Rozdział I. Konwencja RE o cyberprzestępczości otwarta do podpisu w Budapeszcie dnia 23.11.2001 r.

Pierwszym wiążącym aktem prawa międzynarodowego skierowanym przeciwko cyberprzestępczości jest Konwencja o cyberprzestępczości. Jej zasięg nie ogranicza się jednak jedynie do państw europejskich.

W trwających ponad cztery lata pracach, których efektem była Konwencja o cyberprzestępczości, uczestniczyli nie tylko przedstawiciele większości państw członkowskich RE (w tym Polski), ale również – w charakterze obserwatorów – delegaci ze Stanów Zjednoczonych, Kanady i Japonii, reprezentanci różnych europejskich instytucji oraz niezależni eksperci. Jej celem było stworzenie ram prawnych dla zwalczania cyberprzestępstw o charakterze międzynarodowym. W Konwencji o cyberprzestępczości uregulowano wiele nowatorskich (oczywiście jak na owe czasy – trzeba pamiętać, że od jej powstania upłynęły ponad dwie dekady) rozwiązań. Przewidziano w niej nie tylko postanowienia dotyczące typów cyberprzestępstw. Zobowiązano ponadto państwa członkowskie do wprowadzenia karalności form zjawiskowych i stadialnych oraz rozwiązań umożliwiających pociągnięcie do odpowiedzialności „osób prawnych" oraz jednostek organizacyjnych nieposiadających osobowości prawnej, ale posiadających zdolność prawną (mieszczących się – dla potrzeb Konwencji o cyberprzestępczości – w zakresie pojęcia osoby prawnej). Zawarto w niej szereg nowych środków o charakterze proceduralnym, takich jak zabezpieczenie danych, nakaz dostarczenia danych, przeszukanie i zatrzymanie danych, gromadzenie danych w czasie rzeczywistym oraz przechwytywanie danych dotyczących ruchu[1]. W celu stworzenia możliwości udzielania przez państwa strony wzajemnej pomocy przewidziano utworzenie sieci punk-

[1] Zob. szerzej np. *F. Radoniewicz*, Procedural Provisions in the Convention on Cybercrime, *passim*.

tów kontaktowych funkcjonujących dwadzieścia cztery godziny na dobę przez siedem dni w tygodniu (sieć punktów 24/7)[2].

Konwencja o cyberprzestępczości, analogicznie jak większość aktów prawa międzynarodowego tego rodzaju, tworzy „standard minimalny"[3] w zakresie karalności czynów zabronionych „stypizowanych" w jej przepisach. W związku z tym nie stoi na przeszkodzie, by państwa strony dokonując ich transpozycji do swoich porządków krajowych jej postanowień, przyjęły bardziej restrykcyjne rozwiązania z zakresu zarówno odpowiedzialności karnej, jak i jej podstaw, które Konwencja o cyberprzestępczości ogranicza do umyślności (w obu postaciach zamiaru – bezpośredniego i ewentualnego)[4]. Twórcy Konwencji o cyberprzestępczości podkreślili w preambule, że stanowi ona uzupełnienie (nie zaś konkurencję) funkcjonujących umów międzynarodowych dotyczących cyberprzestępczości (dwu- i wielostronnych) zawartych między państwami członkami RE.

Oczywiste jest, że postanowienia zawarte w aktach prawa międzynarodowego dotyczące prawa karnego materialnego nie mogą być w zasadzie stosowane bezpośrednio, nie są bowiem zazwyczaj normami samowykonywalnymi (ang. *self-executing*) – nie są na tyle precyzyjne, że możliwe byłoby wywiedzenie z nich uprawnień lub obowiązków jednostki, ani na tyle kompletne, by dla ich zastosowania nie zachodziła konieczność transpozycji do prawa krajowego[5].

