje.

Niestety w sieci pojawiło się szereg zjawisk niezwykle groźnych, niebezpiecznych, godzących w prawa i wolności człowieka, naruszających jego prywatność, godność, dobre imię i cześć, wymierzone w tajemnicę środków przekazu, zasadzające się na nieuprawnionym dostępie do informacji bądź do całości lub części systemu informacyjnego, objawiające się w nielegalnym podsłuchu oraz w inwigilacji przy użyciu urządzeń technicznych i programów komputerowych, ujawnianych informacji uzyskanych nielegalnie. Przy wykorzystaniu internetu można naruszać integralność zapisu informacji, bądź danych, utrudniać do nich dostęp sabotować przekaz, zakłócać pracę systemów komputerowych by sprawnie wykorzystywać urządzenia, programy i dane, naruszać korespondencje itd. Za pośrednictwem internetu mogą i są

5 S. Sobczyk, *Internet narzędziem oddziaływania na wyborców* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006, s. 109–116; H. Kotarski, *Internet a lokalna polityka. Studium socjologiczne na przykładzie wyborów samorządowych* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006, s. 117–124; G. Schittek, *Internet jako narzędzie politycznego wsparcia w Szwecji* [w:] T. Zasępa (red.), *Internet. Fenomen społeczeństwa informacyjnego*, Częstochowa 2001, s. 219–226.

6 T. Zasępa, *Komunikacja cybernetyczna wyzwaniem dla Kościoła katolickiego* [w:] T. Zasępa (red.), *Internet i nowe technologie – ku społeczeństwu przyszłości*, Częstochowa 2003, s. 51–54.

7 A. Kasińska-Metryka, *Demokratyzacja systemu politycznego a przepływ informacji – od deficytu do przesytu* [w:] M. Sokołowski (red.), *U progu…*, s. 107–114; P. Gulda, *Elektroniczna demokracja – teoria i praktyka, wady i/lub zalety* [w:] M. Sokołowski (red.), *U progu…*, s. 115–121; P. Gulda, *Internet jako przestrzeń polityczna* [w:] M. Sokołowski (red.), *Edukacja medialna. Nowa generacja pytań i obszarów badawczych*, Olsztyn 2004, s. 47 i n.; M. Boszczyk, *Media elektroniczne jako środek komunikowania politycznego* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym*, Sosnowiec 2006, s. 180–198.

8 W. Muszyński, *Wizerunek polskich tradycjonalistów katolickich w Internecie* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006, s. 261–278; A. Korzińska, *Tradycja i nowoczesność. Islam w Internecie. Analiza polskojęzycznych stron internetowych* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006, s. 279–286.

przekazywane treści pornograficzne, upowszechnia się zjawisko pedofilii oraz rozpowszechniany jest wyjątkowo okrutny „język nienawiści”[9]. Pojawiło się też jeszcze groźniejsze zjawisko w postaci cyberterroryzmu, godzące podstawy funkcjonowania demokratycznych państw i społeczeństw, bezpieczeństwo stosunków międzynarodowych, wolność wyborów politycznych w różnych państwach, rozmontowujące, oparte na systemach komputerowych, systemy porozumiewania się, bądź przesyłania energii. Niektóre z tego rodzaju czynów godzą wprost w bezpieczeństwo publiczne, gdyż wymierzone są w funkcjonowanie sił zbrojnych, aparatu bezpieczeństwa państwa, a nadto zmierzają do wywołania paniki publicznej[10].

9 R. Wieruszewski, M. Wyrzykowski, A. Bodnar, A. Gliszczyńska-Grabias, *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010, passim; K. Grzybczyk, *Twórczość internautów w świetle regulacji prawa autorskiego na przykładzie fanfiction*, Warszawa 2015, passim; L.K. Jaskuła, *Wolność działalności dziennikarskiej w perspektywie zjawiska mowy nienawiści. Wybrane aspekty prawne* [w:] W. Lis (red.), *Status prawny dziennikarza*, Warszawa 2014; M. Woiński, *Prawnokarne aspekty zwalczania mowy nienawiści*, Warszawa 2014, passim.

10 M. Gołda-Sobczak, *Spór o definicję terroryzmu*, „Wiedza i Umiejętności” 2004, t. 5, s. 47–63. Alex Schmid dysponując niewątpliwie niepełnymi danymi, bazując głównie na literaturze amerykańskiej i anglojęzycznej, wyliczył ponad sto rozmaitych definicji terroryzmu, nie znajdując wśród nich żadnej zadowalającej. Podobne stanowisko prezentował Walter Laqueur. Zob. A.P. Schmid, *Political Terrorism: A Research Guide*, New Brunswick 1984, s. 10; W. Laqueur, *Terrorism*, London 1997, s. 7; W. Laqueur, *The Ageof Terrorism*, Boston 1987, s. 11. W praktyce istnieje wiele definicji terroryzmu, które zdaniem K. Indeckiego można podzielić ze względu na kryterium ujmowanego przez nie zakresu przedmiotowego na trzy grupy: generalne, cząstkowe oraz mieszane. Własne definicje terroryzmu przedstawili między innymi: T. Hanusek, *W sprawie pojęcia współczesnego terroryzmu*, „Problemy Kryminalistyczne” 1980, nr 143; M. Fleming, *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy”1996, nr 1; S. Pikulski, *Prawne środki zwalczania terroryzmu*, Olsztyn 2000; T. Aleksandrowicz, *Współczesny terroryzm międzynarodowy – próba definicji ze stanowiska prawa międzynarodowego*, „Wojskowy Przegląd Prawniczy” 2003, nr 2; K. Indecki, *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998, s. 19–22. Zob. także: B. Hoffman, *Oblicza terroryzmu*, Warszawa 2001, s. 13–15; tamże ciekawe nawiązanie do stanowiska W. Laqueur, *The Age of Terrorism*, Boston 1987, s. 11. Zob. A Pawłowski, *Terroryzm w Europie w XIX i XX wieku*, Zielona Góra 1980, s. 9. Zjawisko terroryzmu zaczęto analizować jako rodzaj ukrytej lub zastępczej wojny pozwalającej słabszym państwom na konfrontacje z silniejszymi rywalami. Zob. C. Sterling, *Śmierć terroru: prawda o międzynarodowym terroryzmie*, przeł. M. Fogg i E. Petrajtis-O’Neill, Warszawa 1990. Zob. także: R.S. Cline, *Yonah Alexander: The Soviet Connection*, New York 1984, J. Becker (red.), *The Soviet Union and Terrorism*, London 1984. Na konotacje te zwrócił uwagę B. Hoffman, s. 24–25. Termin *terroryzm* niektórzy odnosili do wszystkich działań czynników niepaństwowych i pozarządowych destabilizujących określone regiony lub terytoria miejskie. Terroryzm stał się też wygodnym określeniem pozwalającym na objęcie jego zakresem wszelkich konfliktów współczesnego świata, które nie przystawały do tradycyjnego obrazu wojny toczonej przez regularne armie dwu lub kilku państw. Zob. B. Hoffman, *Low-intensity Conflict: Terrorism and Guerrilla War*

Narodom Europy, w toku wielowiekowych, okupionych śmiercią i cierpieniem wielu ludzi, udało się osiągnąć zakaz cenzury prewencyjnej, zniweczyć kontrole prasy, publikacji, widowisk. Stało się to jednak w momencie, kiedy „tradycyjna" wymiana informacji, ograniczona do prasy, radia, telewizji, książek i spektakli, zaczęła odgrywać coraz mniejszą rolę, a jej znaczenie powoli malało pod wpływem internetu umożliwiającego zdecydowanie szybszą wymianę myśli – lecz także dającemu większe możliwości kontroli treści przekazu. Nagłaśniane przez prasę, często demonizowane niebezpieczeństwa terroryzmu oraz pedofilii pojawiły się jakby na zamówienie władz publicznych, jako dogodny pretekst do rozpoczęcia kontroli treści przekazywanych informacji. Tym samym, władzom państw uznającym się za demokratyczne (i tak traktowanych przez ogół) udało się to, co nie powiodło się reżimom totalitarnym, to, co okazuje się być marzeniem tyranów, władców absolutnych, dyktatorów – kontrola myśli i uczuć obywateli, poznanie ich prawdziwego „ja"[11].

fare in the Coming Decades [w:] L. Howard (red.), *Terrorism: Roots, Ompact, Responses, Praegor*, New York 1992, s. 140. W myśl decyzji ramowej z 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.Urz. UE L 2002, nr 164, s. 3) zobowiązano państwa unijne do przyjęcia zbliżonych definicji przestępstw terrorystycznych. Wspomniana decyzja ramowa została zastąpiona dyrektywą Parlamentu Europejskiego i Rady UE 2017/541 z dnia 15 marca 2017 w sprawie zwalczania terroryzmu i zastępującą decyzję ramową 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW (Dz.Urz. UE L 2017, nr 88, s. 6). W systemie prawnym Rady Europy opracowano Konwencję Rady Europy o zwalczaniu terroryzmu (Dz.U. z 1996, nr 117, poz. 557) w systemie uniwersalnym opracowano Konwencję o zwalczaniu ataków terrorystycznych z użyciem bomb z 15 grudnia 1997 r. oraz międzynarodową Konwencję o zwalczaniu finansowania terroryzmu z dnia 9 grudnia 1999 r. (Dz.U. z 2004, nr 263 poz. 2620). Por. J.W. Wójcik, *Przeciwdziałania finansowaniu terroryzmu*, Warszawa 2007, s. 131–152. Zgodnie z regulacją zawartą w art. 115 § 20 k.k. „przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: poważnego zastraszenia wielu osób; zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu".

11 Zob. J. Sobczak, *Wolność słowa a zjawisko inwigilacji przekazu internetowego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Architektura komunikacyjna sieci*, Elbląg 2007, s. 71–94.

Społeczeństwo informacyjne

Dążenie do społeczeństwa informacyjnego będące skutkiem procesów globalizacyjnych przebiega nieco inaczej w Europie na obszarze Unii Europejskiej i Rady Europy oraz w Stanach Zjednoczonych i Japonii[12].

Po raz pierwszy wizja społeczeństwa informacyjnego pojawiła się w 1993 r. w opublikowanej przez Komisję Europejską białej księdze pod tytułem *White Paper on Growth, Competitiveness, Employment. The Challenge and way forward into 21st century*[13]. Przedstawione w białej księdze społeczeństwo informacyjne miało być wielką szansą dla Europy, dlatego podkreślano w niej jego pozytywne ekonomiczne i społeczne rezultaty dla gospodarki, niewiele miejsca poświęcając negatywnym skutkom informatyzacji. Podstawowym celem strategicznym, związanym z budową społeczeństwa informacyjnego, miała być całkowita liberalizacja sektora telekomunikacji, która oprócz pobudzenia konkurencji w tej dziedzinie, poprzez przykładowo wprowadzenie nowych operatorów, miała stanowić podłoże do utworzenia europejskiego rynku usług i produktów informacyjnych. Założenia białej księgi zostały skonkretyzowane w dokumencie *Europe and the Global Information Society: recommendations to the European Council* (Europa a społeczeństwo globalnej informacji), zwanym Raportem Bangemanna, opublikowanym w 1994 r.[14] Raport stanowił podstawę do opracowania szczegółowych planów działań, obejmujących tworzenie nowych aktów prawnych i różne inicjatywy, finansowane ze środków publicznych Unii Europejskiej. Dokument otworzył publiczną debatę na temat europejskich szans zrównoważonego rozwoju, wzmocnienia gospodarki, aktywnego konkurowania na rynkach światowych. Raport Bangemanna odzwierciedlał

12 J. Sobczak, *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek, *Demokracja w dobie globalizacji*, t. II, *Aspekty teoretyczne*, Katowice 2008, s. 52–79; J. Sobczak, *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007, s. 193–213; J. Sobczak, *Europejski ład komunikacyjny w procesie globalizacji* [w:] J. Sobczak, R. Bäcker, *Europejska myśl polityczna wobec globalizacji*, Łódź 2005, s. 39–70. Zob. także: K. Doktorowicz, *Europejska droga do społeczeństwa informacyjnego* [w:] K. Doktorowicz (red.), *Społeczeństwo informacyjne. Wyzwania dla gospodarki, polityki i kultury*, Katowice 2002, s. 75 i n.

