Ustawa o krajowym systemie cyberbezpieczeństwa[1]

z dnia 5 lipca 2018 r. (Dz.U. 2018, poz. 1560)[2]

Spis treści

Wprowadzenie

Spis treści

[1] Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194 z 19.07.2016, str. 1).

[2] Niniejszą ustawą zmienia się ustawy: ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

1 1. **Uwagi ogólne.** Nie ulega wątpliwości, że z uwagi na globalny charakter współczesnych sieci teleinformatycznych w zapewnieniu cyberbezpieczeństwa, w tym zwalczaniu cyberprzestępczości, pierwszorzędną rolę odgrywa współpraca międzynarodowa. W związku z tym prace nad stworzeniem prawnych ram współpracy państw w celu zapewnienia bezpieczeństwa danych komputerowych i systemów informatycznych toczyły się na forum międzynarodowym od momentu, kiedy sieci teleinformatyczne uzyskały charakter międzypaństwowy. Podkreślić należy, że jakiekolwiek inicjatywy mające na celu zapewnienie cyberbezpieczeństwa by były skuteczne, wymagają współpracy międzynarodowej nie tylko państw. Konieczne jest również zaangażowanie prywatnych podmiotów – przedstawicieli branży informatycznej, głównie dostawców usług internetowych.

2 2. **Regulacje międzynarodowe z zakresu cyberbezpieczeństwa oraz zwalczania cyberprzestępczości.** Poniżej przedstawione zostaną inicjatywy podjęte w ramach organizacji międzynarodowych dotyczące zapewnienia cyberbezpieczeństwa oraz walki z cyberprzestępczością. Rozważania rozpoczęte zostaną od inicjatyw OECD i Rady Europy. Wynika to nie tylko ze swego rodzaju „europocentryzmu", ale przede wszystkim z faktu, że właśnie te dwie organizacje jako pierwsze zajęły się problematyką cyberbezpieczeństwa i cyberprzestępczości. Ponadto Konwencja Nr 185 Rady Europy o cyberprzestępczości z 23.11.2001 r. (Dz.U. z 2015 r. poz. 728) – umowa międzynarodowa stworzona w ramach Rady Europy – jest kamieniem milowym w dziedzinie zwalczania przestępstw komputerowych, jednocześnie pozostając jedynym wiążącym aktem prawa międzynarodowego służącym walce z nimi. O jej znaczeniu najlepiej świadczy stale wzrastająca liczba jej sygnatariuszy (a także państw, które bez podpisywania jej wzorują się na jej postanowieniach, np. Pakistan) oraz fakt, że organizacje międzynarodowe albo zalecają swoim członkom jej przyjęcie (ONZ, Grupa G7/G8, Unia Europejska), albo „kopiują" jej postanowienia, tworząc własne ustawy modelowe (np. Wspólnota Narodów – ang. *Commonwealth of Nations*).

3 3. **Organizacja Współpracy Gospodarczej i Rozwoju (OECD).** Pierwszym, powstałym w ramach Organizacji Współpracy Gospodarczej i Rozwoju (ang. *Organisation for Economic Co-operation and Development*, OECD, fr. *Organisation de coopération et de développement economiques*, OCDE), dokumentem z zakresu cyberprzestępczości było przyjęte 26.11.1992 r. przez Radę OECD zalecenie C(92)188 dotyczące wytycznych w zakresie bezpieczeństwa systemów informatycznych [*Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 (C(92)188/FINAL)*]. W 2000 r. po dokonaniu jego rewizji uznano, że istnieje konieczność stworzenia zupełnie nowych wytycznych (*M. Gercke*, Understanding Cybercrime, s. 220). Prace nad nimi nabrały tempa po zamachu 11.9.2001 r. Ich efektem było zalecenie Rady C(2002)131 z 25.7.2002 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)*], które zastąpiło zalecenie C(92)188. Przez blisko trzynaście lat był to najważniejszy akt OECD zwią-

zany z szeroko pojętym bezpieczeństwem sieci komputerowych. W zaleceniu tym wskazano na rosnące znaczenie systemów i sieci informatycznych, rosnącą zależność od nich gospodarek narodowych, handlu międzynarodowego, życia społecznego, kulturalnego i politycznego, wymagających szczególnych wysiłków zmierzających do ochrony i wspomagania pokładanego w nich zaufania. Jednocześnie – jak stwierdzono w omawianym zaleceniu – systemom, sieciom informatycznym oraz danym w nich procedowanym zagrażają nowe i nasilające się zagrożenia (różnego rodzaju akty nieupoważnionego dostępu, użycia lub modyfikacji danych, przesyłanie szkodliwych programów, zmasowane – dotykające znacznej liczby komputerów i paraliżujące sieci teleinformatyczne – ataki typu *denial of service*). W konsekwencji w zaleceniu C(2002)131 rządom państw członkowskich zarekomendowano przede wszystkim stworzenie nowych lub poprawienie obecnych polityk, praktyk, środków i procedur w oparciu o załączone do niego wytyczne, jednocześnie propagując opisaną w nich kulturę bezpieczeństwa wśród wszystkich zainteresowanych stron (pod tym pojęciem rozumie się wszystkie podmioty, które rozwijają, posiadają, obsługują i użytkują systemy i sieci informatyczne oraz świadczą usługi z nimi związane, tj. rządy państw, przedsiębiorstwa, inne organizacje oraz indywidualnych użytkowników). W związku z postępem technologicznym rozpoczęto w 2012 r. prace nad rewizją wytycznych. Ich efektem jest zalecenie Rady C(2015)115 z 17.9.2015 r. o zarządzaniu ryzykiem w obszarze bezpieczeństwa cyfrowego w celu wspierania dobrobytu gospodarczego i społecznego [*Recommendation of the Council on Digital Risk Management for Economic and Social Prosperity of 17 September 2015 (C(2015)115)*]. W zaleceniu tym wskazano, że globalna łączność cyfrowa przyniosła znaczne możliwości, ale pojawiające się w związku z jej rozwojem zagrożenia są coraz powszechniejsze i wyrafinowane, mogą więc wywierać wpływ na funkcjonowanie zarówno sektora publicznego, jak i prywatnego. Obecnie w związku z tym należy patrzeć na problem bezpieczeństwa szerzej, nie ograniczając się jedynie do aspektów technologicznych. Stąd w zaleceniu zrezygnowano z pojęć „cyberbezpieczeństwo" i „cyberprzestrzeń", posługując się terminami szerszymi – „zagrożenie cyfrowe" i „środowisko cyfrowe". W treści zalecenia podkreślono, że zarówno rządy, jak i firmy prywatne powinny przyjąć na siebie odpowiedzialność za zwalczanie zagrożeń cyfrowych. Sformułowano w nim zasady zarządzania ryzykiem bezpieczeństwa cyfrowego dla wszystkich zainteresowanych stron (rządy państw, organizacje publiczne i prywatne, a także osoby fizyczne, które opierają całość lub część swojej działalności społecznej lub gospodarczej na środowisku cyfrowym) oraz wytyczne dla strategii krajowych dla zapewnienia bezpieczeństwa cyfrowego, na rzecz wdrożenia których powinny działać rządy państw. Strategie te mają jasno wyrażać całościowe podejście rządów, które powinno być elastyczne, technologicznie neutralne oraz spójne z innymi strategiami wspierania społecznego i gospodarczego dobrobytu, obejmować najlepsze praktyki dla sektora publicznego, dużych przedsiębiorstw, małych i średnich firm, jak i poszczególnych obywateli (zob. szerzej *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 152–156).

