Jędrzej SKRZYPCZAK
Uniwersytet im. Adama Mickiewicza, Poznań

BEZPIECZEŃSTWO TELEINFORMATYCZNE W ŚWIETLE EUROPEJSKIEJ KONWENCJI O CYBERPRZESTĘPCZOŚCI

Powodem podjęcia prac nad Konwencją Rady Europy o cyberprzestępczości było przekonanie o potrzebie prowadzenia wspólnej polityki kryminalnej w obszarze sieci teleinformatycznych. Wynikało to z obawy o zapewnienie bezpieczeństwa obywateli w obszarze internetu. Nowa płaszczyzna aktywności ludzkiej przyniosła bowiem wiele pozytywnych zjawisk, ale niestety także szereg negatywnych. Stąd pojawiła się potrzeba ochrony społeczeństwa przed tego rodzaju przestępczością[1]. Zauważono bowiem, że sieci informatyczne i informacje elektroniczne mogą być wykorzystywane w celu popełniania przestępstw. Nowe warunki i środowisko stworzyły możliwości dokonywania czynów zabronionych zasługujących na penalizację. Dostrzeżono, że cyberprzestępczość[2] godzi w takie dobra chronione jak poufności, integralność i dostępność systemów i danych informatycznych. W rezultacie działania zabronione mogą okazać się groźnie zarówno dla poszczególnych osób fizycznych, ale także dla całej infrastruktury publicznej[3]. Wskazuje się na zagrożenie takich sektorów jak bankowość, ruch lotniczy, telefonia, systemy dostaw energii elektrycznej, ochrona zdrowia, usługi edukacyjne[4].

Dodatkowo należy podkreślić, że internet postawił krajowe systemy prawne w wyjątkowo trudnej sytuacji. Ze swej natury zakłada globalny zasięg[5]. Natomiast krajowe

---

[1] J. E. Mehan, *Cyberwar, Cyberterror, Cybercrime*, Cambs 2008, s. 109–112.

[2] W kwestii definicji pojęcia cyberprzestępczość patrz szerzej M. Yar, *Cybercrime and Society*, London 2006, s. 9–11.

[3] Warto zauważyć, że diagnozując potencjalne niebezpieczeństwa w erze po zimnowojennej wskazywano bardziej na zagrożenie interesów jednostek niż państw. Por Raport ONZ *New Dimension of Human Security. Human Development Report 1994*, tekst dostępny na stronie http://hdr.undp.org/en/media/hdr_1994_en_overview.pdf. Zob. także J. Shannon, N. Thomas, *Human Security and Cyber-Security. Operationalising a Policy Framework*, w: *Cyber-crime. The Challenge in Asia*, ed. R. Broadhurst, P. Grabosky, Hongkong 2005, s. 327–328. Przykładów jest wiele. Przywołać należy kazus wirusa komputerowego „Stuxnet", który zaatakował irański program, atomowy („Gazeta Wyborcza" z 17 stycznia 2011). Jak podały media w dniu 26 stycznia 2011 r. dokonano cyberataku na rejestry emisji CO_2 takich krajów jak Austria, Grecja, Czechy, Polska, Estonia. W konsekwencji uniemożliwiono przez ponad tydzień handel emisjami dwutlenku węgla w Unii Europejskiej (patrz „Gazeta Wyborcza" z 20.01.2011).

[4] P. Grabosky, *The Global Cyber-Crime Problem. The Socio-Economic Impact*, w: *Cyber-crime...*, op. cit., s. 30–31.

[5] D. Thomas, B. D. Loaden, *Cybercrime: Law enforcement, security and surveillance in the information age*, London 2000, s. 3.

porządki prawne ograniczają swą jurysdykcję, jedynie do granic państw. Stąd też należało stworzyć narzędzia międzynarodowe do walki z tymi groźnymi zjawiskami[6]. Konieczne stało się zatem przyjęcie właściwych przepisów prawnych na płaszczyźnie europejskiej i wspieranie międzynarodowej współpracy.

Z drugiej jednak strony podkreślono konieczność zachowania balansu między instrumentami chroniącymi przed cyberprzestępczością, a ochroną podstawowych praw człowieka. W szczególności wyrażono przekonanie, że należy chronić wartości i dobra strzeżone na mocy *Konwencji Rady Europy z 1950 roku o ochronie praw człowieka i podstawowych wolności*[7] oraz *Międzynarodowym Paktem Narodów Zjednoczonych z 1966 roku o prawach obywatelskich i politycznych*[8]. W szczególności chodzi o prawo każdej jednostki do posiadania własnych wolnych opinii, jak również prawo do wolności wypowiedzi, łącznie z wolnością poszukiwania, uzyskiwania i dzielenia się wszelkiego rodzaju informacjami i ideami, bez względu na granice oraz prawo do poszanowania prywatności.