---

[2] Por. *A. Adamski*, Przestępczość w cyberprzestrzeni, s. 9–11; *R. Tarnogórski*, Konwencja o cyberprzestępczości (red. *M. Madej*, *M. Terlikowski*), s. 207–210; *D. Rowland*, *U. Kohl*, *A. Charlesworth*, Information technology law, s. 325–326; The Palgrave Handbook of International Cybercrime and Cyberdeviance (eds. *T.J. Holt*, *A.M. Bossler*), s. 225–228.

[3] Co podkreślono w pkt 33 *Explanatory Report to Convention on Cybercrime*, czyli swego rodzaju komentarzu (czy uzasadnienia projektu), sporządzonego do Konwencji o cyberprzestępczości przez jej autorów, niestanowiącego jednak wykładni autentycznej (co podkreślono w jego pkt II, wskazując jednocześnie, że może „służyć pomocą przy stosowaniu postanowień Konwencji o cyberprzestępczości"; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm; dostęp 15.7.2023 r.; dalej jako *Explanatory Report*).

[4] *A. Adamski*, Przestępczość w cyberprzestrzeni, s. 17.

[5] Uwagi te nie dotyczą jednak definicji zawartych w art. 1 Konwencji o cyberprzestępczości, które są dostatecznie precyzyjnie i klarownie skonstruowane, by mogły być stosowane bezpośrednio, za wyjątkiem definicji systemu informatycznego (a w zasadzie komputerowego) z uwagi na wątpliwości dotyczące zakresu tego pojęcia – zob. dalsze uwagi). Mogą być jednak stosowane pośrednio jako wskazówka przy wykładni przepisów prawa krajowego mających dokonać ich transpozycji.

Niezaprzeczalną zaletą Konwencji o cyberprzestępczości jest jej otwarty charakter[6] oraz przewidziane w niej klauzule opcyjnie. Umożliwiają one przyjęcie Konwencji o cyberprzestępczości z wyłączeniem niektórych postanowień, dzięki czemu państwa do niej przystępujące mogą, dokonując transpozycji do swoich porządków prawnych, pogodzić jej rozwiązania ze swoją tradycją i kulturą prawną oraz obowiązującymi już innymi unormowaniami[7]. W związku z powyższym do 1.11.2023 r. Konwencja o cyberprzestępczości została podpisana przez wszystkie państwa członkowskie RE, a ratyfikacji nie dokonała jedynie Irlandia. Ponadto Konwencję o cyberprzestępczości podpisały cztery państwa spoza Europy (Kanada, Japonia, Stany Zjednoczone, Republika Południowej Afryki; Stany Zjednoczone, Kanada i Japonia dokonały już ratyfikacji), kolejne zaś dwadzieścia państw (m.in. Australia, Dominikana, Mauritius, Panama, Sri Lanka) przystąpiło do niej (i ją ratyfikowało)[8]. Na marginesie należy dodać, iż wiele państw – nie podpisując Konwencji o cyberprzestępczości – faktycznie czerpało z jej postanowień, tworząc własne regulacje krajowe. Wśród nich można wskazać Egipt, czy Pakistan[9]. Oczywiście obok Konwencji o cyberprzestępczości istnieją inne umowy międzynarodowe o charakterze regionalnym, np. Porozumienie o współpracy w zwalczaniu przestępstw związanych z informacją przetwarzaną cyfrowo Wspólnoty Niepodległych Państw z 2001 r. (ang. *The 2001 Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information*)[10] lub Konwencja Unii Afrykańskiej o cyberbezpieczeństwie i ochronie danych osobowych z 2014 r. (ang. *The 2014 African Union Convention on Cyber Security and Personal Data Protection*)[11], ale zasięg tych regulacji jest nieporównywalnie mniejszy niż Konwencji o cyberprzestępczości[12].

---

6 Otwarty charakter umowy międzynarodowej oznacza możliwość przystąpienia do niej państw niebędących członkami RE. Mogą one przystąpić do Konwencji, jeżeli ich przedstawiciele uczestniczyli w pracy nad nią lub w wyniku otrzymania zaproszenia od Komitetu Ministrów. Aktualnie istnieje tendencja do otwierania konwencji RE dla państw trzecich. Nie budzi wątpliwości, że niektóre konwencje (w tym Konwencja o cyberprzestępczości) byłyby znacznie mniej skuteczne, gdyby ich zasięg ograniczał się do państw członków RE. *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 164. Zob. szerzej *F. Benoit-Rohmer*, *H. Klebes*, Prawo Rady Europy, s. 104–106.