Z innych zaleceń OECD związanych z szeroko rozumianą technologią informatyczną należy wskazać w szczególności:

1) wciąż obowiązujące zalecenie Rady C(80)58 z 23.9.1980 r. dotyczące wytycznych w sprawie ochrony prywatności i przepływu danych osobowych przez granice [*Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 (C(80)58(final)*] (zrewidowane w 2013 r.), będące pierwszym uzgodnionym na szczeblu międzynarodowym zbiorem zasad, jakimi powinny kierować się państwa, tworząc regulacje w zakresie ochrony prawa do prywatności w związku z transgranicznym przepływem danych osobowych,
2) zalecenie C(2007)67 z 12.12.2007 r. w sprawie współpracy transgranicznej w zakresie egzekwowania prawa chroniącego prywatność [*Recommendation*

of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of 12 December 2007 (C(2007)67(final)] (zrewidowane w 2013 r.), zawierające propozycje działań, jakie należy podjąć w celu poprawy współpracy międzynarodowej w zakresie ochrony prywatności związanej z transgranicznym przepływem danych osobowych,

3) zalecenie C(2006)57 z 13.4.2006 r. w sprawie współpracy transgranicznej w zakresie egzekwowania prawa przeciwko spamowi [*Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam of 13 April 2006 (C(2006) 57)*],

4) zalecenie C(2008)35 z 30.4.2006 r. w sprawie ochrony informatycznych infrastruktur krytycznych [*Recommendation of the Council on Protection of Critical Information Infrastructures of 30 April 2008 (C(2008)35)*], zawierające wytyczne dla państw w zakresie tworzenia ochrony krytycznych infrastruktur informatycznych (CII) na poziomie krajowym i międzynarodowym. Podsumowując analizę aktywności OECD w dziedzinie regulacji dotyczących nowych technologii, należy podkreślić, że chociaż organizacja ta jako pierwsza podjęła działania mające na celu przeciwdziałanie cyberprzestępczości, to obecnie głównym przedmiotem jej zainteresowania jest obecnie cyberbezpieczeństwo (*S. Schjølberg*, The History of Global Harmonization, s. 17).

4 4. **Rada Europy.** Omawiając działalność Rady Europy w zakresie cyberbezpieczeństwa oraz zwalczania cyberprzestępczości, wyjść niewątpliwie należy od zalecenia R(89)9 w sprawie przestępstw komputerowych, przyjętego przez Komitet Ministrów Rady Europy 13.9.1989 r. [*Recommendation No. R(89)9 on computer-related crime*]. Dokument ten nakazywał państwom członkowskim uwzględnienie w trakcie prac legislacyjnych nad regulacjami mającymi na celu zwalczanie przestępstw komputerowych propozycji rozwiązań zawartych w załączonym do nich raporcie (zob. szerzej *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 158–160).

Pierwszą umową międzynarodową dotyczącą zwalczania przestępstw popełnianych za pośrednictwem Internetu oraz sieci komputerowych jest wspominana już Konwencja o cyberprzestępczości. W trwających ponad cztery lata pracach, których była efektem, uczestniczyli nie tylko reprezentanci większości państw członkowskich Rady Europy (w tym Polski), ale również – w charakterze obserwatorów – delegaci z USA, Japonii i Kanady, przedstawiciele instytucji europejskich oraz niezależni eksperci. Celem Konwencji o cyberprzestępczości było stworzenie ram prawnych ścigania przestępstw o charakterze międzynarodowym. Zaproponowano w niej wiele nowatorskich (jak na owe czasy – nie zapominajmy, że powstawała ona pod koniec ubiegłego wieku) rozwiązań. Poszerzono w niej – w stosunku do wcześniejszych dokumentów o charakterze międzynarodowym – listę przestępstw (są to: nielegalny dostęp, nielegalne przechwytywanie transmisji, nielegalna ingerencja w dane komputerowe, nielegalna ingerencja w system komputerowy, czyny dotyczące narzędzi hackerskich, fałszerstwo komputerowe, oszustwo komputerowe, przestępstwa związane z pornografią dziecięcą, przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych). Zawarto w niej ponadto postanowienia dotyczące karalności form stadialnych i zjawiskowych oraz odpowiedzialności osób prawnych (przez pojęcie to rozumie się również jednostki organizacyjne nieposiadające osobowości prawnej). Przewidziano też szereg rozwiązań o charakterze proceduralnym, takich jak zabezpieczenie danych, przeszukanie i zatrzymanie danych, gromadzenie w czasie rzeczywistym danych ruchowych itd. (por. *A. Adamski*, Przestępczość w cyberprzestrzeni, s. 9–11; *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 162–164; *R. Tarnogórski*, Konwencja o cyberprzestępczości, s. 207–210).

Do niewątpliwych zalet Konwencji o cyberprzestępczości należy zaliczyć jej otwarty charakter – możliwe jest przystąpienie do niej państw niebędących członkami Rady Europy – oraz zastosowanie w niej klauzul opcjonalnych. Umożliwiają

one przyjęcie Konwencji o cyberprzestępczości z wyłączeniem niektórych postanowień, dzięki czemu państwa do niej przystępujące mogą, implementując ją do swojego prawa wewnętrznego, pogodzić jej rozwiązania ze swoją tradycją i kulturą prawną oraz obowiązującymi już regulacjami (por. *A. Adamski*, Przestępczość w cyberprzestrzeni, s. 9–17). W związku z powyższym do 1.5.2019 r. Konwencję o cyberprzestępczości podpisały niemal wszystkie państwa członkowskie Rady Europy (dokładnie 46, nie podpisała jedynie Rosja), a ratyfikowało ją 44 z nich. Ponadto Konwencję podpisały 4 państwa spoza Europy (Kanada, Japonia, Stany Zjednoczone, Republika Południowej Afryki; pierwsze trzy już ratyfikowały), kolejne zaś 16 państw (m.in. Australia, Dominikana, Izrael, Panama) do niej przystąpiło. Na marginesie należy dodać, że wiele państw – nie podpisując Konwencji o cyberprzestępczości – faktycznie czerpało z jej postanowień, tworząc własne regulacje krajowe. Wśród nich można wskazać Egipt czy Pakistan.

Konwencja o cyberprzestępczości weszła w życie 1.7.2004 r. po ratyfikacji przez pięć państw-sygnatariuszy. Polska podpisała Konwencję o cyberprzestępczości jako jedna z pierwszych (w dniu otwarcia do podpisu – 23.11.2001 r.), ale ratyfikowała dopiero 29.1.2015 r. Dotychczas przeprowadzono dwie nowelizacje KK [ustawa z 18.3.2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz.U. Nr 69, poz. 626), oraz ustawa z 24.10.2008 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw (Dz.U. Nr 214, poz. 1344)] mające na celu dostosowanie jego przepisów do postanowień Konwencji o cyberprzestępczości.