Konwencja o cyberprzestępczości wpisuje się w zbiór dokumentów przyjmowanych przez Radę Europy, jak i inne organizacje międzynarodowe. I tak wymienić trzeba w tym katalogu *Konwencję Rady Europy z 1981 roku o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*[9] oraz *Konwencję dotyczącą współpracy w dziedzinie spraw karnych*[10]. Warto także przypomnieć przyjęte w ramach tej organizacji europejskiej:

– zalecenie nr R(85)10 dotyczące praktycznego stosowania Europejskiej konwencji o pomocy prawnej w sprawach karnych w odniesieniu do wniosków rekwizycyjnych dotyczących podsłuchu rozmów telefonicznych[11];
– zalecenie nr R(88)2 w sprawie piractwa w dziedzinie prawa autorskiego i praw pokrewnych[12];

---

[6] J. Shannon, N. Thomas, *Human Security and Cyber – Security. Operationalising a Policy Framework*, w: *The Global Cyber-Crime Problem...*, op. cit., s. 327–328.

[7] *Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r.*, (Dz. U. 1993, Nr 61, poz. 264, z późn. zm.).

[8] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku 19 grudnia 1966 r. (Dz. U. 1977, Nr 38, poz. 167).

[9] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28 I 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[10] *European Convention on Mutual Assistance in Criminal Matters*, Strasbourg, 20 IV 1959, tekst dostępny http://conventions.coe.int/Treaty/en/Treaties/Html/030.htm.

[11] Recommendation No. R (85) 10 of the Committee of Ministers to Member States Concerning the Practical Application of the European Convention on Mutual Assistance in Criminal Maters in Respect of Letters Rogatory for the Interception of Telecommunications (Adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers' Deputies), tekst dostępny na stronie https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=605287&SecMode=1&DocId=686878&Usage=2.

[12] Recommendation No. R (88) 2 of the Committee of Ministers to Member States on Measure to Combat Piracy in the Field of Copyright and Neighbouring Rights (Adopted by the Committee of Ministers on 18 January 1988 at the 414th meeting of the Ministers' Deputies), tekst dostępny na stronie https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=608749&SecMode=1&DocId=695620&Usage=2.

– zalecenie nr R(87)15 dotyczące wykorzystywania danych osobowych w sektorze policji[13];
– zalecenie nr R(95)4 o ochronie danych osobowych w sferze usług telekomunikacyjnych ze szczególnym uwzględnieniem usług telefonicznych[14];
– zalecenie nr R(89)9 w sprawie przestępstw komputerowych, które zawiera wytyczne dla legislacji krajowych dotyczące definicji pewnych przestępstw komputerowych[15];
– zalecenie nr R(95)13 w sprawie problemów prawa karnego procesowego związanych z technologią informatyczną[16].

Genezy Europejskiej Konwencji o cyberprzestępczości należy doszukiwać się jednak w decyzji podjętej w 1996 r. o powołaniu Europejskiego Komitetu do spraw Przestępczości. Zespół ten postulował wówczas utworzenie komitetu ekspertów do spraw cyberprzestępczości. Podobne konkluzje wynikały także z przyjętego wówczas raportu H. W. K. Kaspersena, podkreślającego nadto konieczność przyjęcia międzynarodowego dokumentu[17]. W konsekwencji Komitet Ministrów Rady Ministrów w dniu 4 lutego 1997 r. powołał Komitet Ekspertów do spraw Przestępczości w Cyberprzestrzeni (Committee of Experts on Crime in Cyber-space – PC-CY). Ponadto przypomnieć należy rezolucję nr 1 przyjętą na XXI Konferencji Europejskich Ministrów Sprawiedliwości odbywającej się Pradze w dniach 10–11 czerwca 1997 roku. Dokument ten zalecił Komitetowi Ministrów wspieranie prac prowadzonych przez Europejski Komitet ds. Przestępczości (CDPC) w zakresie cyberprzestępczości, w celu wzajemnego zbliżenia postanowień w zakresie prawa karnego oraz umożliwienia stosowania efektywnych środków ścigania takich przestępstw. Z kolei w rezolucji nr 3 przyjętej na XXIII Konferencji tego gremium w Londynie, w dniach 8–9 czerwca 2000 r., podkreślono potrzebę stworzenia efektywnego systemu współpracy międzynarodowej w zakresie walki z cyberprzestępczością. Projekt konwencji o cyberprzstępczości został

---

[13] Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies), teskt dostępny na stronie https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276604&SecMode=1&DocId=694350&Usage=2.