7 Por. *A. Adamski*, Przestępczość w cyberprzestrzeni, s. 9–17.

8 Stan na 1.11.2023 r.

9 *M. Gercke*, Understanding Cybercrime, s. 200.

10 https://cis-legislation.com/document.fwx?rgn=4129 (dostęp 9.11.2023 r.).

11 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (dostęp 9.11.2023 r.).

12 *A. Lavorgna*, Cybercrimes, s. 15–16; Compare Cyber warfare and cyber terrorism (eds. *A.M. Colarik*, *I. Janczewski*), s. 473–474.

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 miały miejsce dwie nowelizacje Kodeksu karnego (nowelizacja z 2004 r. oraz nowelizacja z 2015 r.), których celem było dostosowanie polskich przepisów do postanowień Konwencji.

Konwencja o cyberprzestępczości składa się z preambuły oraz czterech rozdziałów:

1) rozdział I – „Terminologia";
2) rozdział II – „Środki, jakie należy podjąć na szczeblu krajowym";
3) rozdział III – „Współpraca międzynarodowa";
4) rozdział IV – „Postanowienia końcowe".

W rozdziale I, zawierającym jeden artykuł, umieszczono definicje podstawowych pojęć: systemu komputerowego (ang. *computer system*; w polskim tekście Konwencji o cyberprzestępczości błędnie przetłumaczono to pojęcie jako „system informatyczny" – szerzej na ten temat w dalszej części opracowania[13]), danych komputerowych (ang. *computer data*; w polskim tekście Konwencji o cyberprzestępczości przetłumaczonych jako „dane informatyczne"; są to synonimy, stąd można stosować je zamiennie – zob. dalsze uwagi), dostawcy usług (ang. *service provider*) oraz danych dotyczących ruchu (ang. *traffic data*).

Kwestie, będące przedmiotem niniejszego opracowania zostały uregulowane w pierwszej części II rozdziału. Rozdział II Konwencji o cyberprzestępczości składa się z trzech części: dotyczącej prawa karnego materialnego (art. 2–13), proceduralnego (art. 14–21) i problematyki jurysdykcji (art. 22). W części dotyczącej prawa karnego materialnego znalazły się definicje dziewięciu typów cyberprzestępstw, podzielonych na cztery grupy, umieszczonych w czterech tytułach.

Tytuł 1 „Przestępstwa przeciwko poufności, integralności, dostępności danych komputerowych i systemów" otwiera przestępstwo hakingu – umyślnego i bezprawnego uzyskania dostępu do całości lub części systemu komputerowego (art. 2). Możliwe jest ograniczenie karalności tego czynu poprzez wprowadzenie przez państwo sygnatariusza znamienia naruszenia zabezpieczenia

[13] W niniejszym opracowaniu dla określenia „systemu" w rozumieniu Konwencji o cyberprzestępczości – w celu zachowania klarowności przekazu – używany jest termin „system komputerowy". Podkreślić należy, że pojęcia „systemu komputerowego" oraz „systemu informatycznego" istotnie różnią się zakresami przedmiotowymi, co za tym idzie nie można traktować ich jako pojęcia bliskoznaczne i stosować zamiennie. Zob. szerzej rozdz. III § 7, 8 i 13.