Wśród innych dokumentów przyjętych w ramach Rady Europy, pośrednio związanych z omawianą problematyką, wskazać należy przede wszystkim:

1) Konwencję Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych sporządzoną w Strasburgu 28.1.1981 r. (Dz.U. 2003 r. Nr 3, poz. 25);
2) zalecenie CM/R(99)5 z 23.2.1999 r. w sprawie ochrony prywatności w Internecie [*Recommendation Rec(99)5 on the protection of privacy in Internet*];
3) zalecenie CM/R(2009)1 z 18.2.2009 r. o demokracji elektronicznej (e-demokracji) [*Recommendation CM/Rec(2009)1 on electronic democracy (e-democracy)*].

5. **Organizacja Bezpieczeństwa i Współpracy w Europie.** Kwestia bezpieczeństwa danych przetwarzanych w sieciach komputerowych nie znalazła się w obszarze zainteresowań Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE, ang. *Organization for Security and Co-operation in Europe* – OSCE). Nie znaczy to oczywiście, że jej aktywność nie odnosi się w ogóle do kwestii cyberbezpieczeństwa. Jako przykłady można wskazać cztery decyzje Komitetu Ministrów: dwie w sprawie przeciwdziałania używaniu Internetu w celach terrorystycznych (*Ministerial Council Decision of 7 December 2004 No. 3/04 on Combating the use of the Internet for terrorist purposes* oraz *Ministerial Council Decision of 7 December 2006 No. 7/06 on Combating the use of the Internet for terrorist purposes*), w których wskazano, że należy przeciwdziałać wykorzystywaniu przez grupy terrorystyczne Internetu w celach takich, jak rekrutacja członków, zbieranie i przekazywanie funduszy, organizowaniu aktów terroru czy sianiu propagandy, przy jednoczesnym poszanowaniu praw człowieka, zwłaszcza prawa do prywatności oraz wolności wyrażania opinii i poglądów. Służyć temu ma wymiana informacji między państwami-stronami oraz tworzenie strategii zwalczania tego zjawiska. Dwie kolejne dotyczą wzmocnienia wysiłków OBWE w celu zmniejszenia ryzyka konfliktu wynikającego z wykorzystania technologii informacyjnych i komunikacyjnych (*Decision No. 5/16 of 9 December 2016 on enhancing OSCE efforts to reduce the risks of conflict stemming from the use of information and communication technologies* oraz *Decision No.* **5**

5/17 of 8 December 2016 on enhancing OSCE efforts to reduce the risks of conflict stemming from the use of information and communication technologies).

6 6. **Organizacja Narodów Zjednoczonych.** Na wstępie należy zwrócić uwagę, że Organizacja Narodów Zjednoczonych (ONZ) początkowo przywiązywała przede wszystkim wagę do zapobiegania przestępstwom komputerowym, nawiązując do rozważań teoretycznych oraz badań empirycznych poczynionych przez kryminologów w tym zakresie. Podejście to jednak stopniowo zaczęło ulegać zmianie w ciągu ostatnich kilku lat, o czym świadczy zwłaszcza tekst tzw. Deklaracji Salwadorskiej (zob. dalsze uwagi).

Problemom cyberprzestępczości poświęcono na forum ONZ większą uwagę po raz pierwszy w 1990 r. podczas VIII Kongresu w sprawie Zapobiegania Przestępczości i Postępowania ze Skazanymi (*The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*) odbywającego się w Hawanie 27.8–7.9.1990 r. (kongresy takie jak ten, dotyczące zwalczania przestępczości, organizowane są przez ONZ co pięć lat, obecnie – tj. od kongresu w Bangkoku w 2005 r. – jako kongresy w sprawie Zapobiegania Przestępczości i Wymiaru Sprawiedliwości w Sprawach Karnych, *Congresses on Crime Prevention and Criminal Justice*), oraz na towarzyszącym mu Sympozjum dotyczącym Zapobiegania i Ścigania Przestępstw Komputerowych (*Symposium on the Prevention and Prosecution of Computer Crime*), zorganizowanym przez Fundację na rzecz Odpowiedzialnej Informatyki (*Foundation for Responsible Computing*). Wynikiem toczonych dyskusji było przyjęcie przez Zgromadzenie Ogólne ONZ 14.12.1990 r. z inicjatywy przedstawicieli Kanady rezolucji Nr 45/121 dotyczącej przestępstw związanych z wykorzystaniem komputerów (por. *A. Adamski*, Prawo karne komputerowe, s. 9–10; *U. Sieber*, Legal Aspects of Computer-Related Crime, s. 162–163).

Kolejne rezolucje Zgromadzenia Ogólnego ONZ można podzielić w sposób zaproponowany przez *A.M. Hubbard* i *S. Schjølberga* (*A.M. Hubbard*, *S. Schjølberg*, Harmonizing national legal approaches, s. 6) na następujące grupy:

1) rezolucje: Nr 53/70 z 3.12.1998 r., Nr 54/49 z 1.12.1999 r., Nr 55/28 z 20.11.2000 r., Nr 56/19 z 29.11.2001 r., Nr 57/53 z 22.11.2002 r., Nr 58/32 z 18.12.2003 r., Nr 59/61 z 3.12.2004 r., Nr 60/45 z 8.12.2005 r., Nr 61/54 z 6.12.2006 r., Nr 62/17 z 5.12.2007 r., Nr 63/37 z 2.12.2008 r., Nr 64/25 z 2.12.2009 r., Nr 65/41 z 8.12.2010 r., Nr 66/24 z 2.12.2011 r., Nr 67/27 z 3.12.2012 r., Nr 68/243 z 27.12.2013 r. oraz Nr 69/28 z 2.12.2014 r., wszystkie zatytułowane jako „Rozwój w dziedzinie informacji i telekomunikacji w kontekście rozwoju międzynarodowego bezpieczeństwa" (*Developments in the Field of Information and Telecommunications in the Context of International Security*), które zawierają dość ogólne postanowienia, wskazując na zagrożenia, jakie może ze sobą nieść rozwijająca się technologia informatyczna, oraz rekomendując państwom przyjmowanie zaleceń formułowanych w cyklicznie sporządzanych przez grupę ekspertów (*Group of Government Experts on Information Security*) raportach dotyczących bezpieczeństwa informacji;
2) rezolucje: Nr 55/63 z 4.12.2000 r. oraz Nr 56/121 z 19.12.2001 r. (obie zatytułowane „Walka z kryminalnymi nadużyciami technologii informatycznej" – *Combating the Criminal Misuse of Information Technology*), w których wskazano działania, jakie należy podjąć na szczeblu międzynarodowym oraz w ustawodawstwach krajowych w celu skutecznego zwalczania cyberprzestępczości. Zdaniem ich autorów przede wszystkim niezbędne jest stworzenie regulacji prawnych zapewniających ochronę wszystkich aspektów bezpieczeństwa danych komputerowych i systemów (tj. poufności, integralności oraz dostępności) przed nieuprawnionymi naruszeniami oraz zapewnienie, by nadużycia te były kryminalizowane we wszystkich państwach. Ponadto podkreślono konieczność

podjęcia środków umożliwiających współpracę organów wymiaru sprawiedliwości w ściganiu i stawianiu przed sądem sprawców nadużyć komputerowych;

3) rezolucje: Nr 57/239 z 20.12.2002 r. „Tworzenie światowej kultury cyberbezpieczeństwa" (*Creation of a global culture of cybersecurity*), Nr 58/199 z 23.12.2003 r. „Tworzenie światowej kultury cyberbezpieczeństwa oraz ochrona informatycznej infrastruktury krytycznej" (*Creation of a global culture of cybersecurity and the protection of critical information infrastructures*) oraz Nr 64/211 z 21.12.2009 r. „Tworzenie światowej kultury cyberbezpieczeństwa oraz wzmożenie wysiłków na rzecz ochrony informatycznej infrastruktury krytycznej" (*Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*), które zostały poświęcone konieczności zapewnienia większego bezpieczeństwa sieci oraz przetwarzanych w nich informacji. W rezolucji 57/239 skupiono się na problemie skutków współzależności między infrastrukturą informatyczną z innym sektorami światowej infrastruktury krytycznej dla administracji państwowej. Natomiast w rezolucji Nr 64/211 zachęca się państwa członkowskie oraz organizacje międzynarodowe, które rozwijają strategie związane z cyberbezpieczeństwem oraz ochroną infrastruktur krytycznych, do podzielenia się z innymi państwami swoimi doświadczeniami Ponadto w aneksie załączonym do niej zawarto wskazówki mające pomóc przy tworzeniu skutecznego systemu zapewnienia cyberbezpieczeństwa (*F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 196–200).