[14] Recommendation No. R (95) 4 of the Committee of Ministers to Member States on the Protection of Personal Data in the Area of Telecommunication Services with Particular Reference to Telephone Services (Adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the Ministers' Deputies), tekst na stronie https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=535549&SecMode=1&DocId=518682&Usage=2.

[15] Recommendation No. R (85) 10 of the Committee of Ministers to Member States on Computer – Related Crime (Adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies), tekst dostępny na stronie: https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2.

[16] Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies), tekst dostępny na stronie https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2.

[17] R. Targalski, *Konwencja o cyberprzestępczości*, w: *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 208.

przygotowany w 2000 r. i zaopiniowany pozytywnie przez Zgromadzenie Parlamentarne Rady Europy. Wzbudził on jednak spore protesty społeczności internetowej, która zarzucała, że pominięto opinie użytkowników sieci w trakcie prac nad dokumentem. Po kolejnych poprawkach został jednak zaakceptowany przez komitet PC-CY i w dniu 23 listopada 2001 r. w Budapeszcie podczas 109 sesji Komitetu Ministrów Rady Europy konwencja została otwarta do podpisu[18]. Jej sygnatariuszami zostały niemal wszyscy członkowie Rady Europy za wyjątkiem Andory, Monaco, San Marino, Turcji i Federacji Rosyjskiej. Wszedł w życie 1 lipca 2004 r., po dokonaniu ratyfikacji przez 5 krajów. Podkreślenia wymaga okoliczność, iż podpis pod tym dokumentem złożyli przedstawiciele państw partnerskich, a mianowicie Kanady, Japonii, Republiki Południowej Afryki oraz USA. Przy czym tylko Stany Zjednoczone dokonały aktu ratyfikacji tego dokumentu. Według stanu na 13 lutego 2011 r. spośród państw członkowskich Rady Europy ratyfikacji dokonało 30 państw[19]. W tym gronie nie ma niestety Polski.

Z kolei w styczniu 2003 r. otwarto do podpisu *Protokół Dodatkowy do konwencji o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim, ksenofobicznym popełnionych przy użyciu systemów komputerowych*. Po dokonaniu ratyfikacji tego dokumentu przez 5 państw, wszedł w życie 1 marca 2006 r.[20]

Konwencja ta jest w istocie multilateralną umową międzynarodową o charakterze bezterminowym. Składa się z preambuły i czterech rozdziałów. W rozdziale pierwszym zdefiniowano szereg istotnych z punktu widzenia tego dokumentu pojęć. Rozdział II zawiera propozycje środków, jakie należy podjąć na szczeblu krajowym. Wyróżniono tu trzy części. Pierwsza dotyczy prawa karnego materialnego, druga prawa procesowego a trzecia jurysdykcji. Rozdział kolejny poświęcony jest współpracy międzynarodowej, a ostatni zawiera postanowienia końcowe.

Konwencja zdefiniowała szereg istotnych terminów z punktu widzenia poruszanej problematyki. I tak w rozumieniu tego aktu pod pojęciem „system informatyczny" należy rozumieć każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych. Z kolei „dane informatyczne" to dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny. „Dostawca usług" to z kolei zarówno dowolny podmiot prywatny lub publiczny, który umożliwia użytkownikom jego usług komunikowanie się za pomocą systemu informatycznego, jak również dowolny inny podmiot, który przetwarza lub przechowuje dane informatyczne w imieniu takich usług komunikacyjnych lub użytkowników takich usług. Pojęcie „dane dotyczące ruchu" definiuje się tu

---

[18] O procesie przygotowywania tego dokumentu patrz szerzej ibidem, s. 209–210 oraz P. Csonka, *The Council of Europe Convention on Cyber-Crime. A Response to the Challenge of the New Age*, w: *Cyber-crime*..., op. cit., s. 303–304.