lub wystąpienia po stronie sprawcy zamiaru kierunkowego – np. popełnienia przestępstwa w celu zdobycia konkretnych danych komputerowych lub innego „nieuczciwego zamiaru" (ang. *dishonest intent*). Poza tym państwa sygnatariusze mogą ograniczyć odpowiedzialność karną do przestępstw popełnianych w sieci (wymóg, by zaatakowany system komputerowy był połączony z innym systemem), pozostawiając poza zakresem tego przepisu uzyskanie przez sprawcę dostępu do pojedynczego systemu komputerowego w wyniku zdobycia fizycznego dostępu do komputera. W art. 3 Konwencji o cyberprzestępczości przewidziano przestępstwo „umyślnego, bezprawnego przechwytywania 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". Dla przyjęcia odpowiedzialności karnej sprawcy konieczne jest, aby jego zachowanie nosiło cechy bezprawności. W konsekwencji nie można będzie uznać za przestępstwo zachowania osoby inwigilującej wówczas, gdy działa ona w oparciu o uprawnienia nadane przez uczestników przejętej transmisji danych lub na podstawie obowiązujących w tym zakresie przepisów prawa – jak np. w przypadku funkcjonariuszy organów państwa – realizujących czynności mające na celu ściganie przestępstw, czy też zapewnienie bezpieczeństwa.

Analogicznie jak w przypadku nielegalnego dostępu z art. 2 Konwencji o cyberprzestępczości, państwa strony mają wolną rękę w ograniczeniu zakresu kryminalizacji poprzez wprowadzenie warunku istnienia powiązań między inwigilowanym systemem komputerowym i innym (innymi) systemami, co prowadziłoby do kryminalizacji przechwytywania danych jedynie w zakresie sieci, czyli z wyłączeniem sytuacji sprowadzających się do inwigilacji pojedynczych systemów. Dopuszczalne jest również wprowadzenie przez państwa członkowskie warunku odpowiedzialności karnej, polegającego na wystąpieniu po stronie sprawcy „nieuczciwego zamiaru". Artykuł 3 chroni treść komunikacji (ang. *content data*), pozostawiając poza swym zakresem dane związane z komunikacją, tj. tzw. dane dotyczące ruchu (ang. *traffic data*). W art. 4 Konwencji o cyberprzestępczości zobowiązano państwa strony do kryminalizacji „umyślnego, bezprawnego niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych komputerowych". Państwo strona może uzależnić odpowiedzialność karną od wystąpienia skutku w postaci spowodowania przez czyn sprawcy „poważnej szkody". Artykuł 5 Konwencji o cyberprzestępczości przewiduje przestępstwo „umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego poprzez wpro-

wadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych". Państwom stronom pozostawiono swobodę co do doprecyzowania, co należy rozumieć pod pojęciem „poważnego zakłócenia". W ostatnim przepisie dotyczącym cyberprzestępstw będących przedmiotem niniejszego opracowania – art. 6 Konwencji o cyberprzestępczości – zobowiązano państwa strony do poszerzenia zakresu odpowiedzialności karnej także na czynności poprzedzające popełnienie przestępstw z art. 2–5 poprzez kryminalizację czynów dotyczących tzw. narzędzi hakerskich – ich produkcji, udostępniania, rozpowszechniania[14] itd. A zatem w art. 6 ust. 1 lit. a pkt i zobowiązano państwa strony do kryminalizacji bezprawnej i umyślnej „produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania: (...) urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2–5". W art. 6 ust. 1 lit. a pkt ii Konwencji o cyberprzestępczości przewidziano obowiązek kryminalizacji przez państwa strony umyślnych i bezprawnych działań polegających na „produkcji, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania: (...) hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym możliwe jest uzyskanie dostępu do całości lub części systemu komputerowego". Zarówno w przypadku czynów zabronionych opisanych w art. 6 ust. 1 lit. a, jak i w art. 6 ust. 1 lit. b Konwencji o cyberprzestępczości warunkiem pociągnięcia sprawcy do odpowiedzialności karnej jest wystąpienie po jego stronie zamiaru, by narzędzie hakerskie zostało użyte w celu popełnienia czynu zabronionego z art. 2–5. W art. 6 ust. 1 lit. b przewidziano przestępstwo polegające na posiadaniu takiego narzędzia z zamiarem wykorzystania w celu popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2–5. Państwom stronom zapewniono jednocześnie możliwość przewidzenia w tym wypadku „kryterium ilościowego" – uzależnienia odpowiedzialności karnej od posiadania określonej liczby narzędzi[15].