Na wspomnianym VIII Kongresie ONZ w Hawanie w 1990 r. została opracowana rezolucja Nr 45/121 dotycząca przestępstw związanych z wykorzystaniem komputerów. Innym owocem tego Kongresu było opracowanie opublikowanego w 1994 r. „Podręcznika dotyczącego zapobiegania i kontroli przestępstw związanych z użyciem komputera". W deklaracji wydanej na X Kongresie w sprawie Zapobiegania Przestępczości i Postępowania ze Skazanymi w Wiedniu [Deklaracja wiedeńska w sprawie przestępczości i wymiaru sprawiedliwości: sprostanie wyzwaniom XXI wieku (*Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century*); http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/562/93/PDF/N0056293.pdf?OpenElement, dostęp: 1.3.2019 r.)], która stanowi aneks do rezolucji Zgromadzenia Ogólnego Nr 55/59 z 4.12.2000 r., jedynie oględnie wspomniano o przestępstwach komputerowych (w pkt 18, w którym mowa m.in. o planowej polityce wydawania zaleceń dotyczącej zapobiegania temu zjawisku). Natomiast w deklaracji pt. „Współdziałanie i oddziaływanie: sojusze strategiczne w zapobieganiu przestępczości i wymiaru sprawiedliwości w sprawach karnych" (*Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice*), stanowiącej aneks do rezolucji Zgromadzenia Ogólnego Nr 60/177 z 16.12.2005 r. „Działania następcze po jedenastym Kongresie Narodów Zjednoczonych w sprawie zapobiegania przestępczości i wymiaru sprawiedliwości w sprawach karnych" (*Follow-up to the Eleventh United Nations Congress on Crime Prevention and Criminal Justice*; http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/498/22/PDF/N0549822.pdf?OpenElement, dostęp: 1.3.2019 r.), kończącej XI Kongres w Bangkoku, zwrócono uwagę po raz kolejny na znaczenie harmonizacji prawa karnego, jako niezbędnego czynnika dla skutecznej walki z cyberprzestępczością, oraz na istotną rolę, jaką w tym procesie mają do odegrania zarówno ONZ, jak i inne organizacje międzynarodowe. W tzw. Deklaracji Salwadorskiej „Strategie wobec światowych wyzwań, takich jak: zapobieganie przestępczości, system karny oraz ich rozwój w zmieniającym się świecie" (*Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*), podjętej na XII Kongresie w Salwadorze (12–19.4.2010 r.), jako jego dokument końcowy (aneks do

rezolucji Zgromadzenia Ogólnego Nr 65/230 z 21.12.2010 r.), zalecono Komisji ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości (*The Commission on Crime Prevention and Criminal Justice* – CCPCJ) we współpracy z państwami członkowskimi, przedstawicielami międzynarodowej społeczności oraz sektora prywatnego stworzenie projektów nowych krajowych i międzynarodowych rozwiązań będących odpowiedzią na zagrożenie, jakim jest zjawisko cyberprzestępczości. Na ostatnim, XIII Kongresie ONZ, który odbył się 11–19.4.2015 r. w Doha (Al-Dauha) w Katarze, skupiono się na problemie włączenia kwestii zapobiegania przestępczości oraz wymiaru sprawiedliwości w sprawach karnych w ramy szerszego programu ONZ, którego celem byłoby sprostanie wyzwaniom społecznym i gospodarczym oraz promowanie praworządności na szczeblu krajowym i międzynarodowym przy udziale społeczeństwa. Co do kwestii związanych z cyberbezpieczeństwem, w trakcie obrad kongresu po raz kolejny zwrócono uwagę na konieczność podjęcia konkretnych środków mających na celu stworzenie bezpiecznej cyberprzestrzeni. W kontekście zapobiegania i przeciwdziałania działalności przestępczej w Internecie położono nacisk na takie kwestie, jak kradzież tożsamości, botnety, rekrutacja on-line na potrzeby terroryzmu lub handlu ludźmi oraz konieczność ochrony dzieci. Ponadto podkreślano znaczenie wzmocnienia współpracy międzynarodowej jako warunku niezbędnego dla zapewnienia bezpieczeństwa w cyberprzestrzeni. Finalnym dokumentem XIII Kongresu była Deklaracja z Dohy [Deklaracja w sprawie integracji zapobiegania przestępczości i wymiaru sprawiedliwości w sprawach karnych w ramach szerszej agendy ONZ w celu sprostania wyzwaniom społecznym i gospodarczym oraz promowania praworządności na szczeblu krajowym i międzynarodowym oraz udziału społeczeństwa (*Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation*); http://www.unodc.org/documents/congress//Declaration/V1504151~English.pdf, dostęp: 1.3.2019 r.], której tekst został przyjęty przez aklamację pierwszego dnia kongresu. Stanowi ona podsumowanie dotychczasowego 60-letniego dorobku kongresów oraz działalności ONZ w dziedzinie zapobiegania przestępczości oraz próbę odpowiedzi na współczesne wyzwania w tej materii (*E.W. Pływaczewski*, XIII Kongres Organizacji Narodów Zjednoczonych, s. 178; https://www.un.org/press/en/2015/soccp359.doc.htm, dostęp: 1.3.2019 r.). Dla realizacji celów Deklaracji z Dohy, Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC – *The United Nations Office on Drugs and Crime*) – przy finansowym wsparciu Kataru – uruchomiło ambitny program o charakterze globalnym, mający pomóc krajom w zapobieganiu przestępczości, rozwojowi wymiaru sprawiedliwości w sprawach karnych, zwalczaniu korupcji oraz zapewnieniu praworządności. Następny kongres zaplanowany jest na 20–27.4.2020 r. Odbędzie się w Kyoto (miasto to było miejscem IV kongresu w 1970 r.).

Wyspecjalizowaną agencją Organizacji Narodów Zjednoczonych, najprężniej obecnie działającą w kierunku zapewnienia bezpieczeństwa w cyberprzestrzeni poprzez harmonizację porządków prawnych państw oraz tworzenie międzynarodowych regulacji, jest Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union* – ITU) z siedzibą w Genewie. Do zadań ITU należy standaryzacja oraz regulacja rynku telekomunikacyjnego, wspieranie międzynarodowej współpracy w dziedzinie telekomunikacji, pomoc techniczna krajom rozwijającym się, działania na rzecz powstania globalnej sieci telekomunikacyjnej łączącej wiele technologii (zob. szerzej *J. Kubicka*, International organizations, s. 127–128). Działania ITU są prowadzone w trzech zasadniczych obszarach, za które odpowiadają wyodrębnione struktury: sektor radiokomunikacyjny (ang. *Radiocommunication Sector* – ITU-R), sektor standaryzacyjny (ang. *Standardization Sector* – ITU-T) oraz sektor rozwoju telekomunikacyjnego (ang. *Telecommunication Development Sector* – ITU-D).

