Studia Prawnicze. Rozprawy i Materiały 2016, nr 1 (18) • Studies in Law: Research Papers 2016, No. 1 (18)
ISSN 1689-8052 • e-ISSN 2451-0807

Anna Golonka
prof. nadzw. dr hab., Uniwersytet Rzeszowski

Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne

Wprowadzenie

Nowoczesne technologie informacyjne są nie tylko rzeczywistością, w której żyjemy i której doświadczamy na co dzień, ale wręcz urosły one do rangi symbolu XXI wieku, stając się wyznacznikiem ery rozwijającego się w galopującym tempie postępu technologicznego. Jego osiągnięcie nie byłoby możliwe bez globalnego i w zasadzie niczym nieskrępowanego dostępu do informacji. W żadnym ze współczesnych, cywilizowanych państw nie ma chyba takiego obszaru życia społecznego i gospodarczego, w którym nie byłyby one należycie doceniane. Powszechny dostęp do Internetu i jego zasobów sprzyja w szczególności nawiązywaniu i podtrzymywaniu kontaktów interpersonalnych; tworzeniu, wdrażaniu i rozpowszechnianiu nowych rozwiązań w różnych dziedzinach wiedzy i nauki, czy wreszcie poszerzaniu wiedzy oraz wyrównywaniu szans na rynku pracy. Jednym słowem nowoczesne technologie umożliwiają „normalne" funkcjonowanie w społeczeństwie informacyjnym. Ich niezliczone zalety można by jeszcze długo wyliczać. Atrybuty postępu technologicznego to jednak tylko jedna strona medalu. Drugą bowiem pozostaje wiele zagrożeń, jakie niesie za sobą powszechna informatyzacja życia oraz skala, na jaką są obecnie wykorzystywane systemy informatyczne. Ich ogólnoświatowy zasięg, specyficzny obszar, jaki kreują (przestrzeń wirtualna), jak i same narzędzia służące do budowy i udoskonalania sieci teleinformatycznych stają się coraz częściej przedmiotem przestępstw.

Współczesna literatura na ich określenie zwykła posługiwać się terminem cyberprzestępczość. Jego jednoznaczne zdefiniowanie w praktyce może nastręczać pewnych trudności, a to z racji tego, że niemal każda organizacja i podobnie – legislator danego kraju – postrzega to zjawisko nieco inaczej. Jedni traktują je za swoistą „podkategorię" przestępczości komputerowej, wo-

bec czego w rezultacie uznają, że pojęcie to mieści w sobie te przestępstwa (i mechanizmy prowadzące do ich popełniania), które wymagają użycia Internetu lub innych sieci komputerowych, które, jak się zwykło przyjmować, stają się narzędziem do popełnienia przestępstwa lub jego celem, względnie zostają użyte „do zadań dodatkowych związanych z popełnieniem przestępstwa (na przykład do przechowywania danych o nielegalnej sprzedaży narkotyków)”[1]. Inni natomiast w cyberprzestępczości dostrzegają nowe źródło zagrożeń, dla których „wspólnym mianownikiem” jest specyficzny obszar, w którym są one popełniane, czyli cyberprzestrzeń. Ta ostatnia jest pojmowana jako „świat sprzężonych ze sobą sieci komputerowych”, tworzących nową przestrzeń „tzw. przestrzeń informacyjną wraz z wszelkimi możliwościami jej eksploatacji”[2].

Najogólniej rzecz ujmując, cyberprzestępczość można jednak rozumieć jako „przestępstwa cybernetyczne”, czyli takie, które są popełniane w „przestrzeni cybernetycznej”, a więc przestrzeni: „[…] otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie”[3].

W konsekwencji cyberprzestępczość, w znaczeniu *sensu largo,* obejmuje więc wszelkie typy czynów zabronionych, przy których popełnieniu wykorzystywane są technologie informatyczne oraz czyny skierowane przeciwko danym i systemom informatycznym. W takim więc ujęciu, pojęcie to odnosić można do przestępstw popełnionych przy użyciu nowoczesnych technologii, na których oznaczenie (pomijając w tym miejscu odrębną problematykę związaną z pewnym „zamieszaniem terminologicznym”, jakie panuje w tej kwestii[4]) zwykło się stosować także inne terminy takie, jak np.: „przestępstwa związane z technologią cyfrową”, „przestępstwa związane z technologią przetwarzania informacji” czy „przestępstwa internetowe”[5]. W literaturze proponuje się także niekiedy odwoływanie się w tej kwestii do terminologii uznawanej (niekiedy nietrafnie) za synonimiczną, czyli do określeń takich, jak: przestępczość wirtualna, elektroniczna, e-przestępczość etc.[6] W wąskim znaczeniu, terminowi cyberprzestępczość należałoby jednak nadać nieco bardziej precyzyjne objaśnienie, z zastrzeżeniem wszakże, że równocześnie wy-

---

1 D.L. Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004, s. 25.

2 R. Łukasiewicz, *Rozwój informatyczny a cyberterroryzmu*, [w:] *Wojna z terroryzmem w XXI w.*, red. B. Hołyst, K. Jałoszyński, A. Letkiewicz, Szczytno 2009, s. 110.

3 M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB” 2010, nr 4 (113), http://www.ebib.pl/2010/113/a.php?nowak [dostęp: 7.01.2015].

4 Por. M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 9–15.

5 *Ibidem*.

6 *Ibidem.*

pada zgodzić się ze stwierdzeniami, które podkreślają dynamikę i nieustającą zmienność zjawiska[7]. Można więc przyjąć, że cyberprzestępczość *sensu stricto* obejmuje „przestępstwa komputerowe", wobec czego oznacza ona po prostu ataki na systemy komputerowe i przetwarzane przez nie dane, powodujące ich uszkodzenie, bądź całkowite zniszczenie[8]. Przedrostek „cyber" w każdym wypadku wskazuje na ścisłe powiązanie pewnych typów czynów zabronionych z nowymi technologiami, służącymi do kreowania „przestrzeni informacyjnej" (tj. cyberprzestrzeni), czyli przestrzeni komunikacyjnej tworzonej przez system powiązań internetowych[9].

Konkludując kwestie związane z wątpliwościami etymologicznymi cyberprzestępczości, można uznać, że pojęcie to obejmuje szeroką gamę czynów zabronionych, począwszy od „typowych" przestępstw, popełnianych przy wykorzystaniu sieci informatycznych takich, jak: włamania na konta bankowe, kradzież tożsamości czy oszustwa komputerowe, przez przestępstwa przeciwko ochronie informacji takie, jak: *hacking*, sabotaż komputerowy, spowodowanie szkody w bazach danych itp., aż po wieloaspektowe i ze swej natury złożone przestępstwa gospodarcze. Współcześnie sprawcy tych ostatnich przy ich popełnieniu coraz częściej korzystają z systemów i narzędzi informatycznych, co w połączeniu z ich globalnym zasięgiem, czyni je doskonałymi narzędziami do popełniania nawet najpoważniejszych przestępstw. Najlepszym tego przykładem są przestępstwa określane mianem: *cyber-human trafficing* (w tym jego odmiana: *cyber-sex trafficing*), czyli handel ludźmi, a także przestępstwa seksualne popełniane „w sieci", cyberterroryzm czy – nierzadko ściśle z nim związany – *cyberlaundering* (czyli „cyber"-pranie pieniędzy).

Zagrożenia płynące z cyberprzestępczości – wybrane aspekty kryminologiczne i wiktymologiczne

Pojawienie się nowej kategorii przestępstw związanych z nowoczesnymi technologiami informatycznymi nie może pozostawać bez wpływu także na świa-

---

[7] *Ibidem*, s. 15.