Ponieważ pozostałe czyny zabronione, do których penalizacji zobowiązuje Konwencja o cyberprzestępczości, pozostają poza zakresem niniejszego opracowania, należy się ograniczyć jedynie do skrótowego ich przedstawienia.

---

[14] Udostępnianie, rozpowszechnianie, dystrybucja (rozumiana jako odpłatne rozpowszechnianie) mogą odbywać się poprzez umieszczenie narzędzia w internecie i umożliwienie pobrania go nieokreślonej liczbie użytkowników lub umieszczenie linków prowadzących do stron z takimi narzędziami.

[15] *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 187.

W tytule 2 – „Przestępstwa dotyczące komputerów" – przewidziano dwa przestępstwa przy użyciu komputera, tj. fałszerstwo komputerowe i oszustwo komputerowe.

Kolejny tytuł (tytuł 3 – „Przestępstwa ze względu na charakter zawartych informacji"[16]) zawiera jeden przepis dotyczący przestępstw związanych z pornografią dziecięcą. Drugą kategorią przestępstw, których umieszczanie rozważano w tym tytule, była „mowa nienawiści". O zamieszczeniu przepisów dotyczących wskazanego zagadnienia (jako przestępstw motywowanych rasizmem lub ksenofobią) w odrębnym protokole[17], zamiast w Konwencji o cyberprzestępczości, przesądziło stanowisko przedstawicieli państw członkowskich RE uczestniczących w jej tworzeniu. Uznano bowiem, że różnice konstytucyjnych standardów dotyczących wolności słowa poszczególnych państw członkowskich skomplikowałyby proces przyjęcia wspólnego stanowiska, co doprowadziłoby do zahamowania prac nad Konwencją o cyberprzestępczości, a po jej przyjęciu – utrudniło ratyfikację. Stąd koncepcja umieszczenia postanowień dotyczących tej grupy czynów w odrębnym akcie.

W tytule 4 („Przestępstwa związane z naruszeniami praw autorskich i praw pokrewnych") znalazł się jeden artykuł, w którym na państwa strony nałożono obowiązek rozciągnięcia ochrony prawnoautorskiej utworów na przypadki ich rozpowszechniania czy udostępniania za pośrednictwem systemów komputerowych, czyli kryminalizację „piractwa" komputerowego.

Ostatni tytuł rozdziału 2 części 1 („Inne formy odpowiedzialności i sankcje") zawiera trzy regulacje. W treści art. 11 Konwencji o cyberprzestępczości przewidziano poszerzenie zakresu podmiotowego odpowiedzialności karnej – zobowiązano państwa strony do kryminalizacji form zjawiskowych (w postaci umyślnego podżegania i pomocnictwa) do czynów zabronionych przewidzianych w Konwencji o cyberprzestępczości.

Natomiast w art. 11 ust. 2 odniesiono się do form stadialnych, nakładając obowiązek kryminalizacji usiłowania popełnienia niektórych przestępstw

---

16 Tytuł ten należało przetłumaczyć następująco: „Przestępstwa ze względu na treść" (ang. *Content-related offences*).

17 Protokół dodatkowy do Konwencji RE o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, otwarty do podpisu w Strasburgu 28.1.2003 r. (Dz.U. z 2015 r. poz. 730). Dalej jako Protokół. Wypada w tym miejscu nadmienić, że 12.5.2022 r. do podpisu otwarty został Drugi protokół dodatkowy do Konwencji o cyberprzestępczości dotyczący wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224, dostęp 15.10.2022 r.

(z tym że istnieje możliwość niezastosowania w całości lub części tego przepisu).