[19] Ratyfikacji dokonały następujące państwa: Albania, Armenia, Azerbejdżan, Bośnia i Hercegowina, Bułgaria, Chorwacja, Cypr, Dania, Estonia, Finlandia, Francja, RFN, Węgry, Islandia, Włochy, Łotwa, Litwa, Mołdowa, Czarnogóra, Holandia, Norwegia, Portugalia, Rumunia, Serbia, Słowacja, Słowenia, Hiszpania, Macedonia, Ukraina. Zobacz lista państw na stronie http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=13/02/2011&CL=ENG.

[20] R. Tarnogórski, op. cit., s. 213.

jako dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazujące swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę, rozmiar, czas trwania lub rodzaj danej usługi.

Dokument proponuje szereg typów przestępstw, które państwa strony powinny wprowadzić do krajowego ustawodawstwa. Pierwsza grupa przestępstw dotyczy przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów. I tak w tej grupie zobowiązano strony do wprowadzenia do krajowych porządków prawnych przestępstwa polegającego na umyślnym, bezprawnym dostępie do całości lub części systemu informatycznego. Wskazano nadto, że możliwe jest określenie, że przestępstwo musi zostać popełnione poprzez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym. Innym proponowanym czynem zabronionym jest działania polegające na przechwytywaniu za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Zezwolono, aby wprowadzić wymóg, że przestępstwo musi zostać popełnione umyślnie z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym[21].

Kolejną propozycją jest wprowadzenie typu czynu zabronionego polegającego na umyślnym, bezprawnym niszczeniu, wykasowywaniu, uszkadzaniu, dokonywaniu zmian lub usuwaniu danych informatycznych. Dopuszczono w tym przypadku złożenie zastrzeżenia, że każda ze stron może wprowadzić wymóg, aby takie zachowanie skutkowało poważną szkodą.

Innym proponowanym do wprowadzenia do porządków krajowych czynem przestępczym jest zachowanie polegające na umyślnym, bezprawnym istotnym zakłócaniu funkcjonowania systemu informatycznego. Czynnościami sprawczymi mogą być takie działania jak wprowadzanie, transmisja, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych.

Innym przestępstwem proponowanym w świetle tego dokumentu, winno być uznanie za czyn zabroniony postępowania polegającego na produkcji, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania urządzenia, programu komputerowego, hasła komputerowego, kodu dostępu lub podobnych danych, przeznaczonych dla celów popełnienia któregokolwiek z przestępstw opisanych w konwencji. To samo dotyczy faktu posiadania powyższych rzeczy. Zezwolono jednocześnie, aby prawo krajowe wprowadzało wymóg, że odpowiedzialność karna dotyczyć będzie takiej działalności w większej skali.

Kolejna grupa proponowanych typów czynów karnych dotyczy przestępstw komputerowych. W tym katalogu wymieniono fałszerstwo komputerowe[22], polegające na

---

[21] S. W. Brenner, *The Council of Europe`s Convention on Cybercrime*, w: *Cybercrime. Digital Cops and Laws in a Networked Environment*, eds J. M. Backin, J. Grimmelmann, N. Kozlovski, S. Wagman, T. Zarsky, New York–London 2007, s. 210–214.

[22] Tak art. 7 konwencji.

dokonywaniu zmian, wykasowywaniu lub usuwaniu danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne. Możliwe jest wprowadzenie zastrzeżenia, że odpowiedzialność karna dotyczyć będzie tylko działania podjętego w zamiarze oszustwa. Z kolei w art. 8 stypizowano przestępstwo oszustwa komputerowego. Działanie takie – wedle tej propozycji – polega na działaniu polegającym na spowodowaniu utraty majątku przez inną osobę poprzez wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych, jak również każdą ingerencję w funkcjonowanie systemu komputerowego, z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.

Kolejna grupa przestępstw wymienionych w Konwencji dotyczy czynów zabronionych ze względu na charakter zawartych informacji. W tej grupie wskazano przestępstwa związane z pornografią dziecięcą. Za takie będą traktowane zachowania polegające na produkowaniu, rozpowszechnianiu lub transmitowaniu, oferowaniu lub udostępnianiu pornografii dziecięcej za pomocą systemu informatycznego. To samo odnosi się do czynu polegającego na pozyskiwaniu pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby oraz posiadaniu pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych. Jednocześnie zdefiniowano, że pod pojęciem „pornografia dziecięca" należy rozumieć materiał pornograficzny, który w sposób widoczny przedstawia osobę małoletnią w trakcie czynności wyraźnie seksualnej, osobę, która wydaje się być nieletnią, w trakcie czynności wyraźnie seksualnej, realistyczny obraz przedstawiający osobę małoletnią w trakcie czynności wyraźnie seksualnej. Wyjaśniono także, że za „osobę małoletnią" w rozumieniu konwencji traktowana będzie każda osoba poniżej 18 roku życia, choć możliwe jest obniżenie przez każdą ze stron tego limitu wieku do 16 lat.