[8] Definicja cyberprzestępczości w wąskim znaczeniu bazuje m.in. na określeniu tego zjawiska zaakceptowanym podczas odbywającego się w Wiedniu w dniach 11–17 kwietnia 2000 r., 10. Kongresu ONZ w sprawie zapobiegania przestępczości i traktowania przestępców (ang. *tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Vienna 2000*), a także nawiązuje do sposobu jej rozumienia zaakceptowanym w projekcie czwartej Rezolucji Parlamentu Europejskiego z dnia 22 stycznia 2001 r., załączonej do Sprawozdania Komisji Specjalnej ds. Przestępczości Zorganizowanej, Korupcji i Prania Pieniędzy (2013/2107(INI)) z dnia 26 września 2013 r. w sprawie przestępczości zorganizowanej, korupcji i prania pieniędzy: zalecenia dotyczące potrzebnych działań i inicjatyw (sprawozdanie końcowe). Por. także: M. Siwicki, *op. cit.*, s. 17.

[9] Por. R. Łukasiewicz, *op. cit.*

towe „trendy" przestępczości, które zarówno z aspektu kryminologicznego, jak i wiktymologicznego wykazują się pewną specyfiką. Jej zaprezentowanie, chociaż w ogólnym zarysie, na łamach niniejszego artykułu, przekraczałoby znacznie jego ramy objętościowe, a i naraziło na słuszny zarzut zbytniego odbiegania od jego zasadniczego tematu, którym w tym przypadku są regulacje międzynarodowe, analizowane pod kątem stopnia dostosowania do nich polskich przepisów karnych.

W tym miejscu wypada zatem jedynie zasygnalizować, że z punktu widzenia uwarunkowań kryminologicznych, cyberprzestępczość jawi się jako zjawisko o wysokiej dynamice, wynikającej z ciągłego udoskonalania technologii informacyjnych, w tym także wprowadzania na rynek nowoczesnych urządzeń służących m.in. do komunikacji elektronicznej. Pewne trudności związane z wykrywaniem przestępstw komputerowych wiążą się ze specyfiką, jaką one wykazują w stosunku do wszelkich innych. W literaturze przedmiotu zwraca się bowiem uwagę na to, że wyraża się ona w szczególnej kategorii podmiotów odpowiedzialnych za takie czyny i związanych z tym problemów dotyczących ustalenia konkretnego sprawcy, a niekiedy także w nietypowych uwarunkowaniach związanych z miejscem popełnienia danego czynu[10]. W odniesieniu do pierwszej ze wspomnianych kwestii, trudności mogą wynikać z hermetyzmu grup hackerskich, spośród których nierzadko „rekrutują się" sprawcy poważniejszych przestępstw internetowych, tudzież z trudności, jakie mogą wiązać się z potrzebą ustalenia, kto konkretnie jest sprawcą danego incydentu komputerowego (zwłaszcza, gdy IP komputera wskazuje na urządzenie niestanowiące własności sprawcy przestępstwa). Inną sprawą pozostaje wskazanie, gdzie został popełniony dany czyn i czy, wobec tego, w danym przypadku konkretna osoba może za niego ponosić odpowiedzialność karną, na podstawie polskich przepisów karnych. W tym względzie z pomocą przychodzą na pewno zasady prawa karnego międzynarodowego wyrażone w art. 109–113 k.k. Niebagatelną kwestią pozostaje także niezwykły dynamizm, nieporównywalny w zasadzie z żadną inną kategorią przestępstw, jaką cechują się przestępstwa przeciwko bezpieczeństwu informatycznemu. Wynika on z bardzo szybkiego postępu w zakresie rozwoju technologii i procesów informatycznych, które wobec tego wymagają „nadążania" za nimi, a co za tym stoi, także umiejętności prognozowania możliwych kierunków rozwoju i potencjalnych zagrożeń, jakie mogą one ze sobą nieść w przyszłości. Przykładowo na gruncie polskim, specjaliści z dziedziny IT zwracają uwagę na niebezpieczeństwo płynące ze strony nowych technologii, głównie urządzeń mobilnych takich, jak tablety i smartfony, których użytkownicy znacznie rzadziej, niż w przypadku tradycyjnych PC-ów,

[10] Por. B. Hołyst, *Kryminologia*, wyd. 9, Warszawa 2007, s. 572.

sięgają po narzędzia służące ochronie ich systemów, a w rezultacie narażają się także na skutki działania cyberprzestępców. Jak wskazują szacunkowe dane, mniej niż 1/3 użytkowników takich urządzeń korzysta w nich z programów antywirusowych, podczas gdy w przypadku „tradycyjnych" komputerów wskaźnik ten wynosi ponad 80%[11].

Jak nie trudno z powyższego wywnioskować, prowadzi to nie tylko do coraz większej liczby nadużyć popełnianych w cyberprzestrzeni, ale i prowokuje potencjalnych amatorów cyberataków do podejmowania aktywności, która może stwarzać nowe, nieznane dotychczas źródła zagrożeń. Odnosi się to zarówno do nowych metod popełniania cyberataków, jak i teoretycznie znanych już, chociaż wykorzystanych odmiennie sposobów ich przeprowadzania. W tym miejscu tytułem przykładu wystarczy wskazać na jeden (ze sporej ilości) cyberzamachów, polegający na wprowadzeniu do systemu zainfekowanego komputera, metodą konia trojańskiego, wirusa powodującego blokadę jego systemu Windows, możliwą do pokonania po wprowadzeniu specjalnego kodu, uzyskiwanego po wysłaniu płatnego smsa zawierającego żądanie odblokowania systemu na numer telefonu podany w komunikacie wyświetlanym na komputerze[12].

Ciągła dynamika zjawiska wymaga zatem stałego monitorowania zarówno bieżących rozwiązań prawnych, jak i podejmowania, albo przynajmniej dostosowywania działań do istniejących zagrożeń. W tym kierunku działania podejmują nie tylko polskie i zagraniczne służby odpowiedzialne za bezpieczeństwo i utrzymanie porządku publicznego, które w swoich strukturach wyodrębniają komórki organizacyjne do spraw przeciwdziałania różnym formom cyberprzestępczości, ale również międzynarodowe i ponadrządowe organizacje, które wykazują zakrojoną na szeroką skalę aktywność na płaszczyźnie prawodawczej. Przykładem krajowych działań na rzecz przeciwdziałania cyberprzestępczości może być powołanie do życia w lipcu 2014 r. Wydziału do walki z Cyberprzestępczością, działającego od 15 lipca 2014 roku przy Biurze Służby Kryminalnej Komendy Głównej Policji, której podstawowym zadaniem jest koordynacja współpracy wszystkich jednostek Policji na polu wykrywania i zwalczania zagrożeń związanych z cyberprzestępczością, a także wsparcie w postępowaniach prowadzonych przez nie w tym zakresie[13]. Innymi

---

[11] A. Mikołajewska, *Cyberprzestępczość. Czym jest i jak się przed nią bronić?*, wiadomosci24.pl, 25.09.2012, http://www.wiadomosci24.pl/artykul/cyberprzestepczosc_czym_jest_i_jak_sie_przed_nia_bronic_244181.html [dostęp: 1.05.2015].

[12] Mowa o blokerze znanym pod nazwą Trojan.Winlock (i wielu jego wariantach znanych pod różnymi nazwami).

[13] Więcej na temat Wydziału do walki z Cyberprzestępczością i genezy jego tworzenia: *(Nie) wirtualne zagrożenie*, oprac. CZAK, na podst. mat. BSK KGP, „Policja", grudzień 2014, nr 12 (117), s. 12.

przykładami są zespoły eksperckie, powoływane przez środowiska naukowe, które służą nie tylko wsparciem w dziedzinie prewencji przed przestępstwami komputerowymi, ale również dostarczają one niezastąpione rozwiązania systemowe w oparciu o cyklicznie sporządzane raporty na temat bezpieczeństwa informatycznego naszego kraju[14]. W ramach systemu ochrony cyberprzestrzeni został powołany Pełnomocnik Rządu ds. Ochrony Cyberprzestrzeni, jak również funkcjonuje Międzyresortowy Zespół Koordynujący ds. Ochrony Cyberprzestrzeni RP (MZKOC), skupiający jednostki administracji rządowej, co w założeniu ma ułatwić koordynację prowadzonych przez nie działań w ramach realizacji wspomnianego wyżej „Programu rządowego"[15].