W art. 12 Konwencji o cyberprzestępczości została przewidziana konstrukcja odpowiedzialności osób prawnych (i innych jednostek organizacyjnych – zob. wcześniejsze uwagi) za przestępstwa w niej przewidziane, popełnione dla ich korzyści przez dowolną osobę fizyczną, działającą samodzielnie (czyli jako organ monokratyczny) bądź w ramach jej organu zajmującą w niej pozycję wiodącą z uwagi na posiadanie kompetencji do:

1) reprezentacji tej osoby prawnej;
2) podejmowania decyzji w imieniu osoby prawnej;
3) sprawowania wewnętrznej kontroli funkcjonowania tej osoby prawnej.

Rozdział II. Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z 12.8.2013 r. dotycząca ataków na systemy informatyczne

Pierwszą podjętą przez prawodawcę unijnego próbą regulacji problematyki przestępstw komputerowych była nieobowiązująca już decyzja ramowa Rady Nr 2005/222/WSiSW z 24.2.2005 r. w sprawie ataków na systemy informatyczne[1] (dalej jako decyzja ramowa Nr 2005/222)[2]. Jak widać, jest ona stosunkowo świeżej daty, co wynika oczywiście zarówno z nowatorskiego charakteru stanowiących jej przedmiot zagadnień, jak i faktu, że prawo karne zaliczone zostało do III filaru UE, w którym możliwości unijnego prawodawcy ograniczono jedynie do podejmowania wysiłków w kierunku harmonizacji prawa, z pozostawieniem państwom szerokiej swobody w jego stanowieniu. Obrazowo rzecz ujmując – wskazywano cel, nie narzucając sposobu jego osiągnięcia.

Prace nad decyzją ramową Nr 2005/222 podjęto już w 2001 r., w odpowiedzi na tzw. komunikat Komisji o cyberprzestępczości z 2001 r.[3], w którym znalazły się pewne propozycje uregulowań o charakterze materialnym i proceduralnym, przewidzianych do walki z cyberprzestępstwami na szczeblu zarówno krajowym, jak i wspólnotowym. Opisane starania zaowocowały m.in. zaprezentowaniem projektu omawianej decyzji.

---

1 Dz.Urz. UE L Nr 69, s. 67.

2 Oczywiście problematyki cyberprzestępczości dotyczy znaczna liczba aktów prawnych o charakterze niewiążącym – zob. np. *F. Radoniewicz*, Cybersecurity in the European Union Law, s. 73–76.

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.

W art. 1 decyzji ramowej Nr 2005/222 zawarto definicje najistotniejszych pojęć: „systemu informatycznego", „danych komputerowych", „osoby prawnej", „bezprawności" (w zaprezentowanym przez Komisję projekcie decyzji zawarto ponadto definicje „sieci łączności elektronicznej", „komputera", „osoby uprawnionej").

W przepisach art. 2–4 decyzji ramowej Nr 2005/222 nałożono na państwa członkowskie obowiązek kryminalizacji działań polegających na umyślnym uzyskaniu nielegalnego dostępu do całości lub części systemu informatycznego (art. 2), umyślnej i nielegalnej ingerencji w system informatyczny (art. 3), umyślnej i nielegalnej ingerencji w dane (art. 4). Ponadto uregulowano kwestię jurysdykcji (art. 10), zasad odpowiedzialności osób prawnych (art. 8)[4]. Dodatkowo w art. 11 decyzji ramowej Nr 2005/222 zobowiązano państwa członkowskie do korzystania do celów wymiany informacji dotyczących przestępstw w niej określonych z istniejącej sieci operacyjnych punktów kontaktowych dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu (punkty 24/7).

Ograniczona liczba przestępstw określonych w decyzji ramowej Nr 2005/222, konieczność uwzględnienia nowych zagrożeń, a także chęć dostosowania regulacji do nowych inicjatyw UE w dziedzinie cyberbezpieczeństwa i uzupełnienia ich o aktualny i kompleksowy akt dotyczący walki z cyberprzestępczością w celu stworzenia całościowej regulacji tej materii doprowadziła do decyzji o podjęciu prac nad nowym instrumentem prawnym w dziedzinie cyberprzestępczości. Ich efektem jest dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z 12.8.2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady Nt 2005/222/WSiSW[5] (dalej jako dyrektywa Nr 2013/40)[6].