W 2001 r. Zgromadzenie Ogólne ONZ wydało rezolucję Nr 56/183 z 21.12.2001 r. w sprawie Światowego Szczytu dotyczącego Społeczeństwa Informacyjnego (http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf, dostęp: 1.3.2019 r.), w której zaaprobowało przedstawioną przez ITU koncepcję realizacji Światowego Szczytu Społeczeństwa Informacyjnego (*World Summit on the Information Society* – WSIS). Szczyt przebiegał w dwóch etapach: faza pierwsza miała miejsce 10–12.12.2003 r. w Genewie, faza druga – 16–18.11.2005 r. w Tunisie.

Głównym celem pierwszej fazy WSIS było wypracowanie wspólnego stanowiska oraz przyjęcie oświadczenia wyrażającego polityczną wolę tworzenia podstaw „społeczeństwa informacyjnego dla wszystkich", uwzględniającego zróżnicowane interesy wszystkich uczestników oraz zapowiadającego podjęcie pierwszych kroków w kierunku realizacji tego zamierzenia. Efektem prac było przyjęcie 2.12.2003 r. Deklaracji Genewskiej („Deklaracja zasad. Budowanie społeczeństwa informacyjnego: globalne wyzwanie w nowym tysiącleciu" – *Geneva Declaration of Principles. Building the Information Society: a global challenge in the new Millennium*) oraz Genewskiego Planu Działania (*Geneva Plan of Action*). Faza druga WSIS miała na celu przede wszystkim nadanie biegu realizacji postanowień Planu Genewskiego oraz poszukiwanie rozwiązań w takich dziedzinach, jak zarządzanie Internetem czy mechanizmy finansowe w sieci. W dniu 18.11.2005 r. ogłoszono dokument pt. Agenda z Tunisu na rzecz społeczeństwa informacyjnego (*Tunis Agenda on Information Society*), w którym podkreślono rolę współpracy międzynarodowej w walce z cyberprzestępczością, polegającej zarówno na kooperacji między organami wymiaru sprawiedliwości, jak i tworzeniu przez rządy we współpracy z innymi zainteresowanymi stronami (przedstawicielami branży informatycznej, organizacjami pozarządowymi) odpowiednich ram prawnych (zob. szerzej *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 204–207).

W dniu 17.5.2007 r. została zainicjowana ITU *Global Cybersecurity Agenda* – GCA. Ma ona stanowić ramy dla dialogu i współpracy międzynarodowej, umożliwiając koordynację działań o zasięgu globalnym, będących odpowiedzią na wyzwania, jakimi są walka z cyberprzestępczością oraz budowa bezpiecznego społeczeństwa informacyjnego. Opiera się ona na pięciu strategicznych filarach (środki prawne, środki techniczne i proceduralne, struktura organizacyjna, budowanie potencjału, międzynarodowa współpraca), a głównym jej celem jest stworzenie strategii rozwoju modelowej regulacji przeciwdziałania cyberprzestępczości, kompatybilnej z przepisami krajowymi i regulacjami regionalnymi, i mogącej znaleźć zastosowanie na całym świecie (*F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 207–208).

7. **Unia Europejska.** Omawiając problematykę działalności Unii Europejskiej **7**
w dziedzinie cyberbezpieczeństwa oraz zwalczania cyberprzestępczości, należy cofnąć się do lat 90. ubiegłego wieku, kiedy to wydano pierwsze akty prawne o charakterze niewiążącym dotyczące tych kwestii. Zawierały one wezwania do podjęcia odpowiednich działań, wskazania pewnych rozwiązań, propozycje projektów aktów prawnych, strategie i plany działań dotyczących poprawienia bezpieczeństwa sieci. Należy tu w szczególności wskazać:

1) decyzję Rady 92/242/WE z 31.3.1992 r. w dziedzinie bezpieczeństwa systemów informatycznych, stanowiącą zarys ogólnej strategii bezpieczeństwa systemów informatycznych (w formie planu działań), obejmującą: opracowanie strategicznych ram dla bezpieczeństwa systemów informatycznych, określenie wymagań stawianych usługodawcy w celu zapewnienia bezpieczeństwa systemów informatycznych, zaspokajanie bieżących i tymczasowych potrzeb użytkowników, dostawców oraz usługodawców, opracowanie specyfikacji, normalizacji, oceny i certyfikacji w odniesieniu do bezpieczeństwa systemów informatycznych, zapewnienie bezpieczeństwa systemów informatycznych;

2) zalecenie Komisji 95/144/WE z 7.4.1995 r. w sprawie wspólnych kryteriów oceny bezpieczeństwa informatycznego, w którym zarekomendowano przyjęcie przez państwa członkowskie kryteriów ITSEC [(ang. *Information Technology Security Evaluation Criteria*) – zbiór kryteriów oceny bezpieczeństwa systemów teleinformatycznych wprowadzony w latach 90. ubiegłego wieku] oraz pogłębianie międzynarodowej harmonizacji i standaryzacji kryteriów oceny bezpieczeństwa technologii informatycznych;
3) komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM(2000)890 w sprawie tworzenia bezpiecznego społeczeństwa informacyjnego poprzez zwiększenie bezpieczeństwa struktur informacyjnych i zwalczanie przestępczości komputerowej z 26.1.2001 r. (tzw. komunikat o cyberprzestępczości), w którym zwrócono uwagę na konieczność podjęcia skutecznych działań w walce z cyberprzestępczością, zaproponowano zrównoważone podejście do rozwiązywania problemów z nią związanych, uznano za niezbędne wzięcie w pełni pod uwagę opinii wszystkich zainteresowanych zwalczaniem tego zjawiska stron, w tym organów ścigania, dostawców usług, operatorów sieci, innych grup branżowych, grup konsumenckich, organów ochrony danych itd.; w dokumencie tym Komisja zaproponowała szereg inicjatyw legislacyjnych i pozalegislacyjnych;
4) rezolucję Parlamentu z 19.5.2000 r. wzywającą do podjęcia działań legislacyjnych przeciwko przestępczości z wykorzystaniem zaawansowanej technologii;
5) komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Bezpieczeństwo sieci i informacji: Propozycje na rzecz europejskiego podejścia" COM(2001)298 z 6.6.2001 r., w którym przedstawiono analizę aktualnych problemów bezpieczeństwa sieci oraz zaprezentowano strategiczny zarys działań w tym obszarze; zaproponowano znamiona czynów stanowiących zagrożenie dla bezpieczeństwa systemów informatycznych;
6) zalecenie Rady z 25.6.2001 r. w sprawie punktów kontaktowych utrzymujących 24-godzinny dyżur w celu zwalczania przestępczości z wykorzystaniem zaawansowanej technologii;
7) rezolucję Rady z 28.1.2002 r. w sprawie wspólnego podejścia i działań szczególnych w dziedzinie bezpieczeństwa sieci i informacji;
8) komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM(2006)251 z 31.5.2006 r. dotyczący strategii na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatyw", w którym zaproponowano nowe, spójne podejście do kwestii bezpieczeństwa sieci;
9) komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM(2006)288 z 15.7.2006 r. w sprawie walki ze spamem, oprogramowaniem szpiegującym i złośliwym;
10) komunikat Komisji do Parlamentu Europejskiego, Rady i Komitetu Regionów COM(2007)267 z 22.5.2007 r. w kierunku ogólnej strategii zwalczania cyberprzestępczości, stanowiący rozwinięcie tzw. komunikatu o cyberprzestępczości z 2001 r. (tj. komunikatu Komisji COM(2000)890 w sprawie tworzenia bezpiecznego społeczeństwa informacyjnego poprzez zwiększenie bezpieczeństwa struktur informacyjnych i zwalczanie przestępczości komputerowej), w którym Komisja zwróciła uwagę, że liczba przestępstw komputerowych stale wzrasta, stają się one coraz bardziej wyrafinowane, wykraczają poza granice państw, często popełniane są przez zorganizowane grupy przestępcze, a jednocześnie eskalacji tego zjawiska nie towarzyszy wzrost liczby aktów oskarżenia na podstawie transgranicznej współpracy organów ścigania w Europie. Wskazano, że