13 *White Paper on Growth, Competitiveness, Employment. The Challenge and way forward into 21st century*, COM (93) 700 final.

14 Raport *Recommendations to the European Council, Europe and the global information society* został opublikowany przez Komisarza do spraw Społeczeństwa Informacyjnego Unii Europejskiej Martina Bangemanna w 1994, http://europa.eu.int/ISPO/infosoc/backg/bangeman.html.

optymistyczny punkt widzenia przedstawiony w białej księdze i znacząco przyczynił się do aktywizacji wielu środowisk zawodowych i społecznych widzących w technologiach teleinformatycznych szansę dla Europy[15].

Kolejnym ważnym dla rozwoju społeczeństwa informacyjnego dokumentem europejskim była zielona księga Komisji Europejskiej *Living and Working in Information Society. People First* (Życie i praca w społeczeństwie informacyjnym. Człowiek na pierwszym miejscu) z 1996 r.[16] Dokument ten był wyrazem zmian w polityce europejskiej, gdzie priorytetem stały się cele społeczne. Zielona księga koncentrowała się na problematyce społecznej i socjalnej, w tym przede wszystkim na zatrudnieniu oraz budowie społecznej solidarności, równych szans i kulturalnej różnorodności Europy. W styczniu 1999 r. opublikowano kolejną zieloną księgę, zatytułowaną *Public Sector Information in the Information Society* (Zielona Księga na temat Informacji Sektora Publicznego w Społeczeństwie Informacyjnym)[17]. Poruszała ona głównie zagadnienia powszechnego dostępu, kładąc nacisk na wykorzystanie infrastruktury informacyjnej do realizacji fundamentalnych praw człowieka, takich jak wolność informacji czy też prawo do informacji. Podsumowując europejskie wysiłki podejmowane w latach 1993–1999 w celu budowania społeczeństwa informacyjnego, należy podkreślić, iż koncentrowały się one na trzech priorytetach: tworzenie środowiska industrialnego i biznesowego, pozwalającego na inwestowanie w infrastrukturę informacyjno-komunikacyjną, polityka innowacyjności oraz dialog społeczny prowadzący do akceptacji zmian i uczestnictwa w zmianach[18].

Pojęcie cyberprzestrzeni

Pojęcie „cyberprzestrzeni" jest terminem, który narodził się w obszarze dość odległym od prawa, bo w powieści *Burning Chrome*, będącej pierwszym tomem trylogii *Neuromancer* autorstwa Williama Gibsona, amerykańskiego pisarza science fiction. Równolegle pisarz posługiwał się jednak terminem „matrix" – matryca. Spopularyzowały cyberprzestrzeń filmy opierające się na motywach

15 J. Sobczak, *Dylematy społeczeństwa informacyjnego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, Elbląg 2006, s. 13–36.
16 *Living and Working in Information Society. People First*, COM (96) 389 final.
17 *Green Paper on Public Sector Information in the Information Society*, COM (99) 585 final.
18 K. Doktorowicz, *Europejski model społeczeństwa informacyjnego*, Katowice 2005, s. 177.

wspomnianej trylogii, a mianowicie *Matrix* i *Johny Mnemonic*[19]. Do powszechnego użytku określenie „cyberprzestrzeń" wchodzi w początkach lat 90. wraz z rozwojem technologii informacyjnych. Uznaje się ją za ściśle związaną z globalizacją[20] i powstaniem społeczeństwa informacyjnego[21]. Odtąd definiowana

19 Zob. w tej kwestii A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, nr 3, s. 6.

20 Terminem globalizacja chętnie posługują się zarówno uczeni, jak i publicyści, usiłując za jego pomocą wyjaśnić zjawiska i procesy, których widownią stał się świat na przełomie XX i XXI w. Podkreśla się przy tym, że globalizacja stanowi końcowy etap historycznej transformacji i elektronicznie przekazywanej kultury popularnej, połączonej z propagowaniem ideologii liberalnej przez rozwinięte państwa demokratyczne. Przegląd definicji pojęcia globalizacja i próbę ich systematyzacji przynosi praca K. Gilarka, *Państwo narodowe a globalizacja – dynamika powstawania nowego ładu*, Toruń 2003, s. 39–46. Por. także: N. Stammers, *Social movements and the challenge to power* [w:] M. Shaw (red.), *Politics in Globalized Word*, London 1999, s. 73 i n.; J.A. Scholte, *The Globalization of World Politics* [w:] J. Baylis, S. Smith (red.), *The Globalization of World Politics. An Introduction to International Relations*, New York 2001, s. 23; J.A. Scholte, *Globalization: prospects for a paradigm shift* [w:] *Politics in Globalized*, s. 9 i n.; I. Clark, *Globalization and International Relation Theory*, Oxford 1999, s. 35. Opisując je zwraca się zwykle uwagę na jego wymiar polityczny, gospodarczy i militarny zapominając, że u jego podstaw leży ważniejszy chyba wymiar kulturowy, któremu sprzyja nowoczesna technika. W literaturze trwa spór o początek procesów globalizacji, a także o to, jaka jest istota tego procesu lub procesów. W tym względzie por. W. Anioł, *Geneza i rozwój procesów globalizacji*, Warszawa 1989, passim; Z. Barman, *Globalizacja*, Warszawa 2000, s. 5–10. Termin „globalizacja", jak przyjmuje się w literaturze, najprawdopodobniej pojawił się po raz pierwszy w słowniku Webstera z 1961 r. Według R. Kilminstera, jest to moment, od którego zaczęto w nauce dostrzegać, iż wydarzenia polityczne i militarne oraz relacje społeczne mają ciągle wzrastające znaczenie nie tylko dla obszaru, na którym zaistniały, lecz także w skali całego globu. W kwestii globalizacji por. także: M. King, *Globalization, Knowledge and Society*, New York 1990. Sporne jest także i to, czy globalizacja jest wynikiem jednego procesu, czy też wypadkową kilku lub kilkunastu tendencji. Stanowiska prezentowane w tym względzie dotyczące istoty i zakresu procesów globalizacji przedstawił M. Pietras, *Globalizacja jako proces zmian społeczności międzynarodowej* [w:] M. Pietras (red.), *Oblicza procesów globalizacji*, Lublin 2002, s. 36–50.

21 Termin „społeczeństwo informacyjne" to określenie stosunkowo młode. Jako pierwszy miał się nim posłużyć w 1963 r. Tadao Umesao, pisząc o japońskiej gospodarce zdominowanej przez informacje i technologie i zastanawiając się nad ewolucyjną teorią społeczeństwa opartego na przemysłach informacyjnych. Określenie to zostało następnie spopularyzowane przez Kenichi Koyamę w rozprawie *Introduktion to Information Theory* w 1968 r. Do Europy koncepcja społeczeństwa informacyjnego zawitała w 1978 r., kiedy to Simon Nor i Allain Minc omówili ją w raporcie przedstawionym prezydentowi Francji. Nieco później, bo w początkach lat osiemdziesiątych, koncepcja społeczeństwa informacyjnego dociera do USA, robiąc w tamtejszych ośrodkach naukowych zawrotną karierę. T. Goban-Klas, *Społeczeństwo informacyjne i jego teoretycy* [w:] J. Lubacz (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1990, s. 29–30. Koncepcja społeczeństwa informacyjnego nie pojawiła się, co oczywiste, w próżni intelektualnej wpisuje się ona w ten nurt refleksji socjologiczno-politologicznej, które starają się zdefiniować i scharakteryzować współcześnie istniejące zbiorowości. Wydaje się, iż u źródeł koncepcji społeczeństwa informacyjnego leży nurt determinizmu technologicznego oraz ewolucjonizmu naukowego, którego zwolennicy

jest jako przestrzeń komunikacyjna tworzona przez system powiązań

zafascynowani zdobyczami technologicznymi podkreślali, że wymuszają one fundamentalne i nieodwracalne zmiany w kulturze i instytucjach społecznych. U podstaw tej koncepcji leży także niewątpliwie teoria modernizacji M. Webera, widzącego w biurokracji nieuchronną, wręcz metafizyczną siłę napędową współczesnego świata. Por. M. Weber, *Gospodarka i społeczeństwo. Zarys socjologii rozumiejącej*, Warszawa 2002, s. 693–726; por. także: S. Andreski, *Maksa Webera olśnienia i pomyłki*, Warszawa 1992, s. 67 i n. Zarówno determinizm technologiczny, jak i weberowska teoria biurokratycznej modernizacji wraz ze skonstatowaną, w płaszczyźnie historycznej, rewolucją przemysłową doprowadziły do wykształcenia koncepcji społeczeństwa przemysłowego (industrialnego), które miało się cechować wykształconą organizacją państwową, komercjalizacją produkcji masowej, wysokim stopniem uprzemysłowienia oraz zatrudnieniem większości członków społeczeństwa poza sektorem rolniczym. Wraz z mechanizacją i rozwojem technicznym podnoszącym standard życia miało nastąpić zniesienie struktur klasowych i zastąpienie ich przez bardziej zróżnicowane i mniej spolaryzowane systemy stratyfikacji zawodowej. Polityczną konsekwencją miał być pluralizm, rozproszenie władzy, koniec rządów autorytarnych Por. C. Kerr, J.T. Dunlap, F.H. Harbison, C.A. Myers, *Industrialism and Industirial Man*, Cambridge 1960. Koncepcja społeczeństwa przemysłowego prowadziła do teorii społeczeństwa postprzemysłowego, czyli takiego, w którym wiedza zastępuje własność, stając się głównym przedmiotem zabiegów oraz najważniejszym źródłem władzy i dynamizmu społecznego. Miało to być społeczeństwo, w którym głównym miejscem zatrudnienia ludności staje się sektor usług, w szczególności w płaszczyźnie finansów, ubezpieczeń, zdrowia, nauki i oświaty. Twórca tej koncepcji, Daniel Bell, podkreślał, iż dominować w społeczeństwie postprzemysłowym będą specjaliści i naukowcy, a wiedza teoretyczna będzie miała centralne znaczenie, jako źródło innowacji i polityki. Wieścił on także coraz szerszy zakres kontroli społecznej rozwoju techniki oraz tworzenie „technologii intelektualnych", jako podstawy podejmowania decyzji politycznych i społecznych. Por. D. Bell, *The Coming of Post-Industial Society*, New York 1973; wyd. II Harmondsworth 1976. W kolejnych prawach Bell posługiwał się już terminem „społeczeństwo informacyjne", wskazując, że jego cechą charakterystyczną jest wzrost produkcji i przepływu informacji wszelkiego rodzaju. Zdawał sobie jednak sprawę z tego, że ma ono charakter w gruncie rzeczy modelu idealnego, a nie realnego. Pomijając w tym miejscu treść jego wywodów odnoszących się do problematyki zmian społecznych, które miały stymulować powstanie społeczeństwa postindustrialnego oraz jego neoewolucyjnego spojrzenia na historię, wypada podkreślić, że o ile w społeczeństwie przedindustrialnym życie jest walką z przyrodą, to w erze industrialnej bój toczy się przeciwko przetworzonej przyrodzie. W epoce przedindustrialnej dominuje siła człowieka. Następująca po niej era industrialna to okres supremacji maszyny. W następnym okresie, w dobie społeczeństwa postindustrialnego, liczy się już tylko informacja. Wyróżnił w ten sposób D. Bell trzy rodzaje pracy: wydobywczą, fabryczną oraz informacyjną. Tę ostatnią, w społeczeństwie postindustrialnym wykonują nie tylko urzędnicy, lecz nowa inteligencja. Prowadzi to do rozwoju zatrudniania w sferze usług i informacji, a w konsekwencji do powstania nowej mentalności społecznej. Por. D. Bell, *The Coming…*, s. 15–20 i 467 i n. Zob. także: A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 31–37. J. Sobczak, *Dylematy społeczeństwa informacyjnego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, Elbląg 2006, s. 13–36; J. Sobczak, *Problemy społeczeństwa informacyjnego w dobie globalizacji*, T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007, s. 193–213; J. Sobczak, *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała,

internetowych[22]. Pojmowana była jako przestrzeń współpracy, niosąca za sobą zarówno pozytywne, jak i negatywne skutki. Do tych drugich zaliczano zwykle możliwości kontrolowania społeczeństwa za pomocą specjalnych narzędzi teleinformatycznych, stosowanych przez służby państwowe, co określano mianem cyberinwigilacji oraz możliwość wykorzystywania sieci przez przestępczość zorganizowaną (cyberprzestępczość), oraz do działań terrorystycznych (cyberterroryzm)[23]. Wskazuje się także, że cyberprzestrzeń jest obszarem, w którym możliwe jest prowadzenie działań wojennych (cyberwojna)[24].

Cyberprzestrzeń zdefiniował Departament Obrony Stanów Zjednoczonych, wskazując, że jest to „współzależna, powiązana ze sobą sieć infrastrukturalna technologii informacyjnej, obejmująca internet, sieci telekomunikacyjne, systemy komputerowe oraz systemy kierujące procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego"[25].

Pojęcie „cyberprzestrzeni" jest używane, jak wynika z powyższych rozważań, jako synonim „sieci", ale bywa, że odnosi się je także do telekomunikacji, jako fenomenu pozwalającego na łączenie się. „Widzialnym" są przewody, satelity, przekaźniki telekomunikacyjne, telewizory, telefony, komputery,

J. Iwanek (red.), *Demokratyzacja w dobie globalizacji*, t. 2, *Aspekty teoretyczne*, Katowice 2008, s. 52–79.

22 A. Nowak, *Cyberprzestrzeń…*, s. 7.

23 M. Pala, *Wybrane aspekty bezpieczeństwa w cyberprzestrzeni*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, nr 1(1), s. 115; S. Serwiak, *Cyberprzestrzeń jako źródło zagrożenia terroryzmem* [w:] E. Pływaczewski (red.), *Przestępczość zorganizowana, świadek koronny i terroryzm w ujęciu praktycznym*, Kraków 2005.

24 P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielniecki, K. Rajchel (red.), *Cyberterroryzm – nowe wyznawania XXI wieku*, Warszawa 2009, s. 46.

25 US Department of Defense Strategy for Operating in Cyberspace, Departament Obrony USA, lipiec 2011 r., cyt. za: A. Nowak, *Cyberprzestrzeń…*, s. 7. Godzi się zauważyć, że sformułowanie to bywa także tłumaczone w ten sposób, że cyberprzestrzeń to „globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnego (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery". Zob. J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego. Studia i Analizy" 2013, nr 9, s. 225–234. Wobec rozbieżności w tłumaczeniach należy przytoczyć definicję w angielskim oryginale *A global domain within the information environment consisting of the interdependent Network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

a „niewidzialnym" różne formy oprogramowania, przeglądarki, narzędzia do surfowania w sieci teleinformatycznej[26].

Pozostając w kręgu koncepcji amerykańskich trzeba zwrócić uwagę na definicję zawartą w Narodowej strategii dla bezpiecznej cyberprzestrzeni. W jej treści stwierdzono: „Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public, health, emergency services, government, defense, industrial base, information and telecommunications, energy, transportation,banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system —the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security"[27].

Sąd Najwyższy USA zdefiniował cyberprzestrzeń (cyberspace), jako „niekończącą się konwersację o światowym zasięgu". Wskazuje się przy tym, że cyberprzestrzeń jest miejscem nieograniczonej wymiany informacji, rozwoju życia społecznego, uczestniczenia w kulturze, utrzymywania różnego rodzaju więzi personalnych za pośrednictwem komputera[28].

W doktrynie, łącząc cyberprzestrzeń z licznymi przestępstwami, wskazuje się, że tożsamość w cyberprzestrzeni może przybrać trzy wymiary: tożsamości rzeczywistej, fikcyjnej i anonimowej. Wyróżnia się także tożsamość biurokratyczną i biograficzną, zaliczając do tej pierwszej dane przyporządkowane do

26 K.W. Grewlich, *„Cyberspace". Sector – specyfic. Regulatio and Competition Rules in European Telecommunications*, „Common Market Law Review" 1999, nr 6, s. 940.

27 Tekst strategii jest dostępny na stronie internetowej pod adresem: http://www.dhs.gov/national-strategy-secure-cyberspace. W tłumaczeniu polskim dokonanym przez J. Wasilewskiego definicja ta brzmi: „Nasza Krajowa infrastruktura krytyczna jest budowana przez publiczne, jak i prywatne instytucje funkcjonujące w sektorach rolnym, żywieniowym, zaopatrzenia w wodę, służby zdrowia, usług ratunkowych, rządowym, obronnym, przemysłowym, informacyjnym oraz telekomunikacyjnym, energetycznym, transportowym, bankowym oraz finansowym, chemicznym oraz materiałów niebezpiecznych, a także pocztowym oraz dostawczym. Cyberprzestrzeń stanowi ich układ nerwowy – system kontrolny naszego kraju. Cyberprzestrzeń jest zbudowana z setek tysięcy połączonych komputerów, serwerów, routerów, switchy oraz światłowodów, które umożliwiają pracę naszej infrastrukturze krytycznej. Stąd też zdrowe funkcjonowanie cyberprzestrzeni jest kluczowe dla naszej ekonomii oraz bezpieczeństwa narodowego". Zob. J. Wasilewski, *Zarys definicyjny…*, s. 228.

28 I. Matusiak, *Gra komputerowa jako przedmiot prawa autorskiego*, Warszawa 2013, passim.

określonej osoby w celu odróżnienia od innych i przybierające często postać numeru[29]. Żałować należy, że w obszarze naukowym tak rzadko zwraca się uwagę na te kwestie i dochodzi do przykrych sytuacji, kiedy później zaistniała na rynku wydawniczym, zajmująca się tą samą dziedziną działalności, co piszący wcześniej kolega, beztrosko funkcjonuje pod oczywiście swoim imieniem i nazwiskiem, nie zwracając uwagi na to, że jest to imię i nazwisko w literaturze występujące. Niekiedy zmusza to wcześniej publikującego badacza do tłumaczenia, że teksty, które pojawiają się tu i ówdzie nie są jego tekstami, a ten który później zaistniał na rynku w pełnej glorii, daje do zrozumienia, że rozmaite książki, artykuły to jego dzieła. Tymczasem wystarczyłoby w niektórych sytuacjach posłużyć się drugim imieniem, a w razie jego braku po prostu imię takie przybrać.

W literaturze zaproponowano definicję „cyberprzestrzeni globalnej" stwierdzając, że jest to system wymiany przetwarzania informacji (danych) funkcjonujących zgodnie z formalnymi zasadami i uregulowaniami prawnymi, obowiązującymi na terytorium poszczególnych państw działający dzięki połączeniu zasobów technicznych zlokalizowanych na terytorium każdego z nich. Cyberprzestrzeń RP proponuje się w doktrynie zdefiniować, jako system wymiany, przetwarzania informacji (danych) funkcjonujących zgodnie z formalnymi zasadami i uregulowaniami prawnymi, obowiązującymi na terytorium RP, działający dzięki połączeniu zasobów technicznych zlokalizowanych na jej terytorium[30].

29 S. Mason, *Validating identity for the electronic environment*, „Computer Law and Security Report" 2004, nr 3, s. 165; A. Sauer, *Online privacy and the online self*, „Privacy Law Bulletin" 2008, nr 9, s. 44; N. Archet [w:] *Identity Theft and Fraud*, Ottawa 2012, s. 22; B. De Vries, J. Tigchelaar, T. van der Linden, *Describing Identity Fraud: Towards a Common Definition*, „Scripted" 2008, nr 3, s. 485. Zob. także: A. Lach, *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015, s. 18–19. W odniesieniu do internetu i sieci teleinformatycznych wyróżnia się trzy rodzaje tożsamości: tożsamość osoby, tożsamość podmiotu kolektywnego oraz tożsamość sieciowa. Zob. A.M. Marschall, B.C. Tompset, *Identity theft in an online world*, „Computer Law and Security Report" 2005, nr 21, s. 129–130. Konstatuje się przy tym, że w sieci każda osoba może dysponować kilkoma tożsamościami, jedną rzeczywistą i kilkoma fikcyjnymi lub anonimowymi, wskazując, że w cyberprzestrzeni pojęcie tożsamości nabiera innego wymiaru, A. Lach, *Karnoprawna*..., s. 19.

30 A. Nowak, *Cyberprzestrzeń*..., s. 9.

System prawny Rady Europy wobec przestępstw w cyberprzestrzeni

Stopniowo pojęcie cyberprzestrzeni (ang. *cyberspace*) znalazło stałe obywatelstwo w języku potocznym[31] i zaczęło wdzierać się do języka prawniczego, a potem prawnego. W Konwencji Rady Europy o cyberprzestępczości z 23 listopada 2001 r.[32] nie użyto jednak terminu „cyberprzestrzeń". Natomiast w tytule Konwencji, w polskim tłumaczeniu, oraz w preambule i w art. 46 ust. 1 lit. b posłużono się określeniem „cyberprzestępczość", ale w art. 1 poświęconym definicjom, nie wyjaśniono jego treści[33]. Prace nad Konwencją Rady Europy o cyberprzestępczości były dość żmudne. Na pewnym etapie włączyła się w nie Rada Unii Europejskiej, wskazując, że powodem takiego kroku był przyjęty *Plan działania Unii Europejskiej w sprawie wspierania bezpiecznego wykorzystania sieci Internet*. We Wspólnym Stanowisku z dnia 27 maja 1999 r. zadeklarowano, że państwa członkowskie wspierać będą sporządzenie projektu Konwencji Rady Europy o cyberprzestępczości, wskazując, że przepisy Konwencji powinny odpowiednio uzupełnić prawo materialne i objąć przestępstwa przeciwko poufności, integralności oraz dostępności danych komputerowych, przestępstwa związane z komputerami, tak jak komputerowe oszustwo i fałszerstwo oraz przestępstwa związane z treścią, takie jak

31 M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2, s. 19–38. Zob. także: A. Tarkowski, *Internet jako technologia i wyobrażenie. Co robimy z technologią, co technologia robi z nami* [w:] D. Bartowski i inni, *Społeczna przestrzeń Internetu*, Warszawa 2006, s. 30–37.