W treści dyrektywy Nr 2013/40/UE zasadniczo powtórzono postanowienia z decyzji ramowej Nr 2005/222, jednocześnie uzupełniając je o szereg nowych rozwiązań. Po pierwsze, przewidziano nowe typy czynów zabronionych (nielegalne przechwytywanie danych komputerowych oraz przestępstwa dotyczące „narzędzi hakerskich"). Po drugie, określono dodatkowe okoliczności obciążające (obok przewidzianych w decyzji ramowej Nr 2005/222, tj. popełnienia

[4] Rozumianych szeroko, analogicznie jak w Konwencji o cyberprzestępczości, czyli również jako jednostki organizacyjne nieposiadające osobowości prawnej, ale posiadające zdolność prawną.

[5] Dz.Urz. UE L Nr 218, s. 8.

[6] Por. *S. Summers*, *C. Schwarzenegger*, *G. Ege*, *F. Young*. The emergence of EU criminal law, s. 238–239; zob. też *A. Savin*, EU Internet law, s. 330–331.

przestępstwa w ramach organizacji przestępczej, w odniesieniu do której przewidziano surowszą sankcję oraz – mającej charakter fakultatywny na gruncie decyzji ramowej Nr 2005/222 – spowodowanie czynem poważnych szkód[7])[8].

Dyrektywa Nr 2013/40 zobowiązuje państwa członkowskie do kryminalizacji zamachów polegających na:

1) umyślnym i bezprawnym uzyskaniu dostępu do całości lub jakiejkolwiek części systemu informatycznego, z zastrzeżeniem by czyn ten był karalny jako przestępstwo, w przypadku gdy został on popełniony z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (tzw. niezgodny z prawem dostęp do systemów informatycznych – art. 3);
2) umyślnym i bezprawnym poważnym utrudnieniu lub zakłóceniu funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (tzw. niezgodna z prawem ingerencja w system – art. 4);
3) umyślnym i bezprawnym usuwaniu, uszkadzaniu, pogarszaniu, zmienianiu lub eliminowaniu danych komputerowych w systemie informatycznym lub czynieniu ich niedostępnymi, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (tzw. niezgodna z prawem ingerencja w dane art. 5);
4) umyślnym i bezprawnym przechwytywaniu środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (tzw. niezgodne z prawem przechwytywanie danych – art. 6 dyrektywy);
5) umyślnym wytwarzaniu, sprzedaży, dostarczaniu w celu użycia, przywozu, rozpowszechnianiu lub udostępnianiu w inny sposób jednego z narzędzi (narzędzi do popełniania przestępstw – tzw. narzędzi hakerskich), tj. programu komputerowego zaprojektowanego lub przystosowanego głównie do celu popełniania przestępstw, o których mowa

[7] Gwoli ścisłości – w art. 7 ust. 2 decyzji ramowej Nr 2005/222 mowa był o spowodowaniu poważnych szkód lub wywarciu wpływu na istotne interesy (uwzględnienie tej okoliczności było fakultatywne), natomiast w art. 9 ust. 4 lit b dyrektywy Nr 2013/40 – o spowodowaniu poważnych szkód.

[8] Zob. szerzej *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 252–253.

w art. 3–6 albo hasła komputerowego, kodu dostępu lub podobnych danych umożliwiających dostęp do całości lub części systemu informatycznego, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi; do pociągnięcia do odpowiedzialności karnej powinien zostać spełniony dodatkowo wymóg, by zachowanie sprawcy miało na celu popełnienie któregokolwiek z przestępstw, o których mowa w art. 3–6 (czyny dotyczące tzw. narzędzi hakerskich – art. 7).