coraz częściej do popełniania oszustw na masową skalę stosowane są takie metody, jak kradzież tożsamości, phishing, spam oraz używanie złośliwych kodów. Rosnącym problemem staje się również nielegalny handel internetowy (narkotykami, bronią), a także wzrost liczby stron internetowych zawierających nielegalne treści. Komisja wskazała również na problem wzrostu liczby ataków na masową skalę, w tym przybierających formę skoordynowanych ataków na systemy informatyczne infrastruktury krytycznej państw członkowskich. Strategia przeciwdziałania cyberprzestępczości powinna uzupełniać aspekty prawnokarne ścigania przestępczości o inne środki, a polegać na poprawie współpracy operacyjnej organów ścigania, lepszej współpracy i koordynacji politycznej między państwami członkowskimi, współpracy politycznej i prawnej z krajami trzecimi, podnoszeniu świadomości, prowadzeniu szkoleń, badań, ściślejszym dialogu z sektorem przemysłu i ewentualnie działaniach legislacyjnych;

11) komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM(2009)149 z 30.3.2009 r. w sprawie ochrony krytycznej infrastruktury informatycznej „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności" oraz załączony do niego raport, będący efektem trwających kilka lat zakrojonych na szeroką skalę, prowadzonych na szczeblu unijnym konsultacji dotyczących bezpieczeństwa sieci (*F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 233–236).

Pod koniec 1999 r. ogłoszono inicjatywę „eEurope – społeczeństwo informacyjne dla wszystkich" [komunikat Komisji COM (1999) 687 „e-Europe – Społeczeństwo informacyjne dla wszystkich"]. Komunikat dotyczący inicjatywy Komisji skierowany był na specjalny szczyt Rady Europejskiej w Lizbonie 23–24.3.2000 r., której celem było uporządkowanie działań mających prowadzić do budowy społeczeństwa informacyjnego. W komunikacie podkreślono, że informatyzacja musi objąć wszystkie sfery życia mieszkańców Europy, w szczególności pracę, dom, szkołę, uczelnię, służbę zdrowia, transport oraz kontakty z administracją publiczną.

W dokumencie tym wskazano dziesięć obszarów, na które powinien być położony szczególny nacisk w drodze do stworzenia społeczeństwa informacyjnego. Za *M. Kulińskim* obszary te można podzielić na trzy grupy dotyczące:

1) infrastruktury (zapewnienie taniego dostępu do Internetu oraz budowa szybkich łączy internetowych dla środowisk naukowych i studentów);
2) badań i edukacji (przede wszystkim wprowadzenie Internetu do szkół oraz wspieranie małych i średnich przedsiębiorstw w sferze zaawansowanych technologii);
3) aplikacji – zastosowań (przyspieszenie rozwoju handlu elektronicznego, inteligentne karty, e-health, e-government, „inteligentny" transport) (*M. Kuliński*, Regulacje komunikacji elektronicznej, s. 23–24).

Na wspomnianym wyżej specjalnym szczycie Rady Europejskiej, który miał miejsce w Lizbonie 23–24.3.2000 r., zaaprobowano program eEurope oraz przyjęto tzw. Strategię lizbońską. Była ona długookresowym programem rozwoju społeczno-gospodarczego Unii Europejskiej, którego celem było uczynienie Europy najbardziej dynamicznym i konkurencyjnym regionem gospodarczym na świecie poprzez budowę gospodarki opartej na wiedzy (tj. gospodarki bezpośrednio bazującej na produkcji, dystrybucji i stosowaniu wiedzy i informacji).

W czerwcu 2000 r. na szczycie w Santa Maria de Feira został przyjęty plan „eEurope 2002 – Społeczeństwo informacyjne dla wszystkich. Plan działań". Cele, jakie miał realizować, zostały podzielone na trzy grupy:

1) zapewnienie tańszego, szybszego i bezpieczniejszego Internetu;

2) inwestowanie w ludzi i umiejętności;
3) pobudzanie wykorzystania Internetu.

Działania podjęte w ramach programu eEurope 2002 kontynuowano w eEurope 2005, a następnie w strategii i2010 ogłoszonej w komunikacie Komisji COM(2005)229 z 1.6.2005 r. „i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia". Kontynuacją programu i2010 jest strategia „Europa 2020 – strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu" COM(2010)2020, która została zatwierdzona przez Radę Europejską 17.6.2010 r. W jej ramach realizowana jest Europejska agenda cyfrowa. Jej celem jest rozwój jednolitego rynku cyfrowego mającego umożliwić państwom Unii Europejskiej uzyskanie trwałych korzyści ekonomicznych i społecznych.

Na spotkaniu Rady Europejskiej, które odbyło się 4–5.11.2004 r. w Brukseli, przyjęto plan działań w dziedzinie sprawiedliwości i spraw wewnętrznych, który – z uwagi na fakt, iż miało to miejsce podczas przewodnictwa Holandii w Radzie Unii Europejskiej – nazwano Programem haskim. Jednocześnie Rada zaleciła Komisji uszczegółowienie planu poprzez zaproponowanie konkretnych działań oraz przedstawienie harmonogramu ich wykonania. Program haski był wieloletnim planem wzmocnienia Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, odnoszącym się do wszystkich aspektów jej polityk, również w wymiarze zewnętrznym. Położono w nim nacisk na walkę z terroryzmem oraz politykę wizową i azylową (budowa Wspólnego Europejskiego Systemu Azylowego).