Jeszcze dalej idące odrębności wykazuje cyberprzestępczość z wiktymologicznego punktu widzenia. Wynika to po pierwsze z tego, że powodując szkody czy zniszczenia w systemach lub bazach danych, przestępstwa takie narażają przede wszystkim na straty materialne użytkowników tych systemów, a popełniane na ogromną skalę, prowadzą również do zachwiania funkcjonowania państwa (np. zamachy na infrastruktury krytyczne) i przy okazji osłabiając zaufanie obywateli do niego. Bezprawne uzyskanie informacji, nierzadko połączone z włamaniami do systemów komputerowych, kradzież danych czy wręcz pozbawione konkretnego celu ataki na systemy komputerowe ze strony hackerów to, według badań przeprowadzonych w firmach amerykańskich, najczęstsze przyczyny strat w ich zasobach informatycznych[16].

Po wtóre jednak, pod pozorem tak zaprezentowanego aspektu wiktymologicznego, kryje się jednak także indywidualna ofiara, a psychologiczne i społeczne konsekwencje popełnionego na niej cyberprzestępstwa, a w rezultacie także i wyrządzone jej krzywdy, mogą niekiedy okazać się znacznie większe niż pojedynczy zamach o lokalnym zasięgu. Wymiar tragedii, do jakich prowadzą przestępstwa przeciwko wolności (*cyber-human trafficing*) w tym wolności seksualnej (*cyber-sex trafficing cybertrafficking*) bywa przecież niejednokrotnie nieporównywalny ze stratami materialnymi, w szczególności jeżeli nie są one nieodwracalne lub nie powodują paraliżu systemów informatycznych na skalę globalną. Żadnego z obszarów tych zagrożeń nie można jednak lekceważyć. Stąd też władze większości państw przywiązują coraz większą wagę do zapewnienia bezpieczeństwa w dziedzinie bezpieczeństwa

[14] Najbardziej znaczącymi instytutami badawczymi w omawianej dziedzinie są m.in.: NASK (Naukowa i Akademicka Sieć Komputerowa) i działający w jego strukturach Zespół CERT Polska (z ang. *Computer Emergency Response Team*) – więcej o jego działalności na stronie: http://www.cert.pl [dostęp: 2.12.2015] czy Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL – więcej na stronie: http://www.cert.gov.pl [dostęp: 2.12.2015].

[15] Por. Rządowy Program w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, bip.msw.gov.pl/download/4/7445/RPOC-24092010.pdf [dostęp: 4.11.2015].

[16] Por. B. Hołyst, *Wiktymologia*, wyd. 4, Warszawa 2011, s. 461.

teleinformatycznego. Przestępczość w świecie wirtualnym i przy wykorzystaniu technologii teleinformatycznych, nawet w ramach najlepiej zorganizowanych struktur, nie może być z powodzeniem zwalczana przez pojedyncze państwo. Bez współpracy na płaszczyźnie międzynarodowej jakakolwiek aktywność wewnątrzpaństwowa w tym względzie w praktyce sprowadzałaby się wyłącznie do planów rzeczywistego ukrócenia omawianego zjawiska. Jego transgraniczny charakter wymaga unifikacji przepisów materialnych i procedur stosowanych przez poszczególne państwa, tudzież dobrze zorganizowanej koordynacji działań właściwych służb i organizacji powołanych do zwalczania przestępstw popełnianych w cyberprzestrzeni. Z tego powodu także istotne znaczenie mają wysiłki podejmowane od wielu lat przez społeczność międzynarodową. Przybierają one postać rozwiązań prawnych, które z punktu widzenia ich wagi dla polskiego ustawodawstwa, w szczególności karnego, zdają się zasługiwać na szczególną uwagę.

W tym miejscu wypadałoby w pierwszym rzędzie wskazać na: decyzję ramową Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[17], decyzję ramową Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych[18], dyrektywę Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującą decyzję ramową Rady 2004/68/WSiSW[19], czy wreszcie stosunkowo niedawno przyjętą przez Parlament Europejski dyrektywa Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne[20]. Ta ostatnia zastąpiła wspomnianą wyżej decyzję ramową Rady 2005/222/WSiSW, dostosowując jej postanowienia do aktualnego stanu zagrożeń płynących ze strony hackerów komputerowych. Zasadniczym aktem o znaczeniu międzynarodowym w omawianym względzie pozostaje natomiast Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie w dniu 23 listopada 2001 r. i podpisana przez 44 państwa[21]. Warto poświęcić jej nieco więcej uwagi, a to z racji jej stosunkowo niedawnej ratyfikacji przez nasz kraj i przeanalizować

[17] Dz.U. UE.L z 2005 r., Nr 69, s. 67.

[18] Dz.U. UE.L z 2008 r., Nr 328, s. 55.

[19] Dz.U. UE.L z 2011 r., Nr 335, s. 1.

[20] Dz.U. UE.L z 2013 r., Nr. 218, s. 8.

[21] Lista państw-sygnatariuszy Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. według danych z października 2014 r. dostępna na stronie: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [dostęp: 11.01.2015].

przewidziane w niej zapisy pod kątem stopnia dostosowania do nich polskich regulacji karnych[22]. Co więcej, na ten akt prawny powołuje się także ustawodawca wspólnotowy w dyrektywie 2013/40/UE z dnia 12 sierpnia 2013 r.

Warto zatem pokusić się o ocenę stanu implementacji, do krajowego porządku prawnego, unormowań zawartych w tej ostatniej zwłaszcza, że w myśl art. 16 dyrektywy 2013/40/UE, datę jej stosowania określono na dzień 4 września 2015 r.[23]

Analiza postanowień przewidzianych w powyższych regulacjach pozwoli nie tylko na ustalenie w jakim stopniu chronione są polskie systemy informatyczne, z punktu widzenia aktualnych standardów międzynarodowych wyznaczonych przez pryzmat m.in. wspomnianych wyżej aktów prawnych, ale także na tej podstawie wysunięcie postulatów wprowadzenia pewnych zmian do krajowych przepisów karnych.

Karnomaterialne regulacje przewidziane w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. a polskie przepisy karne

W dniu 12 września 2014 r. uchwalona została ustawa o ratyfikacji przez Rzeczpospolitą Polską Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r., która, po jej podpisaniu przez Prezydenta RP w dniu 28 października 2014 r., zaczęła obowiązywać od dnia 19 listopada 2014 r. Przewidziane w niej zapisy odwołują się do pewnych kategorii przestępstw, które w większości przypadków są już penalizowane przez polskiego ustawodawcę albo w kodeksie karnym, albo w przepisach karnych innych ustaw. Wspomniana Konwencja swoim zakresem obejmuje bowiem zachowania stypizowane przede wszystkim w rozdziałach XXXIII, XXXIV, XXV k.k. (obejmujących – odpowiednio: przestępstwa przeciwko ochronie informacji, przestępstwa przeciwko wiarygodności dokumentów, przestępstwa przeciwko wolności seksualnej i obyczajności), a także w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[24].

Wymienione kategorie przestępstw obejmują więc zarówno czyny skie-

---

[22] W dniu 19 listopada 2014 r. weszła w życie ustawa ratyfikująca tę konwencję – por. ustawa z dnia 12 września 2014r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (Dz.U. 2014, poz. 1514). Więcej informacji oraz tekst ustawy są dostępne także na stronie internetowej Sejmu, http://www.sejm.gov.pl/sejm7.nsf/komunikat.xsp?documentId=467CA4B8C53D6D38C1257D-870036D1E0 [dostęp: 15.01.2015].

[23] Data rozpoczęcia stosowania: 4.09.2015 r. Por. http://ec.europa.eu/atwork/pdf/cwp_2015_legislation_pl.pdf.

[24] Tekst jedn. Dz.U. z 2006 r., Nr 90, poz. 631 ze zm.

rowane bezpośrednio przeciwko danym i systemom informatycznym (dla których przedmiotem czynności wykonawczej są zarazem dane przetwarzane w tych systemach), jak z inne przestępstwa, w których technologie informatyczne służą jedynie jako środek (sposób) ich popełnienia. Ich cechą wspólną, jak już zasygnalizowano, jest to, że posiadają one swoje „odpowiedniki" w polskich przepisach karnych. Uważna analiza zapisów przewidzianych w Konwencji dowodzi jednak, że nie we wszystkich aspektach pozostają one w zgodzie z treścią krajowych unormowań.