32 Dz.U. z 2015 r., poz. 728. Konwencja ta została ratyfikowana przez Polskę dopiero 29 stycznia 2015 r., przy czym zgłoszono zastrzeżenia do art. 29 ust. 4 oraz deklaracje w odniesieniu do art. 24 ust. 7, art. 27 ust. 2 lit. a oraz art. 35 Konwencji. Por. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, passim.

33 Opiniujący Konwencję przed ratyfikacją M. Mróz zwracał jednak uwagę, że w językach oficjalnych Rady Europy istnieje pewna rozbieżność terminologii używanej w Konwencji. W tekście angielskim pojęcie „cyberprzestrzeni" nie występuje w ogóle, w tekście sporządzonym w języku francuskim dwukrotnie, przy czym raz w Preambule. W tłumaczeniu Konwencji na język niemiecki nie użyto, jak zauważył, w ogóle terminu „cyberprzestrzeń". Zob. M. Mróz, *Informacja nt. pojęcia cyberprzestrzeni oraz bezpieczeństwa i zagrożenia cyberprzestrzeni w prawie międzynarodowym i ustawodawstwie wybranych państw demokratycznych (w zw. z Drukiem sejmowym nr 4355)*, *Druk sejmowy nr 1757*, Warszawa, 22 lipca 2011. Zob. także: A. Szmyt, *Opinia prawna do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Druk sejmowy nr 4355)*, Warszawa, dnia 11 lipca 2011 r.

pornografia dziecięca. Nie odniesiono się jednak w tym dokumencie do pojęcia cyberprzestrzeni[34].

Do innych poza Konwencją o cyberprzestępczości do inicjatyw Rady Europy w analizowanym obszarze wypada zaliczyć projekty: GLACY – Global Action against Cybercrime, Cybercrime@Octopus, organizację corocznych konferencji *Octopus Interface*, Partnerstwo Wschodnie – „Współpraca przeciwko Cyberprzestępczości" (*Eastern Partnership – Cooperation against Cybercrime – Project on Cybercime@EAPII*).

Godzi się jednak zauważyć, że Konwencję tę poprzedził raport *Przestępstwa związane z komputerem. Analiza polityki legislacyjnej*[35] Organizacji Współpracy Gospodarczej i Rozwoju (*Organization for Economic Co-operation and Development*) opublikowany w 1985 r. W jego treści znalazła się robocza definicja przestępstwa komputerowego rozumianego jako każde, bezprawne, nieetyczne i nieuprawnione zachowanie, którego przedmiotem jest automatyczne przetwarzanie lub transmisja danych. Ważne było także wyróżnienie pięciu kategorii zachowań godzących w funkcjonowanie sieci komputerowej. Wśród nich zaś: oszustwa komputerowego, fałszerstwa komputerowego, uszkodzenia danych komputerowych lub programów, naruszanie praw autorskich do programu komputerowego i nieuprawnione uzyskanie dostępu do komputera lub systemu telekomunikacyjnego w wyniku naruszenia zabezpieczeń[36].

Przeciwdziałanie przestępczości w cyberprzestrzeni w systemie prawa międzynarodowego uniwersalnego (powszechnego)

W systemie uniwersalnym powszechnym, czyli w systemie ONZ problemowi przestępczości poświęcono szereg rezolucji, z których najbardziej istotną wydaje się rezolucja nr 45/121 z dnia 14 grudnia 1990 r. dotycząca przestępstw związanych z wykorzystaniem komputerów. Pozostałe rezolucje dzieli się

34 Dz.Urz. UE L 1999, nr 142, s. 1.

35 *Computer – Related Crime. Analysis of legal Policy in the OECD Area, OECD, ICCP Series nr 10*, Paris 1986.

36 Szerzej w tym przedmiocie: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 152–156.

zwykle w myśl propozycji A.M. Hubbarda i S. Schjølberga[37] na trzy grupy, a mianowicie: rezolucje odnoszące się do rozwoju w dziedzinie informacji i telekomunikacji w kontekście rozwoju w dziedzinie informacji i bezpieczeństwa, rezolucje odnoszące się do walki z kryminalnymi nadużyciami technologii informatycznej oraz rezolucje odnoszące się do tworzenia światowej kultury cyberbezpieczeństwa, a także ochrony informatycznej infrastruktury krytycznej[38]. Poza tym szereg dokumentów dotyczących przeciwdziałania cyberprzestępczości wydało biuro ds. narkotyków i przestępczości, Międzynarodowy Związek Telekomunikacyjny, a także Grupa G7/G8[39]. Zwrócić także należy uwagę na Światowy Protokół dotyczący cyberbezpieczeństwa i cyberprzestępczości[40].

System prawa unijnego wobec zjawiska przestępczości w cyberprzestrzeni

Charakterystyczną cechą dla ustawodawstwa unijnego jest to, iż unika ona w miarę konsekwentnie pojęcia „cyberprzestrzeni", zastępując ją określeniem „systemy informatyczne". Przykładem może być dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady nr 2005/222/WSiSW[41]. W części wstępnej wspomnianej dyrektywy zwrócono uwagę, że „systemy informatyczne (sic! przyp. mój J.S.) stanowią podstawowy element relacji politycznych, społecznych i gospodarczych w Unii". Wskazano, że „zależność społeczeństwa od tego typu systemu jest bardzo wysoka i stale rośnie. Dobre funkcjonowanie i bezpieczeństwo tych systemów Unii są niezbędne dla rozwoju rynku wewnętrznego oraz konkurencyjnej i innowacyjnej gospodarki. Podkreślono także, ze zarówno w obszarze Unii, jak i globalnie rośnie zagrożenie atakami na systemy informatyczne, a zwłaszcza atakami dokonywanymi

37 A.M. Hubbard, S. Schjølberg, *Harmonizing national legal approaches on cybercrime*, s. 6, https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

38 Omówienie wspomnianych rezolucji zob. F. Radoniewicz, *Odpowiedzialność karna…*, s. 196–200.

39 Prezentacja tych dokumentów zob. F. Radoniewicz, *Odpowiedzialność karna…*, s. 200–217.

40 S. Ghernaouti-Helie, S. Schjølberg, *Global Treaty on Cybersecurity and Cyber Crime, Second edition 2011*, https://www.researchgate.net/publication/236200268_A_global_treaty_on_cybersecurity_and_cybercrime.

41 Dz.Urz. UE L 2013, nr 218, s. 8.

w ramach przestępczości zorganizowanej". Warto zauważyć, że w tekście tym nie użyto w ogóle pojęcia „cyberprzestrzeni". Pojęcie to pojawiło się natomiast w rezolucji Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony (2012/2096(INI)) pkt 35, w którym stwierdzono, że ochrona krytycznej infrastruktury teleinformatycznej uwzględniona jest w strategii bezpieczeństwa wewnętrznego UE w kontekście zwiększenia poziomu bezpieczeństwa obywateli i przedsiębiorstw w cyberprzestrzeni[42].

W prawie Unii Europejskiej od dość dawna funkcjonowały akty normatywne o charakterze niewiążącym, których zadaniem jest ochrona bezpieczeństwa systemów informatycznych. Zaliczyć do nich należy decyzję ramową Rady 2005/222/WSiSW z 24 lutego 2005 r.[43] Nie wolno także zapominać o treści rozporządzenia 2004/460/WE Parlamentu Europejskiego i Rady z 10 marca 2004 r. ustanawiającego Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[44]. Z opublikowanego przez Komisję Europejską w dniu 14 lipca 2008 r. sprawozdania z wykonania decyzji ramowej 2005/222/WSiSW wynika, że większość państw członkowskich podjęła kroki w celu implementacji postanowień decyzji ramowej. Niemniej wydając dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 20 sierpnia 2013 r. dotyczącej ataków na systemy informacyjne, zdecydowano się zastąpić tą dyrektywą decyzję ramową Rady 2005/222/WSiSW[45]. W treści dyrektywy sformułowano szereg przestępstw polegających m.in. na: niezgodnym z prawem dostępie do systemów informatycznych (art. 3), niezgodną z prawem ingerencją w systemie informatycznym

42 Dz.Urz. UE C 2015, nr 419, s. 145. W dalszej części tego dokumentu w pkt 44 odniesiono się do konieczności szerszej międzynarodowej współpracy i ostatecznego porozumienia dotyczącego ustalenia wspólnego rozumienia norm zachowania w cyberprzestrzeni. W pkt 55 stwierdzono, że UE i USA to największe źródła cyberprzestrzeni (sic!) i jej użytkowników.

43 Dz.Urz. UE L 2005, nr 69, s. 67. Od razu wypada zwrócić uwagę na istniejące rozbieżności między wspomnianą decyzją ramową a przytoczoną wyżej Konwencją o cyberprzestępczości w systemie Rady Europy. W uzasadnieniu decyzji ramowej odwołano się do wytycznych z zalecenia OEDC C (92) 188 z 26 listopada 1992 r. dotyczącego wytycznych w zakresie bezpieczeństwa systemów informatycznych (92) 188. *Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C (92) 188/ FINAL]*. Wspomniane zalecenie (92) zostało zastąpione przez zalecenie OECD C (2002) 131 z 25 lipca 2002 r. w sprawie wytycznych w zakresie bezpieczeństwa systemów i sieci informatycznych w kierunku kultury bezpieczeństwa. *Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security of 25 July 2002 [C (2002) 131]*. Wytyczne te zostały zrewidowane po raz pierwszy w 2007 r. W grudniu 2013 r. zakończono kolejną ich rewizję.

44 Dz.Urz. UE L 2004, nr 77, s. 1.

45 Dz.Urz. UE L 2013, nr 218, s. 8.

(art. 4), niezgodną z prawem przechwytywania środkami technicznymi niepublicznych przekazów internetowych (art. 6) oraz na bezprawnym wytwarzaniu, sprzedaży, dostarczaniu w celu użycia, przewozie i posiadaniu narzędzi do popełniania przestępstw komputerowych (art. 7). Przewidziano także karalność podżegania, pomocnictwa do wszystkich przestępstw przewidzianych w dyrektywie oraz usiłowanie popełnienia przestępstw polegających na bezprawnej ingerencji w system informatyczny oraz ingerencji w dane komputerowe w systemie informatycznym[46].