Ostania grupa przestępstw odnosi się do naruszeń praw autorskich i praw pokrewnych. Zgodnie z art. 10 należy podjąć takie środki prawne niezbędne dla uznania za przestępstwa naruszeń prawa autorskiego zdefiniowanego w prawie danej Strony zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z *Aktu Paryskiego Konwencji Berneńskiej o ochronie dzieł literackich i artystycznych*[23], *Porozumienia w spra-*

[23] Warto odnotować, że *Konwencja berneńska z 9 września 1886 r. o ochronie dział literackich i artystycznych* była wielokrotnie rewidowana: w 1896 r. w Paryżu, w 1908 r. w Berlinie, w 1914 r. w Bernie, w 1928 r. w Rzymie, w 1948 r. w Brukseli, w 1967 r. w Sztokholmie oraz 24 lipca 1971 r. w Paryżu, a następnie poprawiona 2 października 1979 r. Polska obecnie związana jest redakcją paryską tej konwencji opublikowaną w: Dz. U. 1990, Nr 82, poz. 474. Zob. też J. Sobczak, *Prawo środków masowej informacji. Prasa, radio, telewizja*, Toruń 1999, s. 267–301. Zob. J. Błeszyński, *Ostatnie redakcje Konwencji berneńskiej o ochronie dzieł literackich i artystycznych a prawo wewnętrzne*, „ZNUJ PzWiOWI" 1977, z. 13, s. 9–14; A. Matlak, *Międzynarodowy charakter ochrony utworów i przedmiotów praw pokrewnych*, w: *Prawo mediów*, op. cit., s. 506; J. Błeszyński, *Prawo autorskie*, Warszawa 1985, s. 9, a także idem, *Ostatnie redakcje*..., op. cit., s. 10; S. Ritterman, *Prawa artystów wykonawców a interesy użytkowników i autorów*, „Studia Cywilistyczne" 1968, t. XII, s. 99–135; J. R. Pardo, *Copyright and Multimedia*, The Hague–London–New York 2003, s. 55–63.

wie handlowych aspektów praw własności intelektualnej (TRIPS)[24] oraz *Traktatu Światowej Organizacji Własności Intelektualnej (WIPO) o prawach autorskich* przyjętego przez Konferencję Dyplomatyczną dnia 20 grudnia 1996 r.[25]*,* jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego. Nie obejmuje to jednak naruszeń autorskich praw osobistych, a jedynie majątkowych. Podobne środki należy zapewnić w celu ochrony praw pokrewnych zdefiniowanych w prawie danej Strony, zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Międzynarodowej konwencji o ochronie wykonawców, producentów fonogramów i organizacji nadawczych zawartej w Rzymie[26], TRIPS[27] oraz Traktatu Światowej Organizacji Własności Intelektualnej (WIPO) o artystycznych wykonaniach i fonogramach[28], z wyłączeniem praw osobistych przewidzianych przez te konwencje. Dopuszczono jednak, aby w tych przypadkach możliwe było zapewnienie ochrony innymi środkami niż prawnokarnymi. Muszą one być jednak skuteczne i zgodne ze zobowiązaniami międzynarodowymi. Zobowiązano sygnatariuszy tej konwencji do zastosowania odpowiednich sankcji, w tym również kary pozbawienia wolności lub grzywny.

Jak już wyżej wskazano Konwencja przewidziała również odrębne rozwiązania w zakresie procedury. I tak zobowiązania państw dotyczą zasad zbierania dowodów w formie elektronicznej, warunków zabezpieczenia przechowywanych danych informatycznych, ujawniania danych, nakazów dostarczania danych i informacji, przeszukania i zajęcia przechowywanych danych informatycznych.