Uwaga ta w pierwszej kolejności odnosi się do zachowań bezprawnych uregulowanych w art. 3–6 tytułu I Konwencji Rady Europy o cyberprzestępczości: „Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów". W art. 3 tego aktu opisane zostało zachowanie polegające na nielegalnym przechwytywaniu niepublicznej transmisji danych informatycznych z, do lub w ramach systemu informatycznego (włącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przesyłającego takie dane) za pomocą technicznych urządzeń. W polskim k.k., poza samym nielegalnym uzyskaniem dostępu do informacji (art. 267 § 1 k.k.), penalizowane jest także bezprawne niszczenie, uszkadzanie, usuwanie, zmiana, albo utrudnianie dostępu do danych informatycznych, czy też w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych (art. 268a k.k.), jak również zachowanie polegające na zakłócaniu w istotny sposób pracy systemu komputerowego lub sieci teleinformatycznej, m.in. przez transmisję danych informatycznych (art. 269a k.k.). Wypada uznać, że opisane w nich zachowania „tworzą zrąb" czynu opisanego w art. 3 Konwencji. Ten ostatni jednak nie zakłada potrzeby zakłócenia w istotny sposób bezprawnym zachowaniem pracy systemu komputerowego lub sieci teleinformatycznej. W tym zakresie prawodawca polski poszedł o krok dalej wymagając swoistego skutku, jednocześnie pomijając okoliczność, że „przejęcie danych" (tj. ich przechwycenie – ang. *interception*) nie jest pojęciem tożsamym z zakłóceniem (może za tym przemawiać chociażby fakt uregulowania w art. 5 Konwencji zakłócania pracy systemu – *system interference*)[25]. Takie podejście może zaś prowadzić do wniosku, że samo bezprawne przechwytywanie niepublicznej transmisji danych informatycznych pozostaje poza zakresem uregulowania k.k. Zastrzeżenie takie ma wszakże charakter bardziej postulatu precyzji językowej, bowiem w praktyce wiąże się ono na ogół z zakłóceniem pracy systemu kom-

[25] Konwencja o cyberprzestępczości w świetle art. 5 poleca uznawać, że zakłócanie pracy systemu to zachowanie polegające na utrudnianiu bez uprawnienia prawidłowego funkcjonowania systemu komputerowego (*hindering without right of the functioning of a computer system*).

puterowego lub sieci teleinformatycznej. Natomiast z całą pewnością polski ustawodawca nie przewidział potrzeby wskazania, że zachowanie sprawcy ma nastąpić za pomocą środków/urządzeń technicznych (*by technical means*)[26]. W tym względzie wypadałoby zatem wprowadzić do k.k. odpowiedni zapis, aby pozostać w zgodzie z treścią zapisu przewidzianego w art. 3 Konwencji.

Z kolei w art. 4 Konwencji o cyberprzestępczości (i podobnie w art. 8 lit. a tej Konwencji), nakazujący kryminalizację zachowania polegającego na niszczeniu, wykasowaniu, uszkodzeniu, dokonaniu zmiany albo na usunięciu danych informatycznych, szczególną uwagę przykuwa opis czynności sprawczej, a ściślej dwa spośród kilku alternatywnie ujętych w tym artykule znamion czynnościowych. Odnosi się do terminów „wykasowanie" i „usuwanie", które wspomniana Konwencja wyraźnie odróżnia. Takiego rozróżnienia nie przewiduje natomiast żaden z przepisów k.k., w szczególności zaś tych, które określają przestępstwa przeciwko ochronie informacji. Tym samym pojawia się pytanie o kryminalizację zachowania polegającego na „wykasowaniu danych informatycznych", które w sposób dosłowny nie zostało określone w k.k. Wychodząc z założenia, że w świetle obecnego stanu wiedzy informatycznej „wykasowanie" nie powinno być utożsamiane z „usunięciem" danych, należy uznać, że zachowanie sprawcy, polegające na „wykasowaniu danych", które nie będzie prowadziło do ich usunięcia lub zmiany, ani nie spowodowuje realnego utrudnienia w dostępie do nich, pozostanie poza zakresem kryminalizacji k.k. Zasadnym wydaje się zatem uwzględnienie tego znamienia w treści obowiązujących przepisów k.k., w szczególności w art. 268a i 269 k.k.

Art. 6 omawianej Konwencji Rady Europy, w którym zostało opisane bezprawne zachowanie, polegające na umyślnym podjęciu wymienionego w tym przepisie zachowania (tj. produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, a także dystrybucji lub innego udostępniania) w stosunku do urządzeń systemu teleinformatycznego (w tym programu komputerowego), a także haseł komputerowych, kodów itp. danych „w celu ich wykorzystania" dla potrzeb realizacji innych przestępstw, posiada swój „odpowiednik" w polskim k.k. w art. 269b[27]. Ten ostatni przepis, podobnie zresztą jak i poprzedzający go art. 269a k.k., został dodany ustawą nowelizującą Kodeks karny z dnia 18 marca 2004 r.[28] Porównanie zapisów przewidzianych w Konwencji oraz

[26] W art. 269a k.k. wskazano jedynie na sposób popełnienia opisanego w nim przestępstwa („przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych").

[27] Chodzi o przestępstwa opisane w art. 2–5 Konwencji o cyberprzestępczości (tj. bezprawnego dostępu lub „przechwytywania" danych, bądź naruszenia integralności danych czy systemu teleinformatycznego).

[28] Dz.U. nr 69, poz. 626.

k.k. nasuwa jednak pewne obiekcje związane z odesłaniem zawartym w art. 6 ust. 1a) lit. i Konwencji do czynów zabronionych opisanych w art. 2–5 tej Konwencji, w tym także do jej art. 4. Opisuje on, dla przypomnienia, bezprawny dostęp do informacji. Tymczasem jego „odpowiednik" w polskim kodeksie karnym, czyli art. 269b k.k., odwołuje się w tym względzie jedynie do czynu zabronionego opisanego w § 3 art. 267 tego kodeksu, to jest do zakładania lub posługiwania się urządzeniem podsłuchowym, wizualnym lub innym urządzeniem lub oprogramowaniem w celu bezprawnego uzyskania informacji. Ten ostatni zaś nie posiada swojego odpowiednika w Konwencji o cyberprzestępczości (oczywiście, jeżeli pominąć omawiany art. 6, który nakazuje kryminalizację m.in. udostępniania urządzeń, jednak nie samo ich zakładanie lub posługiwanie się nimi, a w żadnym razie nie wspomina o urządzeniach, o których mowa w § 3 art. 267 k.k., czyli o urządzeniu podsłuchowym, wizualnym lub innym[29]). Co więcej, w świetle Konwencji (umyślnie) podjętym czynnościom na urządzeniach ma towarzyszyć „cel", jakim ma być ich wykorzystanie do popełnienia przestępstwa wskazanego w art. 2–5 Konwencji. Tym samym treść zapisu przewidzianego w art. 6 Konwencji, w odniesieniu do samego bezprawnego udostępniania urządzeń przeznaczonych lub przystosowanych „przede wszystkim dla celów" popełnienia któregokolwiek z przestępstw określonych w 2–5 Konwencji, pozostaje *de lege lata* poza zakresem penalizacji w polskim k.k. Jedynym, logicznie nasuwającym się w tym miejscu rozwiązaniem tego braku spójności pomiędzy obydwoma aktami prawnymi może być próba sięgnięcia po przepis przewidujący odpowiedzialność za pomocnictwo (art. 18 § 3 k.k.). Nie w każdym wypadku jednak, jak się zdaje, będzie to próba zakończona powodzeniem. Nie zawsze bowiem udostepnienie będzie mogło (a już na pewno nie zawsze powinno) zostać uznane za ułatwienie do zakładania czy posługiwania się takim urządzeniem „dla celu" wykonania konkretnego przestępstwa komputerowego.