Kontynuacją Programu haskiego był przyjęty przez Radę Europejską, w okresie prezydencji Szwecji na szczycie w Brukseli 10–11.12.2009 r., tzw. Program sztokholmski – „Otwarta i bezpieczna Europa dla wszystkich obywateli". Był on realizowany w ramach planu działania przyjętego przez Komisję 20.4.2010 r. Zalecono w nim opracowanie strategii bezpieczeństwa wewnętrznego dla UE, mającej na celu zwiększenie ochrony obywateli oraz skuteczne zwalczanie „poważnej" przestępczości, przestępczości zorganizowanej i terroryzmu poprzez wzmocnienie współpracy policyjnej i sądowej w sprawach karnych oraz współdziałanie państw członkowskich w zakresie zarządzania granicami, ochrony ludności oraz pomocy w przypadku klęsk żywiołowych lub katastrof. Strategia bezpieczeństwa wewnętrznego miała być budowana na bazie szerokiego, horyzontalnego i przekrojowego podejścia z wyraźnie podzielonymi zadaniami między UE i państwa członkowskie. Skoncentrowano się na walce z przestępczością transgraniczną obejmującą handel ludźmi, seksualne wykorzystywanie dzieci i przestępstwa związane z pornografią dziecięcą, przestępczość gospodarczą i korupcję, przestępczość związaną z narkotykami oraz cyberprzestępczość. W dziedzinie cyberbezpieczeństwa nacisk położono na konieczność propagowania polityk i tworzenia regulacji w celu zapewnienia bezpieczeństwa sieci oraz zwalczania cyberprzestępczości. Komisji zalecono stworzenie środków mających na celu pomoc w powstawaniu i sprawnym funkcjonowaniu partnerstw publiczno-prywatnych, natomiast Europolowi – zintensyfikowanie analizy strategicznej w zakresie cyberprzestępczości, prowadzonej na podstawie gromadzonych danych uzyskiwanych dzięki utworzeniu europejskiej platformy identyfikowania przestępstw, która powinna również pomagać krajowym platformom powiadamiania w państwach członkowskich w wymianie najlepszych praktyk. Dążono do dalszego uproszczenia przepisów dotyczących jurysdykcji w cyberprzestrzeni. Ponieważ realizacja Programu sztokholmskiego została zaplanowana na lata 2010–2014, Rada Europejska w czerwcu 2013 r. zwróciła się do kolejnych prezydencji o rozpoczęcie w Radzie UE procesu tworzenia nowych strategicznych wytycznych mających stanowić podstawę dla planów dalszego rozwoju PWBiS. Jednocześnie Komisja Europejska została zobowiązana do przedstawienia informacji na temat dotychczasowego przebiegu tego procesu. Efekty przeprowadzonych prac polegających m.in. na organizacji konsultacji społecznych oraz konferencji zostały przedstawione przez

Komisję w marcu 2014 r. w dwóch komunikatach skierowanych do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Unijny program na rzecz wymiaru sprawiedliwości na 2020 r. – zwiększanie zaufania, mobilności i wzrostu w Unii" oraz „Otwarta i bezpieczna Europa: realizacja założeń". Ostatecznie nowe wytyczne dotyczące planowania rozwoju PWBiS zostały określone przez Radę Europejską 26–27.6.2014 r. Nie nadano im jednak – jak to miało miejsce poprzednio – formy programu, ale zawarto w konkluzjach Rady Europejskiej. W dokumencie „Kontynuacja prac nad kompleksowym podejściem do bezpieczeństwa cybernetycznego i cyberprzestępczości" zapewnienie cyberbezpieczeństwa zostało uznane za jedno z podstawowych działań mających na celu zagwarantowanie obywatelom Unii rzeczywistej przestrzeni bezpieczeństwa.

Dnia 6.5.2015 r. została ogłoszona „Strategia jednolitego rynku cyfrowego dla Europy" [komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów (COM(2015)192 final], której celem ma być stworzenie jednolitych ram prawnych dla rynku cyfrowego UE.

Pierwszym wiążącym unijnym instrumentem prawnym, którego przedmiotem było zwalczanie przestępczości komputerowej, była decyzja ramowa Rady 2005/222/WSiSW z 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L Nr 69, s. 67). W akcie tym przede wszystkim zdefiniowano najistotniejsze pojęcia („system informatyczny", „dane komputerowe", „osoba prawna", „bezprawność"), zobowiązano państwa członkowskie do stypizowania przestępstw uzyskania bezprawnego dostępu, bezprawnej ingerencji w system informatyczny oraz bezprawnej ingerencji w dane komputerowe, odniesiono się do kwestii odpowiedzialności osób prawnych, jurysdykcji oraz stworzenia sieci operacyjnych punktów kontaktowych dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu w celu wymiany informacji dotyczących ataków na systemy informatyczne. Ograniczona liczba przestępstw określonych w decyzji ramowej 2005/222, konieczność uwzględnienia nowych zagrożeń, a także chęć dostosowania regulacji do nowych inicjatyw Unii Europejskiej w dziedzinie cyberbezpieczeństwa i uzupełnienia ich w celu stworzenia całościowej regulacji tej materii doprowadziły do decyzji o podjęciu prac nad nowym instrumentem prawnym w dziedzinie cyberprzestępczości. Prace nad nową regulacją zbiegły się w czasie z przyjęciem Traktatu z Lizbony, co umożliwiło posłużenie się dyrektywą w celu uregulowania kwestii cyberprzestępstw.

W treści dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z 12.8.2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową 2005/222/WSiSW (Dz.Urz. UE L Nr 218, s. 8) zasadniczo powtórzono postanowienia decyzji ramowej 2005/222, uzupełniając je jednak o szereg nowych rozwiązań. Przewidziano bowiem nowe typy czynów zabronionych (nielegalne przechwytywanie danych komputerowych oraz przestępstwa dotyczące „narzędzi hackerskich") oraz określono dodatkowe okoliczności – obok popełnienia przestępstwa w ramach organizacji przestępczej, przewidzianej w decyzji ramowej 2005/222 (określono jednak surowszą sankcję) – które państwa członkowskie powinny obligatoryjnie uznać za zaostrzające odpowiedzialność karną, a mianowicie: użycie botnetów, spowodowanie poważnej szkody (spowodowanie poważnej szkody lub wywarcie wpływu na istotne interesy było przewidziane w decyzji ramowej, ale przepis miał charakter fakultatywny), popełnienie czynu przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej, posłużenie się przez sprawcę przestępstwa prawdziwą tożsamością innej osoby.

Obecnie problematykę ochrony danych osobowych w Unii Europejskiej reguluje rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO. Wkrótce unormowanie to ma zostać uzupełnione o regulację o charakterze szczególnym, którego przedmiotem będzie ochrona danych osobowych przetwarzanych w sieciach łączności elektronicznej. Trwają bowiem prace nad projektem rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej).

Głównym instrumentem prawnym, którego celem jest zwalczanie terroryzmu, jest dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z 15.3.2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.Urz. UE L Nr 88, s. 6.). Zgodnie z postanowieniami art. 3 dyrektywy 2017/541, by czyn zabroniony mógł zostać uznany za przestępstwo terrorystyczne, musi – po pierwsze – spełniać kryterium przedmiotowe, tj. być jednym z czynów wymienionych w zamkniętym katalogu zawartym w tym przepisie lub grożeniem jego popełnienia. Po drugie – spełniać co najmniej jedną z wymienionych w drugiej części definicji przesłanek podmiotowych w postaci celu działania sprawcy, tj. musi być popełniony w celu:

1) poważnego zastraszenia ludności, lub
2) bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania, lub
3) poważnej destabilizacji lub zniszczenia podstawowych politycznych, konstytucyjnych, gospodarczych lub społecznych struktur danego państwa lub danej organizacji międzynarodowej.