Z kolei wspomniany protokół dodatkowy został przyjęty w celu penalizacji aktów o charakterze rasistowskim i ksenofobicznym popełnionych przy użyciu systemów komputerowych. Warto przypomnieć, że dokument zdefiniował pojęcie materiału rasistowskiego i ksenofobicznego, jako każdy materiał pisemny, każdy wizerunek lub każde inne wyrażenie myśli lub teorii, które nawołują, popierają lub podżegają do nienawiści,

---

[24] *Porozumienie ustanawiające Światową Organizację Handlu (WTO) sporządzone w Marakeszu dnia 15 kwietnia* (Dz. U. 1995, Nr 98, poz. 483); *Oświadczenie rządowe z 31 lipca 1995 r. w sprawie ratyfikacji przez Rzeczpospolitą Polską Porozumienia ustanawiającego Światową Organizację Handlu (WTO)*, opublik. w Dz. U. Nr 98, poz. 484; *Porozumienie w sprawie handlowych aspektów praw własności intelektualnej* stanowiące Załącznik 1C do tego Porozumienia opublik. w Dz. U. 1996, Nr 32, poz. 143 (ang. *Trade Related Aspects of Intellectual Property Rights – skrótowo TRIPS).* Patrz szerzej P. E. Geller, *Własność intelektualna na rynku światowym*, „ZNUJ PzWiOWI" 1997, z. 68, s. 9–19.

[25] *WIPO Copyright Treaty* – dalej skrótowo jako WCT. Tekst opublikowany w j. polskim w: A. Matlak*, Prawo autorskie w społeczeństwie informacyjnym*, Kraków 2004, s. 207–219.

[26] *Międzynarodowa konwencja o ochronie wykonawców, producentów fonogramów oraz organizacji nadawczych sporządzona w Rzymie dnia 26 października 1961 r* (Dz. U. 1997, Nr 125, poz. 800). Zob. także *Oświadczenia Rządowe z dnia 6 czerwca 1997 r. w sprawie przystąpienia Rzeczypospolitej Polskiej do Międzynarodowej konwencji o ochronie wykonawców, producentów fonogramów oraz organizacji nadawczych, sporządzonej w Rzymie dnia 26 października 1961 r.* (Dz. U. Nr 125, poz. 801), tekst dostępny także w J. Sobczak, *Prawo środków masowej informacji*, op. cit., s. 302–313.

[27] Patrz wyżej.

[28] *WIPO Performance and Phonograms Treaty*, tłumaczenie tekstu w j. polskim w: A. Matlak, *Prawo autorskie*..., op. cit., s. 220–237. Patrz także N. Lucchi, *Digital Media @ Intellectual Property. Management of Rights and Consumer Protection in a Comparative Analysis*, Berlin–Heidelberg–New York 2006, s. 42–43.

dyskryminacji, przemocy przeciw jakiejkolwiek osobie lub grupie osób, ze względu na rasę, kolor, pochodzenie narodowe lub etniczne, jak również religię, jeżeli wykorzystywana jest ona jako pretekst dla któregokolwiek z tych czynników. Stąd też zaproponowano szereg typów przestępstw w tym obszarze. Za takie należy uznać rozpowszechnianie materiałów rasistowskich i ksenofobicznych w systemie komputerowym, grożenie przy użyciu systemu komputerowego popełnieniem poważnego przestępstwa na tym tle, publicznej zniewagi powodowanej rasizmem i ksenofobią, a także zaprzeczania lub poważnego umniejszania znaczenia, usprawiedliwiania zbrodni ludobójstwa oraz zbrodni przeciwko ludzkości.

Znaczenie *Europejskiej Konwencji o Cyberprzestępczości* trudne jest do przecenienia. Jest to jeden z pierwszych aktów prawa międzynarodowego, który stanowi odpowiedź na nowe, negatywne zjawiska wynikające z postępu technologicznego, ery cyfrowej i pojawienia się internetu. Jest to o tyle istotne, że zważywszy na globalny charakter sieci komputerowych, działania krajowe są często nieskuteczne.

STRESZCZENIE

Przedmiotem artykułu jest analiza najważniejszych postanowień Europejskiej Konwencji o cyberprzestępczości. W szczególności, jest to próba odpowiedzi na pytanie czy Konwencja zapewnia wystarczające środki architektury europejskiego systemu bezpieczeństwa teleinformatycznego.

TELEINFORMATICS SECURITY IN LIGHT OF THE CONVENTION ON CYBERCRIME

ABSTRACT

The subject of this paper is the analysis of the main regulation of the the European Convention on Cybercrime. In particular, it attempts to answer the question whether the Convention provides sufficient level of European IT security.