Dla podjętej w tym miejscu problematyki, istotniejsze znaczenie wydaje się mieć dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze o łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[47]. Dyrektywa ta generalnie zakazuje przejmowania kontroli nad komputerami, przechwytywania komunikatów przesłanych za pośrednictwem publicznych sieci komunikacyjnych, nakazując jednocześnie państwom członkowskim zapewnienie poufności komunikacji i nie pozwalając na monitorowanie, nagrywanie, przechowywanie, kontrolowanie komunikatów i związanych z nimi danych o ruchu przez osoby inne niż użytkownicy bez zgody zainteresowanych użytkowników. Wyjątkiem jest działanie w celu zapewnienia bezpieczeństwa narodowego i bezpieczeństwa państwa, obron-

46 W opinii *Electronic Frontier Foundation (EFF)* wskazano, że istnieje możliwość pociągnięcia do odpowiedzialności karnej aktywnych użytkowników p2p tj. np. Tor, która daje możliwość zapewnienia sobie anonimowości w trakcie korzystania z internetu lecz nie ma na celu zapewnienia anonimowości w związku z wymianą plików, jak to ma miejsce, w takich systemach jak ANts, P2P, Freenet, GNUnet czy MUTE. Z założenia Tor służyć ma obronie przed wszystkimi sieciowej inwigilacji, umożliwiając swobodną, wolną od kontroli państwa wymianę informacji. Zob. *EFF Comments on the Draft Directive on Attacks against Computer Systems*, https://www.eff.org/Directive-Attacks-against-Computer-Systems. Jak wskazuje F. Radoniewicz podniesiony w opinii problem nie dotyczy polskiego systemu prawnego z uwagi na to, że przewiduje on możliwość podżegania i pomocnictwa w odniesieniu do konkretnych osób, a nie do niesprecyzowanej, nieokreślonej grupy podmiotów. F. Radoniewicz, *Odpowiedzialność karna…*, Warszawa 2016, s. 198.

47 Dz.Urz. UE L 2002, nr 201, s. 37, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE Dz.Urz. UE L 2009, nr 337, s. 11. Zob. w tej kwestii: M.B. Kanarski, J. Radzikowska, *Nowe ramy regulacyjne dla usług łączności elektronicznej* [w:] M. Rogalski (red.), *Prawo telekomunikacyjne*, LEX 2011. Z problematyką tą wiąże się także dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) Dz.Urz. UE L 2002, nr 108, s. 33, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/140/WE z 25 listopada 2009 Dz.Urz. UE L 2009, nr 337, s. 37 i sprostowana Dz.Urz. UE L 2013, nr 241, s. 8.

ności, bezpieczeństwa publicznego oraz dążenie do zapobiegania, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej[48].

Naruszeniem prywatności jest w wielu przypadkach posługiwanie się mową nienawiści mimo istnienia międzynarodowych standardów zakazujących tego rodzaju działań. Wskazać wśród nich należy w pierwszym rzędzie decyzję ramową z dnia 28 listopada 2008 r. 2008/913/WSiSW w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych[49]. W treści art. 1 decyzji ramowej nałożono na każde państwo członkowskie Unii Europejskiej zastosowanie niezbędnych środków w celu zapewnienia karalności czynów polegających na publiczne nawoływanie do przemocy lub nienawiści skierowanej przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, popełnianych także przez publiczne rozpowszechnianie lub rozprowadzanie tekstów, obrazów lub innych materiałów (art. 1 ust. 1 pkt a i b). Ponadto w decyzji ramowej wskazano, że każde państwo członkowskie Unii Europejskiej ma zapewnić karalność czynów polegających na publicznym aprobowaniu, negowaniu lub rażącym pomniejszaniu zbrodni ludobójstwa, zbrodni przeciwko ludzkości oraz zbrodni wojennych w rozumieniu art. 6, 7 i 8 statutu Międzynarodowego Trybunału Karnego skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi (art. 1 ust. 1 pkt c). Zobowiązano w końcu państwa do zapewnienia karalności czynów polegających na publicznym aprobowaniu, negowaniu lub rażącym pomniejszaniu zbrodni określonych w art. 6 Karty Międzynarodowego Trybunału Wojskowego załączonej do porozumie-

48 E. Preis, *Glosa do wyroku Trybunału Sprawiedliwości z dnia 29 stycznia 2008, C – 275/06*, „Europejski Przegląd Sądowy" 2009, nr 4, s. 49.

49 Dz.Urz. UE 2008 L 328/55 z 6 grudnia 2008 r. Decyzja ta rozszerza treść zawartą we Wspólnym Działaniu Rady 96/443/WSiSW z dnia 15 lipca 1996 r. dotyczącą działania w celu zwalczania rasizmu i ksenofobii (Dz.Urz. UE 1996 L 185 z 24 lipca 1996 r.), deklarując istnienie konieczności dodatkowych działań legislacyjnych w związku z potrzebą dalszego zbliżenia przepisów ustawowych i wykonawczych państw członkowskich oraz pokonania przeszkód w skutecznej współpracy sądowej, wynikających głównie z rozbieżności w systemach prawnych poszczególnych państw członkowskich, przy czym w treści art. 11 decyzji ramowej uchylono Wspólne Działanie 96/443/WSiSW.

nia londyńskiego z dnia 8 sierpnia 1945 r., a skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi (art. 1 ust. 1 pkt d).

Niezwykle istotna w prawie unijnym jest dyrektywa Parlamentu Europejskiego i Rady (UE) 2017 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW[50]. W jej treści przypomniano przyjęty przez Radę Europy w 2015 r. Protokół Dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim i ksenofobicznym popełnionych przy użyciu systemów komputerowych[51]. Warto zauważyć, że w treści tego Protokołu – ratyfikowanego przez Polskę 29 stycznia 2015 r., zdefiniowano „materiały rasistowskie i ksenofobiczne", wskazując, że pod tym terminem należy rozumieć każdy materiał pisemny, każdy wizerunek lub każde inne wyrażenie myśli i teorii, które nawołują, popierają lub podżegają do nienawiści, dyskryminacji lub przemocy przeciw jakiejkolwiek osoby lub grupie osób ze względu na rasę, kolor, pochodzenie narodowe lub etniczne, jak również religię, jeżeli wykorzystywana jest ona jako pretekst do zachowań o charakterze rasistowskim lub ksenofobicznym, gwałcących prawa człowieka i stanowiących zagrożenie dla rządów prawa i demokratycznej stabilności. W treści Protokołu zwrócono uwagę na środki, jakie państwa unijne powinny podjąć na szczeblu krajowym w kwestii zwalczania: rozpowszechniania materiałów rasistowskich i ksenofobicznych w systemie komputerowym; gróźb i zniewag spowodowanych rasizmem i ksenofobią; a także w kwestii zwalczania, zaprzeczania lub poważnego umniejszania znaczenia, akceptacji lub usprawiedliwienia, zbrodni ludobójstwa oraz zbrodni przeciwko ludzkości.

We wspomnianej dyrektywie z 15 marca 2017 r. zauważono także, że przestępstwo związane z publicznym nawoływaniem do popełniania czynów mający charakter terrorystyczny obejmuje m.in. pochwalanie i usprawiedliwianie terroryzmu, rozpowszechnianie w internecie lub poza nim wiadomości lub obrazów, w tym obrazów dotyczących ofiar terroryzmu, w celu zdobycia poparcia dla idei terrorystycznych lub w celu poważnego zastraszania ludności.

50 Dz.Urz. UE L 2017, nr 88, s. 6.
51 Dz.U. 2015, poz. 730.

Taki czyn – jak wskazano – powinien podlegać karze, jeżeli stwarza niebezpieczeństwo popełnienia aktów terrorystycznych. W każdym konkretnym przypadku przy ocenianiu, czy takie niebezpieczeństwo istnieje, uwzględnić należy szczególne okoliczności sprawy, takie jak autora i adresata wiadomości, a także kontekst, w jakim doszło do popełnienia czynu. To czy niebezpieczeństwo jest istotne, i czy ma ono wiarygodny charakter, należy również brać pod uwagę przy stosowaniu przepisu o publicznym nawoływaniu zgodnie z prawem krajowym.

Podkreślono także, że dyrektywa zawiera wyczerpujący wykaz poważnych przestępstw, takich jak ataki na życie ludzkie stanowiących czyny umyślne, które można zakwalifikować jako przestępstwa terrorystyczne wyłącznie w przypadku, gdy zostały popełnione w określonym celu terrorystycznym, mianowicie, aby poważnie zastraszyć ludność, bezprawnie zmusić rząd lub organizację międzynarodową do podjęcia lub zaniechania działania, lub aby poważnie zdestabilizować lub zniszczyć podstawowe struktury polityczne, konstytucyjne, gospodarcze lub społeczne danego państwa lub danej organizacji międzynarodowej. Groźby popełnienia takich czynów umyślnych również – jak podkreślono w motywach dyrektywy – należy uznawać za przestępstwa terrorystyczne, jeżeli obiektywne przesłanki wskazują, że dopuszczono się ich, kierując się jednym z wymienionych celów terrorystycznych. Natomiast czynów, których celem jest na przykład zmuszenie rządu do podjęcia lub zaniechania jakiegokolwiek działania, ale których nie umieszczono w wyczerpującym wykazie poważnych przestępstw, nie uznaje się zgodnie z niniejszą dyrektywą za przestępstwa terrorystyczne.

Zauważono także, że niezbędne jest uznanie za przestępstwo podróży zagranicznych w celach terrorystycznych, obejmując nie tylko popełnianie przestępstw terrorystycznych i prowadzenie lub odbywanie szkolenia, lecz także uczestnictwo działalności grupy terrorystycznej. Podkreślono, że karze powinno w państwach członkowskich podlegać – jako pomocnictwo w terroryzmie lub finansowanie terroryzmu – udzielanie materialnego wsparcia terroryzmowi poprzez osoby zajmujące się dostarczaniem lub przemieszczaniem usług, mienia i towarów, w tym transakcji handlowych obejmujących wprowadzanie na obszar Unii lub wyprowadzanie z tego obszaru, takich jak sprzedaż, nabycie lub wymiana dóbr kultury o wartości archeologicznej, artystycznej, historycznej lub naukowej, które nielegalnie wywieziono z obszaru kontrolowanego przez grupę terrorystyczną w momencie wywozu lub osoby będące pośrednikami w takich działaniach, jeżeli dokonywane są one ze świadomością, że operacje te lub pochodzące z nich przychody są w całości lub w części

przeznaczone do celów terrorystycznych lub przysporzą one korzyści grupom terrorystycznym. Podniesiono, że państwa członkowskie powinny zapewnić środki ochrony wsparcia i pomocy ofiarom terroryzmu zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2012/29/UE z dnia 25 października 2012 r. ustanawiającą normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw oraz zastępującą decyzję ramową Rady 2001/220/WSiSW[52]. W treści dyrektywy wskazano czyny umyślne, które zgodnie z prawem krajowym ze względu na swój charakter lub kontekst mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej i z tego tytułu powinny być zaliczone do przestępstw terrorystycznych. Wskazano wśród nich m.in. także niezgodne z prawem ingerencje w systemy informatyczne, utrudnianie lub zakłócanie ich funkcjonowania, przekazanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych[53].

W doktrynie podkreśla się, że standardy w zakresie przestępczości w cyberprzestrzeni, w tym także ścigania mowy nienawiści wypracowują także judykaty Europejskiego Trybunału Praw Człowieka, Komitetu Praw Człowieka ONZ, Rady Europy oraz w przyszłości Trybunału Sprawiedliwości w Luksemburgu[54]. Można poddawać w wątpliwość możliwość zwalczania mowy

52 Dz.Urz. UE L 2012, nr 315, s. 57. Zob. E. Bieńkowska, L. Mazowiecka (red.), *Dyrektywa Parlamentu Europejskiego i Rady ustanawiająca normy minimalne w zakresie praw wsparcia i ochrony ofiar przestępstw. Komentarz*, Warszawa 2014, passim.

53 Oprócz tego zaliczono do czynów terrorystycznych działania, których celem jest poważne zastraszenie ludności, bezprawne zmuszenie rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania, poważna destabilizacja lub zniszczenie podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych jakiegoś państwa lub organizacji międzynarodowej, przejawiająca się w atakach na życie ludzkie, które mogą spowodować śmierć, w atakach na integralność fizyczną osoby, a także: porwanie lub branie zakładników; powodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury w tym także systemu informacyjnego, platform na szelfie kontynentalnym, miejsc publicznych, mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze. Ponadto za przestępstwa terrorystyczne uznano wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie, lub używanie materiałów wybuchowych lub broni, w tym także chemicznej, biologicznej, radiologicznej lub jądrowej, a także badania nad taką bronią; uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi, względnie wybuchów zagrażających życiu ludzkiemu, wreszcie zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego.

54 A. Gliszczyńska-Grabias, *Międzynarodowoprawne standardy wolności a mowa nienawiści* [w:] D. Bychawska-Sinarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013, s. 45–50.

nienawiści środkami prawa karnego[55], aczkolwiek istnieje wyraźna tendencja do tego, aby przepisy prawa karnego użyć do tego właśnie celu[56].

Wypada przy tym zauważyć, że ilość regulacji normatywnych nie przekłada się na sukcesy w zwalczaniu zjawiska przestępczości i programy oraz działania Rady Europy i Unii Europejskiej zmierzające w kierunku ochrony użytkowników internetu, dają nikłe rezultaty[57]. Niewiele więcej przynoszą inicjatywy obywatelskie, działania lobbingowe, a także próby społecznych re-

55 Czyni tak Ewa Łętowska, stwierdzając, że: „Granice między słowem, bez którego nie ma demokracji, i słowem, które zabija wolność lub prawo innego człowieka, obecnie nie rysują się u nas jasno. Sądowy standard, który służy ich wytyczeniu na tle prawa, znajduje się ciągle na etapie ustalania metodą prób i błędów". Zwraca ona jednak uwagę, że istnieje „wielka różnica między celowym zniesławieniem, obrażaniem, szczuciem, a krytycznym dyskursem publicznym. Wolność słowa i wolność wyrażania poglądów nie usprawiedliwia naruszania praw i wolność innych. To elementarz praw człowieka". Dodaje przy tym, „dlatego nie przekonują mnie ci, którzy uważają, że w internecie i właśnie akurat w nim, tylko dlatego, że jest internetem można umieścić wszystko o wszystkim. W internecie wolno tyle i tylko tyle, ile wolno w innych mediach. »Złe słowo« to słowo szczujące, raniące, poniżające, szydzące, nawołujące do czynów gwałtownych". E. Łętowska, *Zwodnicze pokusy karania hate speech* [w:] D. Bychawska-Siniarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013, s. 18–19. Zob. także: A. Śledzińska-Simon, *Decyzja ramowa w sprawie zwalczania pewnych form przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii Europejskiej* [w:] R. Wieruszewski, M. Wyszykowski, A. Bodnar, A. Gliszczyńska-Grabias (red.), *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010, s. 93–113.

56 Por. w tym przedmiocie I. Hare, J. Weinstein (red.), *Extreme Speech and Democracy*, Oxford 2009; A. Cortese, *Opposing hate speech*, Westport 2006; R. Cohen-Almagor, *Holocaust Denial is a Form of Hate Speech*, „The Amsterdam Law Forum" 2009, no. 2; D.O. Brink, *Millian Principles, Freedom of Speech, and Hate Speech*, „Legal Theory" 2001, no. 7; N. Ghanea, *Expression and Hate Speech in the ICCPR: Compatible or Clashing?*, „Religion and Human Rights" 2010, no. 5.

57 Zob. m.in. *Program Safer Internet Action Plan* ustanowiony *Decyzją Parlamentu Europejskiego i Rady nr 276/1999/WE z dnia 25 stycznia 1999 r. przyjmującą wieloletni plan działań Wspólnoty w zakresie promowania bezpieczniejszego korzystania z Internetu poprzez zwalczanie sprzecznych z prawem i szkodliwych treści w światowych sieciach komputerowych* Dz.Urz. UE L, 1999, L 33 z 6 luty 1999 r. zmieniona Decyzją Parlamentu Europejskiego i Rady nr 1151/2003/WE z 16 czerwca 2003, Dz.Urz. UE L 162 z 1 lipca 2003. Program *Safer Internet Plus* (2005–2008) przyjęty Decyzją Parlamentu Europejskiego i Rady nr 854/2005/WE z 11 maja 2005 r. w sprawie ustanowienia wieloletniego programu wspólnotowego na rzecz promowania bezpieczniejszego korzystania z internetu i nowych technologii sieciowych Dz.Urz. UE L 2005, nr 149, s. 1. Obowiązywanie tej decyzji wygasło z dniem 31 grudnia 2008 r. Program *Safer Internet* wynikający z decyzji Parlamentu Europejskiego i Rady nr 1351/2008/WE z 16 grudnia 2008 r. w sprawie ustanowienia wieloletniego, wspólnotowego programu ochrony dzieci korzystających z internetu oraz z innych technologii informacyjnych Dz.Urz. UE L 2008, nr 348, s. 118. Kolejnym projektem jest *Roundtable* prowadzony w ramach programu *Safer Internet Action Plan*. Zob. *Youth Protection Roundtable*, www.yprt.ue.

gulacji[58]. W tej sytuacji wydaje się być uzasadnione stanowisko wyrażone jakiś czas temu w literaturze, iż internet jawi się jako przysłowiowa „butelka", z której nieostrożnie wypuszczono złośliwego dżina, który nie bacząc na nic narusza prywatność, depcze godność i cześć terroryzując swoimi działaniami przerażone społeczności. Za tym dżinem kryją się jednak złośliwi i przebiegli lub jedynie obojętni na cudzą krzywdę ludzie[59].

Zwalczenie cyberprzestępczości w polskim systemie prawnym

W polskim systemie prawnym definicja cyberprzestrzeni pojawiła się w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[60], po nowelizacji tej ustawy ustawą z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polski oraz niektórych innych ustaw[61]. W myśl art. 2 ust. 1b dodanym przez art. 1 pkt 2 wspomnianej ustawy z 30 sierpnia 2011 r. przez cyberprzestrzeń należy rozumieć przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[62] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Identyczne rozwiązanie wprowadzono: do tekstu ustawy z 21 czerwca 2002 r. o stanie wyjątkowym – przez art. 2 ust. 1a w oparciu o art. 2 pkt 2 ustawy z 30 sierpnia 2011 r.[63] o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw oraz do tekstu ustawy z 18 kwietnia 2002 r. o stanie

58 M. Gruchoła, *Ochrona użytkowników Internetu w państwach Unii Europejskiej*, Lublin 2012, s. 267–302.
59 J. Sobczak, K. Kakareko, *Odpowiedzialność za przestępstwa popełnione w sieci, a kwestia prywatności* [w:] J. Sobczak, K. Chałubińska-Jentkiewicz, K. Kakareko, *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, s. 1–32.
60 T.j. Dz.U. 2016, poz. 851.
61 Dz.U. 2011, nr 222, poz. 1323.
62 Dz.U. 2005, nr 64, poz. 565 ze zm.
63 Dz.U. 2011, nr 222, poz. 1323.

klęski żywiołowej[64], dodając art. 3 ust. 1 pkt 4 przez art. 3 pkt 1 wspomnianej już ustawy z 30 sierpnia 2011 r.[65]

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022 przyjęta 9 kwietnia 2013 r. uchwałą nr 67 Rady Ministrów[66] nie definiuje pojęcia „cyberprzestrzeni", natomiast terminem tym się posługuje, wskazując, że do głównych działań pogłębienia współpracy na rzecz bezpieczeństwa cybernetycznego na forum NATO i UE należy uwzględnienie w polityce bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej nowych elementów wynikających z prac NATO i UE nad polityką bezpieczeństwa cybernetycznego. Wskazano także, że dążąc do nasycenia nowoczesnym uzbrojeniem i sprzętem wojskowym sił zbrojnych, trzeba doprowadzić do tego, aby były one odporne na zagrożenia z cyberprzestrzeni. Za główne działania w zakresie podwyższania stopnia zabezpieczeń zasobów teleinformatycznych administracji publicznych i państwowej przed zagrożeniami sieci internet oraz terroryzmem, uznano przyjęcie polityki ochrony cyberprzestrzeni Rzeczpospolitej Polskiej[67]. Skonstatowano przy tym, że wzrost zagrożeń w obszarze cyberprzestrzeni wymaga dostosowywania i ciągłego rozwijania istniejących struktur systemu reagowania, wiążąc to z rozwojem Rządowego Zespołu Reagowania na Incydenty Komputerowe. Wskazano, że posiadania przez Agencję Bezpieczeństwa Wewnętrznego oraz resort obrony narodowej silnych wyposażonych w zaawansowane technologie zespołów reagowania, usprawni realizowanie współpracy międzynarodowej oraz pozwoli osiągnąć nowe zdolności operacyjne w zakresie zadań reagowania na incydenty bezpieczeństwa teleinformatycznego oraz dowodzenia i kierowania w celach przestrzeni. Nałożono przy tym na ministra właściwego do spraw administracji publicznej, informatyzacji i łączności zadanie opracowanie polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. Podkreślając, że projekt taki winien zostać przyjęty przez Radę Ministrów jeszcze w 2013 r.

64 T.j. Dz.U. 2014, poz. 333 ze zm.

65 Zob. w tym przedmiocie J. Kosiński, *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013, s. 462–463. F. Radoniewicz, *Odpowiedzialność karna…*, s. 67.

66 M.P. 2013, poz. 377.

67 Odwołano się w tym miejscu do dokumentu przyjętego przez Komitet Rady Ministrów ds. Cyfryzacji w dniu 28 listopada 2012 r.

Uchwałą nr 252 Rady Ministrów z 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na 2015–2019”[68], precyzując założenia i systematykę programu, podkreślono, że winien być on skorelowany z Polityką Ochrony Cyberprzestrzeni. Zauważono także, że cyberprzestrzeń może być istotną sferą działalności terrorystycznej, wykorzystywaną przez organizacje terrorystyczne, zarówno do prowadzenia bezpośrednich ataków na serwery rządowe w celu uniemożliwienia ich funkcjonowania, dezinformacji lub pozyskiwania danych, jak i upowszechniania radykalnej ideologii, pozyskiwania ich zwolenników, czy prowadzenia instruktażu w zakresie podejmowania indywidualnych aktów terroru. Może być ona także – jak zauważono – wykorzystywana do dokonywania nielegalnego transferu środków finansowych na działalność terrorystyczną. Zdefiniowano, że atak cyberterrorystyczny winien być rozumiany, jako nielegalne działanie w cyberprzestrzeni o podłożu politycznym lub ideologicznym ukierunkowane na wywołanie strachu i skutkujące przemocą przeciwko ludziom lub mieniu, którego celem jest wymuszanie na rządzie oraz społeczeństwie realizacji celów politycznych lub społecznych zakładanych przez atakującego. Atakami terrorystycznymi mogą być więc – jak stwierdzono – nielegalne groźby i ataki przeciwko komputerom, sieciom komputerowym i informacjom w nich przechowywanym, a także działania sabotażowe prowadzone w cyberprzestrzeni, w tym także w odniesieniu do infrastruktury krytycznej oraz prowadzenie dezinformacji. Wskazano, że na poziomie strategicznym Rada Ministrów może podjąć uchwałę o skierowaniu do prezydenta wniosku o wprowadzenie stanu wyjątkowego w razie zewnętrznego zagrożenia państwa spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni i wnioskować o wprowadzenie stanu wojennego. Wywiedziono, że należy intensyfikować działania właściwych służb i instytucji w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni. Dążąc do ochrony w cyberprzestrzeni wskazano na konieczność jej monitorowania i zwalczania zagrożeń, i ataków o charakterze cyberterrorystycznym[69]. W dalszej części Narodowego Programu Antyterrorystycznego w sposób szczegółowy w załącznikach wskazano na konieczność współdzia-

68 M.P. 2014, poz. 1218.

69 Kwestią przeciwdziałania zagrożeniom w cyberprzestrzeni poświęcony jest dokument *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* przyjęty uchwałą nr 111/2013 Rady Ministrów z 25 czerwca 2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html.

łania z organizacjami międzynarodowymi zajmującymi się przeciwdziałaniem i zwalczaniem zagrożeń o charakterze terrorystycznym, w tym z Organizacją Narodów Zjednoczonych, Unią Europejską, NATO, Radą Europy, OBWE. Zauważyć jednak należy, że posługując się wielokrotnie terminem „cyberprzestrzeń" w żadnym miejscu wspomnianego dokumentu nie zdefiniowano tego pojęcia[70].

W uchwale nr 23 Rady Ministrów z 8 marca 2016 r. w sprawie „Programu ograniczenia przestępczości i aspołecznych zachowań *Razem Bezpieczniej im. Władysława Stasiaka na lata 2016 i 2017*"[71] wskazano formułując jako jeden z celów szczegółowych, iż edukacja dla bezpieczeństwa powinna dotyczyć także cyberprzestrzeni. Potrzeba współpracy w zakresie zapobiegania i wykrywania sprawców przestępstw pojawiła się także w umowach 2 lipca 2005 r. między Rządem Rzeczypospolitej Polskiej a Rządem Indonezji o współpracy w zwalczaniu międzynarodowej przestępczości zorganizowanej i innych rodzajów przestępczości[72] oraz w umowie z dnia 9 października 2006 r. między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii o współpracę w zakresie zwalczania przestępczości zorganizowanej i innych rodzajów przestępczości[73].

Pojęcie cyberprzestrzeni zdefiniowano jednak we wspomnianym już dokumencie *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* z 25 czerwca 2013 r.[74] Cyberprzestrzeń zdefiniowano: „jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności

70 Należy podkreślić, że ustawą z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. 2015, poz. 2281 ze zm.) w art. 1 pkt 1 wskazano, że dział informatyzacja obejmuje także bezpieczeństwo cyberprzestrzeni – jednak i tu z oczywistych względów nie zdefiniowano pojęcia cyberprzestrzeń.

71 M.P. 2016, poz. 293

72 Dz.U. 2016, poz. 1660.

73 Dz.U. 2016, poz. 1323.

74 http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html. Został on opracowany w Ministerstwie Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego w oparciu o: omówiony 9 marca 2009 r. przez Komitet Stały Rady Ministrów dokument „Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia", okresowe raporty o stanie bezpieczeństwa obszaru gov.pl, publikowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, decyzję przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji nr 1/2012 z dnia 24 stycznia 2012 r. w przedmiocie powołania Zespołu zadaniowego do spraw ochrony portali rządowych.

podmiotów realizujących zadania publiczne[75] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami; zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[76], art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym[77] oraz art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej"[78]. Natomiast cyberprzestrzeń Rzeczypospolitej Polskiej określono jako: „cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)". Wypada zauważyć, że w oparciu o te rozwiązania cyberprzestrzeń nie będzie obejmowała komputerów, ponieważ wskazuje na tzw. „urządzenia końcowe", czyli modem, telefon, router, ewentualnie karta sieciowa, które są „zakończeniem sieciowym", wskazanych w przytoczonej definicji w przepisach prawa. W literaturze podkreśla się, że należałoby zmienić definicję cyberprzestrzeni i cyberprzestrzeni RP w taki sposób, aby ta definicja obejmowała zasoby techniczne każdego użytkownika zarówno osoby fizycznej, obywatela oraz przedsiębiorcy. Zwraca się także uwagę, że używane w dokumencie pojęcie „cyberatak" nie obejmuje swoim zakresem ataków przeprowadzonych z cyberprzestrzeni RP na cyberprzestrzeń innych państw. Ma być to wynikiem tego, że pojęciem cyberprzestrzeni zostało zawężone do zasobów technicznych opisanych w przepisach prawa polskiego, tj. w pierwszym rzędzie do ustawy z dnia 17 maja 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz do prawa telekomunikacyjnego[79]. Z faktu, że pojęcie „cyberprzestrzeń" użyte w tym dokumencie nie obejmuje swoim zakresem pojęciowym w cyberprzestrzeni innego państwa, ewentualnie w cyberprzestrzeni globalnej, można by wysnuć wniosek, że atak przeprowadzony z wykorzystywaniem cyberprzestrzeni RP w odniesieniu do cyberprzestrzeni innego państwa nie jest cyberatakiem.

Przestępstwa popełniane przy użyciu komputerów nie mają charakteru jednorodnego. Wyróżnia się wśród nich skierowane przeciwko ochronie

75 Dz.U. nr 64, poz. 565 ze zm.
76 Dz.U. nr 156, poz. 1301 ze zm.
77 Dz.U. nr 113, poz. 985 ze zm.
78 Dz.U. nr 62, poz. 558 ze zm.
79 A. Nowak, *Cyberprzestrzeń*..., s. 9.

informacji, zawarte w rozdz. XXXIII k.k.[80], przestępstwa przeciwko mieniu[81] i wiarygodności dokumentów[82], do innych przestępstw komputerowych zwykło się zaliczać sprowadzanie powszechnego niebezpieczeństwa na skutek zakłócenia procesów automatycznego przetwarzania danych (art. 165 § 1 pkt 4 k.k.), szpiegostwo komputerowe (art. 130 § 3 k.k.), rozpowszechnianie oraz posiadanie treści pornograficznych przedstawiających małoletniego lub uzyskanie do nich dostępu (art. 202 § 4 a, b i c k.k.), nawiązywanie kontaktu z małoletnim w celu produkowania lub utrwalania treści pornograficznych za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej (art. 200 a k.k.).

Oczywiście przy użyciu komputera za pośrednictwem internetu, możliwe jest także propagowanie faszyzmu lub innego totalitarnego ustroju państwa (art. 256 k.k.), znieważanie grup ludności lub poszczególnych osób z powodu ich przynależności narodowej, etnicznej i rasowej, wyznaniowej (art. 257 k.k.), ujawnianie tajemnicy państwowej (art. 265 k.k.), obrażanie uczuć religijnych (art. 196 k.k.), rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody (art. 191 k.k.), groźba karalna (art. 190 k.k.), uporczywe nękanie (art. 190a k.k.), a także stręczycielstwo poprzez przekaz internetowy i czerpanie z tego tytułu korzyści majątkowych (art. 204 k.k.). Ponadto przy użyciu przekazu internetowego możliwe jest popełnienie przestępstwa zniesławiania (art. 212 k.k.), bądź zniewagi (art. 216 k.k.).

Dla sprawcy dopuszczającego się większości z tych przestępstw, internet jest jedynie narzędziem, środkiem służącym do popełnienia przestępstwa. Nie wszystkie z występków popełnionych przy użyciu komputerów godzą w prywatność. Niewątpliwie z naruszeniem prywatności wiąże się *hacking*

80 Wśród nich nieuprawniony dostęp do informacji (hacking) (art. 267 § 1 k.k.), nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych (art. 267 § 2 k.k.), nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych (art. 267 § 3 k.k.), ujawnianie informacji uzyskanych nielegalnie (art. 267 § 4 k.k.), naruszenie integralności zapisu informacji (art. 268 § 2 i 3 k.k.), niszczenie danych informatycznych (art. 268 a k.k.), sabotaż komputerowy (art. 269 k.k.), zakłócanie pracy systemu komputerowego lub sieci informatycznej (269a k.k.), bezprawne wykorzystanie programów i danych (art. 269 b k.k.).

81 Nielegalne uzyskanie programu komputerowego w celu osiągnięcia korzyści majątkowej (art. 278 § 2 k.k.), paserstwo programu komputerowego (art. 293 § 1 k.k.), oszustwo komputerowe (art. 287 k.k.), oszustwo telekomunikacyjne tj. kradzież impulsów telefonicznych (art. 285 k.k.).

82 Fałszerstwo komputerowe (art. 270 k.k.), niszczenie lub pozbawianie mocy dowodowej dokumentu elektronicznego (art. 276 k.k.), wyłudzenie (art. 297 § 1 k.k.), nierzetelne prowadzenie dokumentacji gospodarczej (art. 303 k.k.), fałszowanie kart płatniczych (art. 310 k.k.).

(nieuprawniony dostęp do informacji)[83], a także nielegalny podsłuch i inwigilacja przy pomocy urządzeń technicznych i programów komputerowych. Podkreślenia wymaga, że „siła rażenia" przekazu komputerowego jest znacznie szersza i dotkliwsza niż działanie za pomocą metod „tradycyjnych", tj. przekazu osobistego, a nawet informacji w prasie drukowanej bądź za pośrednictwem radiofonii, bądź telewizji. Sytuacja ta dotyczy zwykle zniesławień i zniewag, które z sadystyczną wręcz lubością zamieszczają użytkownicy rozmaitych for internetowych i portali społecznościowych. To właśnie w internecie napotkać można przejawy mowy nienawiści, odwołującej się do sądów, przekonań i ocen w utrwalonych stereotypach[84].

Zakończenie

Polskie rozwiązania legislacyjne odpowiadają zasadniczo rzecz biorąc wymogom systemu prawa unijnego, uniwersalnego, a także systemu Rady Europy. Niemniej podobnie jak wspomniane regulacje międzynarodowe nie do końca nadążają za szybkim postępem techniki, rozwojem sieci i wyzwaniami, jakie niesie ona za sobą. Wciąż pojawiają się nowe w większym lub mniejszym stopniu sprzeczne z obowiązującym prawem czyny obnażające jednocześnie niedoskonałość przyjętych regulacji. Proces ten wydaje się nieuchronny. Prowadzi on do niezwykle pesymistycznych wniosków, gdyż w ślad za czynami naruszającymi stabilność społeczną pojawiają się coraz silniejsze głosy, żądające kontroli przekazu w celu powstrzymania zjawisk wysoce negatywnych społecznie. Mowa nienawiści, towarzyszące jej fake newsy to tylko przykłady działań wysoce dolegliwych dla jednostek a niebezpiecznych dla grup społecznych. Znacznie groźniejsze może być przewidywane zjawisko cyberwojny bądź rozmaite typy zachowań godzące w struktury gospodarcze. Niestety rzeczywistość wydaje się potwierdzać konstatacje niektórych myślicieli, że ludzie

83 Szczegółową analizę technicznych aspektów hackingu przynosi doskonała monografia F. Radoniewicza, *Odpowiedzialność karna za hacking*..., s. 74–118. Zwrócić w tym miejscu wypada szczególniejszą uwagę na używane przez hackerów metody, wśród których szczególnie istotne wydają się tzw. socjotechnika lub inżynieria społeczna *(social engineering)*, polegająca na uzyskiwaniu poufnych informacji poprzez interakcje z ludźmi oraz *phising* (*password harvesting fishing)*, czyli uzyskiwanie poufnych danych poprzez podszywanie się pod podmioty i instytucje znane i zaufane.