Powyższe postanowienia nakazują kryminalizację opisanych zachowań w formie sprawstwa oraz dokonania. Do pozostałych form zjawiskowych i stadialnych odnosi się art. 8 dyrektywy Nr 2014/30 przewidujący, że podżeganie i pomocnictwo do przestępstw, o których mowa w art. 3–7, było karalne jako przestępstwo (ust. 1), a usiłowanie jedynie w przypadkach czynów z art. 4 i 5. W odniesieniu do problematyki doboru kar dyrektywa Nr 2013/40 zaleca ogólnie, by wszystkie wymienione tam przestępstwa zagrożone były skutecznymi, proporcjonalnymi i odstraszającymi sankcjami o charakterze karnym, ale jednocześnie wprowadzono wymóg, by czyny określone w art. 3–7 dyrektywy Nr 2013/40 (co oznacza, że nie dotyczy on ich usiłowania oraz pomocnictwa i podżegania do nich) podlegały karze w maksymalnym wymiarze nie mniejszym niż dwa lata pozbawienia wolności co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Zobowiązując państwa członkowskie do kryminalizacji zamachów polegających na bezprawnej ingerencji w system informatyczny (art. 4 dyrektywy Nr 2013/40) oraz bezprawnej ingerencji w dane komputerowe w systemie informatycznym (art. 5 dyrektywy Nr 2013/40), przewiduje ona w ich przypadku szereg okoliczności obciążających: popełnienie ich w ramach organizacji przestępczej, w rozumieniu decyzji ramowej Rady Nr 2008/841, niezależnie od tego, jaki wymiar kary w niej przewidziano (art. 9 ust. 4 lit. a dyrektywy Nr 2013/40), spowodowanie poważnej szkody (art. 9 ust. 4 lit. b dyrektywy Nr 2013/40) lub popełnienie czynu przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej (art. 9 ust. 4 lit. c dyrektywy Nr 2013/40), których wystąpienie powinno powodować możliwość orzeczenia wobec sprawcy kary, o górnej granicy nie niższej od pięciu lat pozbawienia wolności. Ponadto w art. 9 ust. 5 dyrektywy Nr 2013/40 nałożono na państwa członkowskie obowiązek wprowadzenia koniecznych rozwiązań, tak aby w przypadkach przestępstw z art. 4 i art. 5 można było uznać – zgodnie z przepisami prawa krajowego – za okoliczności obciążające fakt popełnienia ich przez niewłaściwe użytkowanie danych osobowych innego człowieka w celu uzyskania zaufania osoby trzeciej i wyrządzenie tym samym szkody prawowi-

temu posiadaczowi tej tożsamości (o ile wskazane okoliczności nie zostały już uwzględnione w zakresie innych przestępstw ściganych przepisami prawa krajowego[9])[10].

Podobnie jak Konwencja o cyberprzestępczości, dyrektywa Nr 2013/40 zobowiązuje do zagwarantowania możliwości pociągnięcia osób prawnych do odpowiedzialności za przestępstwa w niej określone (o których mowa w art. 3–8, czyli łącznie z usiłowaniem, podżeganiem i pomocnictwem do czynów wskazanych w art. 8), popełnione na ich korzyść przez jakąkolwiek osobę działającą indywidualnie (jako organ monokratyczny) albo jako członek organu osoby prawnej i pełniącą funkcje kierownicze w ramach tej osoby prawnej na podstawie:

a) upoważnienia do reprezentowania osoby prawnej;
b) upoważnienia do podejmowania decyzji w imieniu osoby prawnej;
c) upoważnienia do sprawowania kontroli w ramach tej osoby prawnej (art. 10).

W art. 12 uregulowano kwestię jurysdykcji. Natomiast w art. 13 zobowiązano państwa członkowskie do zapewnienia istnienia krajowych punktów kontaktowych i korzystania do celów wymiany informacji dotyczących przestępstw w niej określonych z istniejącej sieci operacyjnych punktów kontaktowych dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu.

9 Por. np. The legal regulation of Cyber Attacks (red. *I. Iglezakis*), s. 28–29.

10 Problematyka okoliczności obciążających przewidzianych w dyrektywie Nr 2013/40 została szerzej omówiona w rozdz. V, stąd w tym miejscu ograniczono się do ich wymienienia.