Odrębną kwestią pozostaje natomiast sama konstrukcja zapisu przewidzianego w art. 6 Konwencji o cyberprzestępczości, która odwołuje się do umyślności zachowania sprawcy, sygnalizując przy tym, że winno ono zarazem cechować się zamiarem zabarwionym (celem działania), co jest zabiegiem legislacyjnym zbędnym, z punktu widzenia polskiej techniki legislacyjnej. Wystarczające byłoby w tym przypadku wskazywanie na kierunkowy charakter tego przestępstwa (działanie „w celu"). Próba obrony poglądu w oparciu o argument, jakoby celowość zachowania miała być odnoszona jedynie do

[29] Konwencja o cyberprzestępczości jedynie powołuje w tej kwestii na istniejące Zalecenie Rady Europy nr R (85) 10, dotyczącego praktycznego stosowania Europejskiej Konwencji o Wzajemnej Pomocy w Sprawach Karnych w odniesieniu do wniosków rekwizycyjnych dotyczących podsłuchu rozmów telefonicznych.

czynności podjętych na urządzeniach, nie zaś na hasłach, czy kodach dostępu gdzie okazuje się chybiona. W ustępie 3 art. 6 Konwencji (w którym *nomen omen* wskazane jest wyłączenie spod odpowiedzialności karnej zachowań nieobjętych celem popełnienia przestępstwa wymienionego w art. 2–5 Konwencji, czyli powtórne, tym razem negatywne zaakcentowanie celu działania) jest bowiem mowa o całym ustępie 1 tegoż artykułu, czyli celowość popełnienia jednego z wymienionych przestępstw obejmuje także jego popełnienie przez uzyskanie dostępu do hasła, kodu dostępu itp.

Ponadto w myśl art. 6 ust. 1b) Konwencji, państwa-sygnatariusze powinny uznać także za bezprawne zachowania polegające na „posiadaniu" urządzeń wskazanych w art. 6 ust.1a lit. i. oraz haseł, kodów etc., o których mowa w art. 6 ust.1a lit. ii Konwencji „z zamiarem ich wykorzystania w celu popełnienia przestępstw opisanych w art. 2–5 Konwencji". W polskim Kodeksie karnym nie istnieje odrębny typ czynu zabronionego, który stanowiłby „odpowiednik" tego przestępstwa. Teoretycznie odpowiedzialność karna za dopuszczenie takiego zachowanie mogłaby być rozważana na płaszczyźnie karalnego usiłowania. Zgodnie z art. 13 § 1 k.k. jednym ze znamion charakteryzujących tę fazę stadialną jest jednak podjęcie przez sprawcę „zachowania bezpośrednio zmierzającego do dokonania" (które oczywiście nie następuje). Jak zwykło się przyjmować w doktrynie i judykaturze prawa karnego, owa „bezpośredniość" zachowania zmierzającego do dokonania pozwala zarazem na „odgraniczenie" (zazwyczaj niekaralnego) przygotowania od usiłowania[30]. Odnosząc te uwagi do zapisu przewidzianego w art. 6 ust. 1b Konwencji Rady Europy z dnia 23 listopada 2001 r. wypada przyjąć, że samo posiadanie (nawet jeżeli towarzyszy mu zamiar jego wykorzystania w przyszłości w celu popełnienia określonego przestępstwa) nie może zostać uznane za karalne usiłowanie, przynajmniej tak długo, jak długo dana osoba nie podejmie zachowania pozwalającego na uzasadnione stwierdzenie, iż zmierza ona do realizacji tego celu. W tym względzie wydaje się zatem, że polski ustawodawca karny w aktualnym stanie prawnym nie wypełnia postanowień omawianej Konwencji.

Analizowana Konwencja Rady Europy, poza przestępstwami przeciwko poufności, integralności i dostępności danych informatycznych i systemów, zawiera również zapisy dotyczące przestępstw komputerowych (art. 7 i 8), przestępstwa związane z pornografią dziecięcą (art. 9), a także przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych (art. 10).

[30] Por. A. Zoll, [w:] *Kodeks karny. Część ogólna. Komentarz LEX*, t. I: *Komentarz do art. 1–116 k.k.*, red. A. Zoll, wyd. 4, Warszawa 2012, s. 251–254.

Art. 7 Konwencji reguluje przestępstwo polegające na umyślnym i bezprawnym dokonaniu zmian, wykasowaniu lub usuwaniu danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane jako autentyczne w celach zgodnych z prawem. W świetle wspomnianego art. 7 odpowiedzialność karna nie jest przy tym uzależniona od tego, czy dane takie są możliwe do bezpośredniego odczytania i są one zrozumiałe dla odbiorcy. W polskim kodeksie karnym brak jest typu czynu zabronionego, który odpowiadałby zaprezentowanemu opisowi zachowania. Penalizowane jest samo dokonywanie zmian, niszczenie, uszkadzanie lub usuwanie zapisu istotnej informacji (utrudniające zresztą, czego nie wymaga Konwencja, zapoznanie się z jego treścią osobie uprawnionej) – art. 268 k.k. oraz tzw. sabotaż komputerowy – art. 269 k.k. (obejmujący jednak wyłącznie pewną kategorię danych o szczególnym znaczeniu dla państwa). Żaden z przepisów k.k. nie uzależnia jednak odpowiedzialności sprawcy od zamiaru wykorzystania powstałych w ten sposób nieprawdziwych danych jako autentycznych. Ustawodawca karny nie wiąże zatem czynności na danych informatycznych z fałszem. Z kolei przestępstwo tzw. fałszu materialnego (art. 270 § 1–3 k.k.) czyni za przedmiot dokument, którym zgodnie z art. 115 § 14 k.k. może być również zapisany nośnik informacji. Zatem jedynie czynności podjęte na nośniku informacji, polegające na podrobieniu lub przerobieniu zapisanych na nim danych będą stanowiły fałszerstwo, o którym mowa w art. 270 k.k. Natomiast chcąc pozostać w pełnym zakresie w zgodzie z postanowieniami Konwencji o cyberprzestępczości należałoby rozważyć wprowadzenie dodatkowego przepisu, określającego jako odrębny typ czynu zabronionego „fałszowanie danych informatycznych". Przepis ten mógłby przybrać następujące brzmienie: „Kto w zamiarze użycia jako autentyczne w tym celu niszczy, uszkadza, usuwa lub zmienia dane informatyczne, podlega karze…". Pojęcie „dane informatyczne" zostało w tym przypadku użyte w znaczeniu, jakie temu określeniu nadaje Konwencja o cyberprzestępczości, czyli zgodnie z jej art. 1 lit. b) obejmuje ono: „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny".

Z kolei art. 8 Konwencji reguluje kwestie dotyczące odpowiedzialności za tzw. oszustwo komputerowe. W myśl tego artykułu, kryminalizowane winno być zachowanie polegające na umyślnym i bezprawnym spowodowaniu utraty majątku przez inną osobę poprzez wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych, względnie jakąkolwiek inną ingerencję w funkcjonowanie systemu komputerowego, o ile podjęte jest ono z zamiarem oszustwa „lub nieuczciwym zamiarem" uzyskania korzy-

ści ekonomicznych dla siebie lub innej osoby. Odpowiadający temu opisowi typ czynu zabronionego jest uregulowany w art. 287 k.k. Określone w tym przepisie przestępstwo oszustwa komputerowego w pełni dostosowuje polskie przepisy karne do wymagań wynikających z omawianego aktu prawa międzynarodowego.

Art. 9 Konwencji o cyberprzestępczości znajduje odzwierciedlenie w polskich przepisach karnych w art. 202 § 1–5 k.k. Po zmianie ustawami nowelizującymi k.k. z dnia 27 lipca 2005 r. oraz z dnia 24 października 2008 r., do art. 202 dodane zostały §§ 4 a i b, a następnie zmieniona treść § 4a[31], zaś za sprawą nowelizacji z dnia 4 kwietnia 2014 r. do artykułu tego został dodany § 4c[32]. Statuują one typy czynów zabronionych, zwane potocznie przestępstwami „pornograficznymi", popełnione na szkodę małoletniego. W odróżnieniu od polskiego ustawodawcy, omawiany akt prawny, wypracowany na forum Rady Europy, podaje definicję „pornografii dziecięcej", przez którą poleca on rozumieć: „[…] materiał pornograficzny, który w sposób widoczny przedstawia:

a) osobę małoletnią w trakcie czynności ewidentnie seksualnej,
b) osobę, co do której może zachodzić przypuszczenie, że jest małoletnia w trakcie czynności ewidentnie seksualnej,
c) realistyczny obraz prezentujący osobę małoletnią w trakcie czynności ewidentnie seksualnej" (art. 9 ust. 2 Konwencji).

Zastrzec przy tym należy, że za osobę małoletnią wspomniana Konwencja uznaje osobę, która nie ukończyła 18 roku życia, z tym, że dopuszcza możliwość obniżenia granicy wiekowej do lat 16 przez ustawodawców państw sygnatariuszy Konwencji.

Polski legislator w aktualnym stanie prawnym penalizuje powyższe czyny popełnione na szkodę małoletniego bez dalszego doprecyzowania w tym względzie. Pomijając spory, jakie na łamach literatury prawniczej prowadzone są od lat w odniesieniu do sposobu rozumienia tego terminu[33], wolno w tym

---

[31] Ustawa z dnia 27 lipca 2005 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. Nr 163, poz. 1363) oraz ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. Nr 214, poz. 1344).

[32] Ustawa z dnia 4 kwietnia 2014 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2014 r. poz. 538).

[33] Por. art. 1 § 1 i 2 ustawy z dnia 26.10.1982 r. o postępowaniu w sprawach nieletnich (tekst jeden. Dz.U. z 2014 r., poz. 382 ze zm.); V. Konarska-Wrzosek, [w:] P Górecki, V. Konarska-Wrzosek, *Postępowanie w sprawach nieletnich. Komentarz*, Warszawa 2015, s. 32–36; A. Krawiec, *Małoletni pokrzywdzony w polskim procesie karnym*, Toruń 2012, s. 113; M. Filar, *Polityka kryminalna czy polityka? (Nowelizacja Kodeksu karnego w zakresie przestępstw seksualnych)*, [w:] *Węzłowe problemy prawa karnego, kryminalnego i polityki kryminalnej*, red. V. Konarska-Wrzosek, Warszawa 2010, s. 853–854; J. Warylewski, *Przestępstwo uwiedzenia małoletniego*, „Palestra" 2008, nr 9–10, s. 54.

miejscu uznać, że status taki będzie posiadała osoba, która nie ukończyła 18 lat, czyli jest niepełnoletnia w rozumieniu art. 10 k.c. W wyniku nowelizacji k.k. ustawą z dnia 4 kwietnia 2014 r. usunięto niedociągnięcie legislacyjne istniejące w omawianej kwestii, a polegające na zawężeniu przedmiotu czynności wykonawczej przestępstw określonych w art. 202 § 2, 4 oraz 4a do małoletniego, który nie ukończył 15 lat[34]. Takie rozwiązanie pozostawało w ewidentnej sprzeczności z zaprezentowanymi wyżej postanowieniami Konwencji o cyberprzestępczości. Warto odnotować również, że wraz z wprowadzeniem § 4c do art. 202 k.k., aktualnie penalizowane jest również zachowanie polegające na uczestniczeniu w prezentacji treści pornograficznych z udziałem małoletniego w celu zaspokojenia seksualnego. W połączeniu z § 4b tego przepisu, czyni od zadość postulatom dotyczącym dostosowania krajowych rozwiązań prawnokarnych do wymagań płynących z obowiązujących aktów prawa międzynarodowego[35].

Ostatnią kategorią cyberprzestępstw opisanych w Konwencji Rady Europy z dnia 23 listopada 2001 r. są przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych, które w polskim prawie uregulowane zostały przede wszystkim w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[36]. Zgodnie z art. 10 Konwencji, państwa–Strony w krajowych regulacjach powinny przewidzieć wprowadzenie karalności umyślnie podjętego zachowania polegającego na naruszeniu prawa autorskiego oraz praw pokrewnych (pojmowanych w sposób określony w jego prawie wewnętrznym) za pomocą systemu teleinformatycznego i podjętego na skalę komercyjną[37].

---

[34] W tej sprawie na etapie projektu wprowadzenia zmian do k.k. – por. M. Płachta, *Opinia w sprawie projektu ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń z 12 stycznia 201 r. (Sejm IV kadencji, druk nr 2031)*, sporządzona w Gdańsku, dnia 12.01.2004 r., s. 7, http://orka.sejm.gov.pl/rexdomk4.nsf/($All)/4FC60869D85A3A73C1256E0B0047EE25/$File/I2677-03b.rtf?OpenElement [dostęp: 21.11.2015].

[35] Por. A. Adamski, *Opinia na temat Rządowego projektu dostosowania polskiego kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości*, s. 4–5. – PROSZĘ O DANE CYTOWANIA!!!

[36] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, tekst jedn. Dz.U. z 2006 r., Nr 90, poz. 631 ze zm.

[37] Poza Konwencją o cyberprzestępczości z 2001 r., zobowiązania wynikające z potrzeby zapewnienia ochrony praw autorskich wynikają także z innych aktów międzynarodowych, w tym przede wszystkim z: Aktu Paryskiego z dnia 24 lipca 1971 r., zmieniającego Konwencję Berneńską o ochronie dzieł literackich i artystycznych, Porozumienia w sprawie handlowych aspektów praw własności intelektualnej, sporządzonego w Marrakeszu dnia 15 kwietnia 1994 r. (Dz.U. z 1996 r., Nr 32, poz. 143), Traktatu Światowej Organizacji Własności Intelektualnej o prawach autorskich, sporządzonego w Genewie w dniu 20 grudnia 1996 r., Międzynarodowej Konwencji o ochronie wykonawców, producentów fonogramów organizacji nadawczych, zawartej w Rzymie, dnia 26 października 1961 r. (tzw. Konwencja Rzymska),

W odniesieniu do tej kategorii czynów, uwagę zwraca przede wszystkim bardzo ogólne sformułowanie czynności sprawczej, przez co z jednej strony, jak się wydaje bez trudu sprostać można wymaganiom dotyczącym usankcjonowania odpowiednich czynów przez krajowe przepisy karne, z drugiej jednak, powstaje wątpliwość czy określone w ustawie z dnia 4 lutego 1994 r. typy czynów zabronionych wyczerpują znamię „naruszenia", wobec czego, czy przewidują odpowiedzialność za każdy możliwy sposób prowadzący do naruszenia praw autorskich i pokrewnych? Wydaje się, że odpowiedź na to pytanie będzie jednak negatywna. Najlepszym przykładem zachowania nieposiadającego jasnego statusu prawnego (jako zachowania karalnego), pomimo że z moralnego punktu widzenia niewątpliwie wysoce nagannego, a przy tym dającego się zakwalifikować jako prowadzące do naruszenia prawa autorskiego jest *ghostwriting,* czyli wykonanie przez jedną osobę na zlecenie innej utworu (np. publikacji naukowej, tekstu do utworu muzycznego, sprawozdania etc.), której autorstwo następnie przypisuje sobie osoba, na zlecenie której powstał utwór, a także pewne jego odmiany np. *ghost authorship* (przy współautorstwie – pominięcie jednego/pewnych autorów) lub *honorary authorship* (powołanie jako autora osoby, której faktycznie nie można uznać za autora części opracowania, jednak z uwagi na jej wkład finansów figuruje ona jako jeden z autorów utworu). W dobie coraz powszechniejszego wykorzystania Internetu do publikacji utworów, zachowania takie stają się zarazem naruszeniem prawa autorskiego, bądź praw pokrewnych, o czym mowa w art. 10 omawianej Konwencji.

Po wtóre, warto odnotować również, że w art. 10 Konwencji mowa jest o systemie informatycznym, co – zgodnie z legalną definicją tego pojęcia, podaną w art. 1 lit. a) tego aktu prawa międzynarodowego, oznacza: „każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych". Warto byłoby natomiast rozważyć posłużenie się w tym przypadku określeniem funkcjonującym na gruncie rodzimych przepisów, czyli w szczególności ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[38], a więc odnoszącym się do „systemu teleinforma-

Porozumienia w sprawie handlowych aspektów praw własności intelektualnej (TRIPS – ang. *Agreement on Trade-Related Aspects of Intellectual Property Rights*), Dz.U. z 1996 r., Nr 32, poz. 143, stanowiącego zał. 1C do porozumienia w sprawie utworzenia Światowej Organizacji Handlu WTO, podpisanego w Marrakeszu dnia 15 kwietnia 1994r. (opublikowane w Dz.U. z 1995 r., nr 98, poz.483) oraz Traktatu Światowej Organizacji Własności Intelektualnej o wykonaniach i fonogramach, sporządzony w Genewie, dnia 20 grudnia 1996 r., Dz.U. z 2003 r., Nr 41, poz. 375 (Konwencja zastrzega, iż nie dotyczy to praw osobistych przewidzianych przez powyższe Konwencje).

[38] Tekst jedn. Dz.U. z 2013 r., poz. 1422 ze zm.

tycznego". Zgodnie z art. 2 pkt. 3 tej ustawy, pod tym pojęciem należy rozumieć: „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800, ze zm.)".

Jeszcze inną kwestią pozostaje natomiast samo sformułowanie użyte w art. 10 Konwencji, odnoszące się do „skali komercyjnej" (ang. *on a commercial scale*), na jaką mają być popełnione czyny opisane w tym artykule. Nie jest bowiem jasne, czy chodzi w nim o ograniczenie tych czynów do obrotu gospodarczego[39], czy też o aspekt związany z profesjonalnym charakterem podmiotów dopuszczających się ich popełnienia, czy może o ich wymiar na masową skalę, co zresztą wydaje się być interpretacją pozostającą w zgodzie z *ratio legis* tego przepisu. Wydaje się, że ten ostatni aspekt jest jednak nie do pominięcia, bowiem w przeciwnym wypadku, gdyby chodziło o sam związek czynu z działalnością gospodarczą (obrotem gospodarczym), prawodawca międzynarodowy wskazałby na to wyraźnie w treści art. 10 Konwencji. Z drugiej strony przymiotnik „komercyjny" nie pozwala na oderwanie czynu opisanego w tym artykule od jego kontekstu, którym ma być w tym wypadku „działalność nastawiona na osiągnięcie zysku".

Karnomaterialną część regulacji zawartych w Konwencji o cyberprzestępczości uzupełniają zapisy przewidujące potrzebę rozszerzenia karalności opisanych wcześniej zachowań bezprawnych także na niesprawcze formy przestępnego współdziałania, uwzględnienie odpowiedzialności za usiłowanie ich popełnienia, określenie zasad odpowiedzialności podmiotów innych niż osoby fizyczne, tudzież usankcjonowanie ich odpowiednimi karami lub środkami karnymi. W tym względzie zadość oczekiwaniom, stawianym przez konwencję o cyberprzestępczości, czynią odpowiednie przepisy przewidziane Kodeksie karnym (w szczególności art. 13 § 1 i 2 oraz art. 18 § 2 i 3), jak również zasady odpowiedzialności podmiotów zbiorowych, uregulowane przede wszystkim w ustawie z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary[40].

---

[39] Przymiotnik „komercyjny', pochodzi od słowa „komercja" i oznacza działalność przynoszącą dochód, nastawioną na osiągnięcie zysku, uzależniającą działanie od ekwiwalentu pieniężnego, por. *Słownik wyrazów obcych PWN*, red. E. Sobol, Warszawa 2003, s. 572.

[40] Tekst jedn. z 2015 r., poz. 1212 ze zm.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. w sprawie ataków na systemy informatyczne i perspektywy implementowania jej postanowień do krajowego porządku prawnego

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r., dotycząca ataków na systemy informatyczne, zastąpiła obowiązującą dotychczas w tym zakresie decyzję ramową Rady 2005/222/WSiSW. Powyższa dyrektywa obowiązuje od dnia 4 września 2013 r., a zasadniczym powodem jej uchwalenia było wzmocnienie współpracy między organami państw członkowskich UE, powołanymi do ochrony bezpieczeństwa systemów informatycznych, a także wyspecjalizowanymi agencjami i organami Unii, takimi jak Eurojust, Europol i należące do niego Europejskie Centrum ds. Walki z Cyberprzestępczością oraz Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz ustanowienie pewnych minimalnych zasad dotyczących definicji i istoty przestępstw godzących w takie systemy. Ponadto uchwalenie tej dyrektywy ma służyć uzgodnieniu pewnych minimalnych standardów dotyczących odpowiedzialności za ich popełnienie[41]. Warto również odnotować, że dyrektywa 2013/40/UE stanowi odpowiedź na potrzebę dostosowania regulacji prawnych do podlegającego stałemu przeobrażaniu obliczu cyberprzestępczości. Jak trafnie zauważyli jej twórcy, wraz z pojawieniem się nowych źródeł zagrożeń, konieczne staje się również zapewnienie należytej ochrony przed takimi czynami na płaszczyźnie legislacyjnej. Najlepszym tego przykładem jest coraz powszechniejsze wykorzystywane „botnetów" do przeprowadzania ataków na systemy informatyczne. „Botnet" – to inaczej grupa komputerów zainfekowanych przez „boty", czyli złośliwe oprogramowania (np. robaki), które umożliwiają zdalne kontrolowanie komputera należącego do innego użytkownika. Stąd też zainfekowany komputer bywa nazywany „zombie", na wzór „żywego trupa" jakim staje się on wówczas, gdy użytkownik traci nad nim kontrolę[42]. Bowiem w tym przypadku inna osoba (cyberprzestępca) zarządza faktycznie bonetem. Botnety są współcześnie wykorzystywane do rozsyłania spamu czy rozprzestrzeniania wirusów, ale równie często stanowią one narzędzie w rękach sprawców takich przestępstw, jak np.

---

41 Por. dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. w sprawie ataków na systemy informatyczne, Dz. Urz. WE L z dnia 14.08.2013 r., Nr 218, s. 8.

42 Więcej o tym, co to jest „botnet" i jak się przed nimi chronić, por. *Co to jest botnet i dlaczego jest niebezpieczny?* Gazeta.pl. Technologie z dnia 19 lutego 2009 r., http://technologie.gazeta.pl/technologie/1,81010,6295156,Co_to_jest_botnet_i_dlaczego_jest_niebezpieczny_.html [dostęp: 2.12.2015].

kradzież tożsamości (w tym *spoofing,* czyli bezprawne podszywanie się pod innego użytkownika system), kradzież haseł i innych danych, oszustwa komputerowe, *sniffing*, czyli „śledzenie" ruchów w sieci innego użytkownika itp.[43]

Istota zachowań bezprawnych, określonych w dyrektywie z dnia 12 sierpnia 2013 r., w dużej mierze, zresztą zgodnie z deklaracją uczynioną w jej Preambule, nawiązuje do postanowień Konwencji o cyberprzestępczości z 2001 r. Opisy czynów zabronionych pokrywają się w znacznej mierze z tymi, jakie przewiduje ta ostatnia. Wspólnotowy akt prawny określa następujące kategorie czynów: bezprawny dostęp do systemów informatycznych (art. 3 dyrektywy), bezprawną ingerencję w systemy informatyczne (art. 4 dyrektywy), bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych (art. 5 dyrektywy), bezprawne przechwytywanie środkami technicznymi niepublicznych przekazów danych (art. 6 dyrektywy), wytwarzanie, sprzedaż, dostarczanie w celu użycia, przywóz, rozpowszechnianie lub udostępnianie w inny sposób programu komputerowego lub hasła komputerowego, kodu dostępu czy innych, podobnych danych umożliwiających dostęp do systemu informatycznego, wykorzystanych w celu popełnienia któregokolwiek ze wspomnianych wyżej przestępstw. Pewną, dostrzegalną różnicą pomiędzy wspomnianą dyrektywą a Konwencją o cyberprzestępczości (pomijając nieistotną chronologię zapisów odnoszących się do poszczególnych przestępstw) jest większa precyzja, jaką wykazał się legislator wspólnotowy w opisie czynności sprawczej przestępstw określonych w art. 4 i 5 dyrektywy. Wskazuje on odpowiednio na: „poważne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi" oraz usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi". Dopuszcza on także bezkarność tzw. „wypadków mniejszej wagi", czego zresztą rodzimy ustawodawca (może i całkiem słusznie) nie przewiduje.

Wzorem zapisów przewidzianych w Konwencji o cyberprzestępczości, unijny prawodawca przewidział również rozszerzenie zasad odpowiedzialności na formy niesprawcze, usiłowanie popełnienia takich przestępstw oraz możliwość ponoszenia odpowiedzialności za nie osób prawnych, na zasadach określonych w wewnętrznym prawie każdego z państw członkowskich.

Warto również odnotować, że „poprzedniczka" ww. dyrektywy, tj. Decyzja ramowa Rady 2005/222/WSiSW, w zakresie penalizacji przestępstwa hackin-

[43] Więcej na ten temat: https://pl.wikipedia.org/wiki/Botnet_%28bezpiecze%C5%84stwo_komputerowe%29 oraz https://www.cybsecurity.org/co-to-jest-botnet-i-dlaczego-nalezy-zachowac-ostroznosc [dostęp: 2.12.2015].

gu, wymagała objęcia zakresem penalizacji zachowań polegających na uzyskaniu nielegalnego dostępu do informacji, podczas gdy polski k.k. przewidywał odpowiedzialność karną za bezprawne uzyskanie informacji przez osobę do tego nieuprawnioną. Zmiana art. 267 k.k., przeprowadzona za sprawą nowelizacji z dnia 24 października 2008 r., doprowadziła do dostosowania w tej mierze krajowych przepisów karnych do wymogów unijnych[44].

Podsumowanie

Obydwa zaprezentowanie wyżej akty prawa międzynarodowego uznawane są aktualnie za kluczowe w walce z cyberprzestępczością. Można zatem śmiało uznać, że stanowią one trzon wyznaczający międzynarodowe standardy karne w tej dziedzinie. Oczywiście należy przy tym mieć na uwadze szeroki katalog innych aktów prawnych, w szczególności inne, niż opisana wyżej dyrektywy UE, rozporządzenia Parlamentu Europejskiego i Rady, Zalecenia Rady Europy itp., obejmujące swoim zakresem materię związaną z dziedziną informacji, bezpieczeństwa powszechnego, komunikacji etc. Ich kompleksowe omówienie na łamach tego opracowania, nawet w największym skrócie, byłoby niemożliwe. Zresztą dla problematyki walki z cyberprzestępczością wydają się mieć one drugorzędne znaczenie. Istotą jest bowiem w tym przypadku odpowiedź na pytanie o to, jakie działania są aktualnie podejmowane na płaszczyźnie międzynarodowej w kontekście zapobiegania temu zjawisku i walki z jego przejawami, w szczególności zaś, jakie rozwiązania prawne są w tej mierze promowane. Z kolei najlepiej o tym świadczą zapisy przewidziane w Konwencji o cyberprzestępczości z 2001 r. oraz jej wspólnotowym „odpowiedniku", jakim jest dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. Ich znajomość pozwala na dokonanie oceny stanu dostosowania polskich przepisów karnych do wymagań dyktowanych obowiązującymi normami prawa międzynarodowego.

Uważna analiza wspominanych regulacji prowadzi do wniosku, że nie w każdym przypadku krajowy ustawodawca karny w pełni pozostaje z nimi w zgodzie, zwłaszcza jeżeli wziąć „pod lupę" Konwencję o cyberprzestępczości z 2001 r. Nakreślona powyżej istota karnomaterialnych regulacji, zawartych w tej Konwencji, i ich porównanie z odpowiednimi przepisami k.k. oraz ustawy o prawie autorskim i prawach pokrewnych wskazują, że pomimo kilku nowelizacji k.k., w jego przepisach nadal istnieją luki lub niedociągnięcia legislacyjne w omawianym względzie. Na ich obecność wskazują uwagi krytycznie poczynione w tym opracowaniu, a także inne działania, szczegól-

[44] Dz.U. Nr 214, poz. 1344.

nie kontrole przeprowadzane na szczeblu państwowym. Jak bowiem podkreśla Najwyższa Izba Kontroli w swoim raporcie, dotyczącym stanu realizacji przez podmioty państwowe „Rządowego projektu ochrony cyberprzestrzeni na lata 2011–2016", „[…] administracja państwowa nie podjęła dotychczas niezbędnych działań, mających na celu zapewnienie bezpieczeństwa teleinformatycznego Polski", a co więcej dążenia do informatyzacji życia publicznego zdają się być odwrotnie proporcjonalne do działań zmierzających do ochrony systemów teleinformatycznych przed ich wykorzystaniem do celu popełnienia przestępstwa. NIK odnotowała szereg nieprawidłowości, wśród których znalazły się m.in. zarzuty dotyczące swoistej ignorancji nowych źródeł zagrożeń, jakie może nieść za sobą stały rozwój i doskonalenie technologii informatycznych, braku opracowania spójnych rozwiązań systemowych, pozwalających na monitorowanie bieżącego stanu zagrożenia systemów teleinformatycznych, w tym zwłaszcza zabezpieczenia infrastruktur krytycznych przed incydentami prowadzącymi do zakłócenia czy wręcz paraliżu pracy całego systemu, niedostateczne przygotowanie procedur reagowania na takie zdarzenia czy wreszcie braków dotyczących realizacji rządowego programu bezpieczeństwa narodowego w zakresie ochrony cyberprzestrzeni[45]. Dokument ten dowodzi najlepiej, że w parze z doskonaleniem polskich regulacji karnych w dziedzinie bezpieczeństwa informacyjnego i ich dostosowaniem do standardów wyznaczonych międzynarodowymi aktami prawnymi, winny iść konkretne działania, zmierzające do ich wcielenia w życie.

Abstract
Cybercrime – international standards in combating this phenomenon and the Polish penal regulation

Subject of this study are issues relating to cybercrime. Starting point seems to be here the attempt to determine way of understanding of this concept. It allows to perform in the next step the dogmatic analysis of criminal law regulations relating to the main issue. Matters discussed in this paper are shown through the comparative legal prism. The aim of such an approach is to demonstrate and evaluate the extent of compliance some of Polish regulations and the acts of international law, which regard cybercrime. The latter in fact shall appoint certain criminal law standards in the field of protection of the information security.

Key words: criminal law, cybercrime, Council of Europe Convention on Cybercrime

[45] Por. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP. Informacja o wynikach kontroli,* https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf [dostęp: 11.11.2015].

Streszczenie
Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne

Przedmiotem niniejszego opracowania są zagadnienia dotyczące cyberprzestępczości. Punktem wyjścia uczyniono w nim próbę wyjaśnienia samego pojęcia cyberprzestępczości, które nasuwa wiele wątpliwości. Zaprezentowano w nim również zagadnienia związane z etiologią zjawiska oraz pewne aspekty wiktymologiczne. Takie podejście umożliwia przeprowadzenie w następnej kolejności analizy dogmatycznej regulacji prawnokarnych odnoszących się do zasadniczej problematyki poruszanej w tym opracowaniu. Jak sygnalizuje to jego tytuł, przedstawiono w nim regulacje międzynarodowe, które, jak zwykło się współcześnie uznawać, wyznaczają standardy w zakresie ochrony systemów informatycznych. Tym samym zagadnienia omawiane w artykule naukowym zostały ukazane przez pryzmat prawnoporównawczy. Celem takiego podejścia było przede wszystkim wykazanie stanu dostosowania polskich regulacji karnych do aktów prawa międzynarodowego i jego końcowa ocena.
Słowa kluczowe: prawo karne, cyberprzestepczość, Konwencja Rady Europy o cyberprzestępczości