84 Zob. w tym przedmiocie: R. Wieruszewski, M. Wyrzykowski, A. Bodnar, A. Gliszczyńska-Grabias, *Mowa nienawiści*..., S. Kowalski, M. Tulli, *Zamiast procesu. Raport o mowie nienawiści*, Warszawa 2003, s. 21 i n.

niekoniecznie z natury są dobrzy, gdyż znaczący odsetek wśród nich stanowią jednostki powodowane chęcią odwetu na społeczeństwie lub na jego wybranych przedstawicielach za poniesione porażki, niepowodzenia i klęski.

Bibliografia

Aleksandrowicz T., *Współczesny terroryzm międzynarodowy – próba definicji ze stanowiska prawa międzynarodowego*, „Wojskowy Przegląd Prawniczy" 2003, nr 2.

Andreski S., *Maksa Webera olśnienia i pomyłki*, Warszawa 1992.

Barman Z., *Globalizacja*, Warszawa 2000.

Becker J. (red.), *The Soviet Union and Terrorism*, London 1984.

Bell D., *The Coming of Post-Industial Society*, New York 1973.

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2.

Bickerton P., Bickerton M., Pardesi U., *Marketing w internecie*, Gdańsk 2006.

Bieńkowska E., Mazowiecka L. (red.), *Dyrektywa Parlamentu Europejskiego i Rady ustanawiająca normy minimalne w zakresie praw wsparcia i ochrony ofiar przestępstw. Komentarz*, Warszawa 2014.

Boszczyk M., *Media elektroniczne jako środek komunikowania politycznego* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym*, Sosnowiec 2006.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Brink D.O., *Millian Principles, Freedom of Speech, and Hate Speech*, „Legal Theory" 2001, no. 7.

Clark I., *Globalization and International Relation Theory*, Oxford 1999.

Cline R.S., *Yonah Alexander: The Soviet Connection*, New York 1984.

Cohen-Almagor R., *Holocaust Denial is a Form of Hate Speech*, „The Amsterdam Law Forum" 2009, no. 2.

Cortese A., *Opposing hate speech*, Westport 2006.

Doktorowicz K., *Europejska droga do społeczeństwa informacyjnego* [w:] K. Doktorowicz (red.), *Społeczeństwo informacyjne. Wyzwania dla gospodarki, polityki i kultury*, Katowice 2002.

Doktorowicz K., *Europejski model społeczeństwa informacyjnego*, Katowice 2005.

Fleming M., *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy" 1996, nr 1.

Ghanea N., *Expression and Hate Speech in the ICCPR: Compatible or Clashing?*, „Religion and Human Rights" 2010, no. 5.

Gilarka K., *Państwo narodowe a globalizacja – dynamika powstawania nowego ładu*, Toruń 2003.

Gliszczyńska-Grabias A., *Międzynarodowoprawne standardy wolności a mowa nienawiści* [w:] D. Bychawska-Sinarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013.

Goban-Klas T., *Społeczeństwo informacyjne i jego teoretycy* [w:] J. Lubacz (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1990.

Gołda-Sobczak M., *Spór o definicję terroryzmu*, „Wiedza i Umiejętności" 2004.

Grewlich K.W., *„Cyberspace". Sector – specyfic. Regulatio and Competition Rules in European Telecommunications*, „Common Market Law Review" 1999, nr 6.

Gruchoła M., *Ochrona użytkowników Internetu w państwach Unii Europejskiej*, Lublin 2012.

Grzybczyk K., *Twórczość internautów w świetle regulacji prawa autorskiego na przykładzie fanfiction*, Warszawa 2015.

Gulda P., *Elektroniczna demokracja – teoria i praktyka, wady i/lub zalety* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005.

Gulda P., *Internet jako przestrzeń polityczna* [w:] M. Sokołowski (red.), *Edukacja medialna. Nowa generacja pytań i obszarów badawczych*, Olsztyn 2004.
Hanusek T., *W sprawie pojęcia współczesnego terroryzmu*, „Problemy Kryminalistyczne" 1980, nr 143.
Hare I., Weinstein J. (red.), *Extreme Speech and Democracy*, Oxford 2009.
Hoeren T., *Werberecht im Internet am Beispiel der ICC Guidelines on Interactive Marketing Communications* [w:] M. Lehmann (red.), *Internet – und Multimediarecht (Cyberlaw)*, Stuttgart 1997.
Hoffman B., *Low-intensity Conflict: Terrorism and Guerrilla War fare in the Coming Decades* [w:] L. Howard (red.), *Terrorism: Roots, Ompact, Responses, Praegor*, New York 1992.
Hoffman B., *Oblicza terroryzmu*, Warszawa 2001.
Indecki K., *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998.
Jaskuła L.K., *Wolność działalności dziennikarskiej w perspektywie zjawiska mowy nienawiści. Wybrane aspekty prawne* [w:] W. Lis (red.), *Status prawny dziennikarza*, Warszawa 2014.
Kasińska-Metryka, *Demokratyzacja systemu politycznego a przepływ informacji – od deficytu do przesytu* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005.
Kerr C., Dunlap J.T., Harbison F.H., Myers C.A., *Industrialism and Industirial Man*, Cambridge 1960.
King M., *Globalization, Knowledge and Society*, New York 1990.
Korcz I., *Internet a człowiek w kontekście globalizującego się świata?* [w:] M. Sokołowski, M. Furmanek (red.) *Oblicza Internetu. Internet a globalne społeczeństwo informacyjne*, Elbląg 2005.
Korzińska A., *Tradycja i nowoczesność. Islam w Internecie. Analiza polskojęzycznych stron internetowych* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006.
Kosiński J., *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak, (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013.
Kotarski H., *Internet a lokalna polityka. Studium socjologiczne na przykładzie wyborów samorządowych* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006.
Kowalski S., Tulli M., *Zamiast procesu. Raport o mowie nienawiści*, Warszawa 2003.
Lach A., *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015.
Laqueur W., *Terrorism*, London 1997.
Laqueur W., *The Age of Terrorism*, Boston 1987.
Łęski Z., Wieczorek Z., *Społeczeństwo wirtualne – czy mamy jakiś wybór?* [w:] M. Sokołowski, M. Furmanek (red.), *Oblicza Internetu. Internet a globalne społeczeństwo informacyjne*, Elbląg 2005.
Łętowska E., *Zwodnicze pokusy karania hate speech* [w:] D. Bychawska-Siniarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013.
Marschall A.M., Tompset B.C., *Identity theft in an online world*, „Computer Law and Security Report" 2005, nr 21.
Mason S., *Validating identity for the electronic environment*, „Computer Law and Security Report" 2004, nr 3.
Matusiak I., *Gra komputerowa jako przedmiot prawa autorskiego*, Warszawa 2013.
Muszyński W., *Wizerunek polskich tradycjonalistów Internecie* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006.
Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, nr 3.
Pala M., *Wybrane aspekty bezpieczeństwa w cyberprzestrzeni*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, nr 1.
Pawłowski A., *Terroryzm w Europie w XIX i XX wieku*, Zielona Góra 1980.

Pietras M., *Globalizacja jako proces zmian społeczności międzynarodowej* [w:] M. Pietras (red.), *Oblicza procesów globalizacji*, Lublin 2002.
Pikulski S., *Prawne środki zwalczania terroryzmu*, Olsztyn 2000.
Preis E., *Glosa do wyroku Trybunału Sprawiedliwości z dnia 29 stycznia 2008, C – 275/06*, „Europejski Przegląd Sądowy" 2009, nr 4.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Rinaldi A.H. *Internationale Netze und das Wettberbstrecht* [w:] J. Becker (red.) *Rechtsprobleme internationalen Dattenetze*, Baden-Baden 1996.
Sauer A., *Online privacy and the online self*, „Privacy Law Bulletin" 2008, nr 9.
Schittek G., *Internet jako narzędzie politycznego wsparcia w Szwecji* [w:] T. Zasępa (red.), *Internet. Fenomen społeczeństwa informacyjnego*, Częstochowa 2001.
Schmid A.P., *Political Terrorism: A Research Guide*, New Brunswick 1984.
Scholte J.A., *The Globalization of World Politics* [w:] J. Baylis, S. Smith (red.), *The Globalization of World Politics. An Introduction to International Relations*, New York 2001.
Serwiak S., *Cyberprzestrzeń jako źródło zagrożenia terroryzmem* [w:] E. Pływaczewski (red.), *Przestępczość zorganizowana, świadek koronny i terroryzm w ujęciu praktycznym*, Kraków 2005.
Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielniecki, K. Rajchel (red.), *Cyberterroryzm – nowe wyznawania XXI wieku*, Warszawa 2009.
Sobczak J., *Dylematy społeczeństwa informacyjnego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, Elbląg 2006.
Sobczak J., *Europejski ład komunikacyjny w procesie globalizacji* [w:] J. Sobczak, R. Bäcker, *Europejska myśl polityczna wobec globalizacji*, Łódź 2005.
Sobczak J., Kakareko K., *Odpowiedzialność za przestępstwa popełnione w sieci, a kwestia prywatności* [w:] J. Sobczak, K. Chałubińska-Jentkiewicz, K. Kakareko, *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017.
Sobczak J., *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007.
Sobczak J., *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek, *Demokracja w dobie globalizacji*, t. II, *Aspekty teoretyczne*, Katowice 2008.
Sobczak J., *Wolność słowa a zjawisko inwigilacji przekazu internetowego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Architektura komunikacyjna sieci*, Elbląg 2007.
Sobczyk S., *Internet narzędziem oddziaływania na wyborców* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006.
Stammers N., *Social movements and the challenge to power* [w:] M. Shaw (red.), *Politics in Globalized Word*, London 1999.
Śledzińska-Simon A., *Decyzja ramowa w sprawie zwalczania pewnych form przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii Europejskiej* [w:] R. Wieruszewski, M. Wyszykowski, A. Bodnar, A. Gliszczyńska-Grabias (red.), *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010.
Turska A., *Marketing polityczny w Internecie* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego. Studia i Analizy" 2013, nr 9.
Weber M., *Gospodarka i społeczeństwo. Zarys socjologii rozumiejącej*, Warszawa 2002.
Wieruszewski R., Wyrzykowski M., Bodnar A., Gliszczyńska-Grabias A., *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010.
Woiński M., *Prawnokarne aspekty zwalczania mowy nienawiści*, Warszawa 2014.
Wójcik J.W., *Przeciwdziałania finansowaniu terroryzmu*, Warszawa 2007.

Zacher L.W., *Etykietowanie przyszłych społeczeństw – kryteria, określenia, ewaluacje* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005.
Zasępa T., *Komunikacja cybernetyczna wyzwaniem dla Kościoła katolickiego* [w:] T. Zasępa (red.), *Internet i nowe technologie – ku społeczeństwu przyszłości*, Częstochowa 2003.

Cybercrime between Polish and international regulations

Abstract

The article presents the problem of cybercrime, regulated by national and international regulations. In the era of information society where the internet plays an important role and where the number of its users is constantly growing, the law is often infringed which often leads to crimes. Crimes in cyberspace, understood as a communication area created by the system of internet connections, are getting more and more serious and more and more difficult to detect and investigate. National regulations, as well as international ones, not always keep up with the dynamic technological progress, network development and many challenges it poses. New offences, that appear in the cyberspace and that are more or less contrary to the applicable law, are still committed which exposes the weaknesses of the adopted regulations.

Key words: crime, cyberspace, information society, national law, international law, threat, cyberterrorism, cyberattack, security system