W katalogu, o którym mowa wyżej, znajdują się m.in. czyny zabronione określone w art. 4 i 5 dyrektywy 2013/40 (odpowiednio niezgodna z prawem ingerencja w systemy oraz niezgodna z prawem ingerencja w dane), pod warunkiem zaistnienia którejś ze wskazanych w tej dyrektywie okoliczności obciążających (w przypadku czynu z art. 4, gdy działaniem sprawcy przy wykorzystaniu jednego z „programów hackerskich" dotknięta została znaczna liczba systemów informatycznych albo czyn spowodował poważne szkody lub był skierowany przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej, a w wypadku przestępstwa z art. 5 – gdy zostało popełnione przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej) (zob. szerzej *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 266–267). Ponadto zobowiązano państwa członkowskie do przyjęcia środków umożliwiających natychmiastowe usuwanie treści internetowych publicznie nawołujących do popełnienia przestępstwa terrorystycznego oraz blokujących takie, których nie można usunąć (art. 21 dyrektywy 2017/541).

W celu podniesienia poziomu bezpieczeństwa infrastruktury krytycznej o charakterze transgranicznym przyjęto dyrektywę 2008/114/WE z 8.12.2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.Urz. UE L Nr 345, s. 75). Zgodnie z jej art. 2 lit. a „infrastruktura krytyczna" oznacza składnik, system lub część infrastruktury, zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji, natomiast pod pojęciem „europejskiej infrastruktury krytycznej" (EIK), stosownie do art. 2 lit. b wskazanej wyżej dyrektywy, należy rozumieć „infrastrukturę krytyczną zlokalizowaną na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie. To, czy wpływ jest istotny, ocenia się w odniesieniu do kryteriów przekrojowych. Obejmuje to skutki wynikające z międzysektorowych współzależności z innymi rodzajami infrastruktury". Zgodnie

z art. 3 ust. 2 tej dyrektywy kryteria przekrojowe są następujące: kryterium ofiar w ludziach, kryterium skutków ekonomicznych oraz kryterium skutków społecznych. Wprawdzie koncentruje się ona na sektorach energii i transportu, ale planowane jest objęcie jej zakresem innych sektorów, m.in. sektora technologii informacyjno-komunikacyjnych („TIK").

Na zakończenie wspomnieć należy jeszcze o Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji oraz o Europejskim Centrum ds. Walki z Cyberprzestępczością. Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) została utworzona 15.3.2004 r. na mocy rozporządzenia Parlamentu Europejskiego i Rady (WE) Nr 460/2004 z 10.3.2004 r. ustanawiającego Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz.Urz. UE L Nr 77, s. 1). Jej celem jest pomoc państwom członkowskim Unii Europejskiej w kwestiach związanych z szeroko rozumianym cyberbezpieczeństwem oraz przyczynianie się do rozwoju społeczeństwa informacyjnego. Zgodnie z art. 27 rozporządzenia 460/2004 Agencja została utworzona na okres 5 lat, licząc od 14.3.2004 r. Następnie dwukrotnie kolejnymi rozporządzeniami przedłużano jej istnienie [rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 1007/2008 z 24.9.2008 r. zmieniające rozporządzenie (WE) Nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania (Dz.Urz. UE L Nr 293, s. 1) oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 580/2011 z 8.6.2011 r. zmieniające rozporządzenie (WE) 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania (Dz.Urz. UE L Nr 165, s. 3)]. Obecnie funkcjonuje na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 526/2013 z 21.5.2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylającego rozporządzenie (WE) 460/2004 (Dz.Urz. UE L Nr 165, s. 41). Tym razem jako okres jej istnienia przewidziano siedem lat. Jak słusznie zwracają uwagę *C. Banasiński* i *W. Nowak*, ten ograniczony czasowo mandat, nawet jeżeli jest przedłużany, znacznie ogranicza zdolności Agencji, utrudniając długofalowe planowanie oraz niekorzystnie wpływa na sytuację podmiotów, którym świadczy usługi. Okoliczność ta pozostaje również w sprzeczności z dyrektywą NIS, która (jak wskazano wyżej) powierza Agencji pewne zadania (*C. Banasiński*, *W. Nowak*, w: Cyberbezpieczeństwo, s. 151). Wkrótce ma jednak nastąpić kres tej tymczasowości – Komisja złożyła projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) Nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") (COM(2017)477), który nie tylko przewiduje mandat Agencji na czas nieokreślony, ale nadaje jej nowe uprawnienia i powierza dodatkowe zadania (m.in. w zakresie certyfikacji i normalizacji).

Z kolei powołane komunikatem Komisji do Rady i Parlamentu Europejskiego – „Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością" (COM/2012/0140 final) – Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) ma za zadanie koordynować zwalczanie cyberprzestępczości ma poziomie unijnym. Ponadto działa jako centrum specjalistycznej wiedzy technicznej w tej dziedzinie. Jego kompetencje nakładają się w związku z tym z kompetencjami ENISA.

8. **Dyrektywa NIS.** Projekt dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L Nr 194, s. 1) został przedstawiony w 2013 r. jako jeden z głównych elementów strategii cyberbezpieczeństwa, a jej podstawowym celem jest „zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji" (ang. *network and information security*, stąd nazywana jest dyrektywą NIS), czyli zwiększenia **8**

bezpieczeństwa sieci teleinformatycznych stanowiących podstawę funkcjonowania współczesnych społeczeństw i gospodarek państw członkowskich UE, co ma prowadzić do poprawy funkcjonowania rynku wewnętrznego UE. W tym celu w art. 2 ust. 1 dyrektywy NIS przewidziano:

a) ustanowienie obowiązków dla wszystkich państw członkowskich dotyczących przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;
b) utworzenie grupy współpracy w celu wspierania i ułatwiania strategicznej współpracy i wymiany informacji między państwami członkowskimi oraz rozwijania wśród nich zaufania i pewności;
c) utworzenie sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego, mającej przyczyniać się do rozwijania zaufania i pewności między państwami członkowskimi oraz promować szybką i skuteczną współpracę operacyjną;
d) stanowienie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych;
e) ustanowienie obowiązków dla państw członkowskich dotyczących wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT mających zadania związane z bezpieczeństwem sieci i systemów informatycznych.

Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w dyrektywie NIS nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z 7.3.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywy ramowej) (tj. przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej), ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

Dyrektywa NIS nie stanowi przeszkody dla działań podejmowanych przez państwa członkowskie w celu zagwarantowania ich podstawowych funkcji państwowych, w szczególności w celu ochrony bezpieczeństwa narodowego – w tym działań na rzecz ochrony informacji, których ujawnienie państwa członkowskie uważają za sprzeczne z podstawowymi interesami swojego bezpieczeństwa – oraz w celu utrzymania porządku publicznego, w szczególności w celu umożliwienia prowadzenia postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania (art. 2 ust. 6). Podkreślić należy, że stanowi harmonizację minimalną – zgodnie z jej art. 4 państwa członkowskie mogą przyjmować lub utrzymywać przepisy mające na celu osiągnięcie wyższego poziomu bezpieczeństwa sieci i systemów informatycznych.

Na potrzeby dyrektywy NIS przyjęto (art. 4 pkt 1), że „sieci i systemy informatyczne" oznaczają:

a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a dyrektywy 2002/21/WE;
b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub
c) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a i b w celu ich eksploatacji, użycia, ochrony i utrzymania.

Przez bezpieczeństwo sieci i systemów informatycznych należy rozumieć ich odporność, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazy-