Filip Radoniewicz*

Przestępstwa komputerowe w polskim Kodeksie karnym

Streszczenie

Celem artykułu jest analiza przepisów kryminalizujących w polskim prawie zjawisko tzw. przestępstw komputerowych w rozumieniu ścisłym (computer crimes, cybercrimes), czyli takich czynów, w których komputer lub sieć są celem przestępstwa (niejako „ofiarą"; *computer as a target*). Artykuł składa się z trzech części – wstępu, w którym w sposób syntetyczny omówiono najważniejsze kwestie terminologiczne, części głównej, w której przeprowadzono analizę przepisów art. 267–269c Kodeksu karnego z 1997 r., znajdujących się w rozdziale XXXIII, zatytułowanym *Przestępstwa przeciwko ochronie informacji*, w których polski ustawodawca przestępstwa te stypizował oraz zakończenia zawierającego uwagi de lege lata i de lege ferenda.

Słowa kluczowe: cyberprzestępczość, hacking, narzędzia hackerskie, inwigilacja, podsłuch komputerowy

* Dr Filip Radoniewicz, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

Wstęp

Dotychczas w żadnym ustawodawstwie nie zdefiniowano pojęcia, „przestępstwa komputerowego". Oczywiście w nauce prawa karnego nie brakuje definicji tego terminu. Jako jedną z pierwszych można wskazać niezwykle szeroką i pojemną definicję „przestępstwa komputerowego" zaproponowaną przez Ulricha Siebera na spotkaniu ekspertów OECD w Paryżu w 1983 r., użytą następnie w tzw. Raporcie OECD[1], zgodnie z którą „za przestępstwo komputerowe uważa się wszelkie bezprawne, nieetyczne i nieupoważnione zachowania odnoszące się do procesu przetwarzania i (lub) przekazywania danych"[2] . Bardzo ogólną definicję przestępczości komputerowej sformułowano kilka lat później dla potrzeb Interpolu, określając ją jako „przestępczość w zakresie technik komputerowych" i dzieląc na następujące grupy: 1) naruszenie praw dostępu do zasobów; 2) oszustwo przy użyciu komputera; 3) modyfikacja zasobów komputera; 4) powielanie programów; 5) sabotaż sprzętu i oprogramowania; 6) przestępstwa dokonywane za pomocą BBS-ów; 7) przechowywanie zabronionych prawem zbiorów; 8) przestępczość w internecie[3].

W związku z postępem technologicznym ewoluują również pojęcia określające zjawisko przestępczości komputerowej. Najwcześniejsze to oczywiście „przestępstwo komputerowe" (ang. *Computer crime*), „przestępstwo związane z komputerem" (ang. *Computer related crime*), „przestępstwo popełniane za pomocą komputera" (ang. *crime by computer*), „przestępstwo związane z technologią cyfrową" (ang. *Digital crime*; zakres tego pojęcia jest szerszy niż „przestępstwo komputerowe"). Natomiast rozwój internetu w ostatnich latach doprowadził do powstania silnego, praktycznie nierozerwalnego związku między technologią informatyczną i telekomunikacyjną. Dlatego też pojawiło się wiele nowych propozycji terminów i definicji na określenie zjawiska przestępstw komputerowych. Wskazać można „przestępstwa internetowe" (ang. *internet crimes*), „e-przestępstwa" (ang. *e-crimes*), „przestępstwa sieciowe" (ang. *net-crimes*), „wirtualne" (ang. *Virtual crimes*) i wreszcie „cyberprzestępstwa" (ang.

1 Computer-Related Crime. Analysis of legal policy in the OECD Area ICCP Series nr 10, OECD, Paryż 1986. Dokument zawierający wyniki podjętych przez OECD w 1983 r. badań nad możliwością stworzenia międzynarodowych regulacji prawnokarnych dotyczących przestępstw i nadużyć komputerowych.

2 U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society – Comcrime – Study*, Würzburg 1998, s. 20–21; por. R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, Warszawa 1993, s. 52.

3 B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 27–28.

Cyber crimes), „przestępstwa związane z technologią informatyczną" (ang. *IT-crimes*), „przestępstwa związane z przetwarzaniem danych"[4]. Wśród przestępstw komputerowych wyróżnić można pewne grupy: 1) przestępstwa, które nie wymagają, by komputer był podłączony do sieci – obecnie zdarzające się stosunkowo rzadko; 2) przestępstwa, które można popełnić wyłącznie w internecie (przestępstwa internetowe, wirtualne); 3) przestępstwa generalnie związane z nowoczesną technologią, czyli te, które związane są z komputerami i sieciami komputerowymi, ale dotyczą również nanotechnologii czy bioinżynierii[5].

Sformułowaniem, które robi największą karierę, jest zdecydowanie termin „cyberprzestępstwo", używany zarówno w literaturze przedmiotu, jak i w niektórych dokumentach międzynarodowych (w szczególności w Konwencji o cyberprzestępczości).

Na X Kongresie ONZ w sprawie zapobiegania przestępczości i postępowania z przestępcami (*The Tenth United Nation Congress on the Prevention of Crime and Treatment of Offenders*), który odbył się w kwietniu 2000 r. w Wiedniu, uznano, że cyberprzestępstwem jest każde przestępstwo, które może być popełnione za pośrednictwem systemów komputerowych lub sieci, w systemie komputerowym lub sieci albo przeciwko takiemu systemowi lub sieci. Jednocześnie zaproponowano następujący podział cyberprzestępstw: 1) cyberprzestępstwo w wąskim ujęciu (przestępstwo komputerowe): każde nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych i przetwarzanych przez te systemy danych, tj.: a) nieautoryzowany dostęp, b) uszkodzenie komputera, danych lub aplikacji, c) sabotaż komputerowy, d) nieautoryzowane przejęcie komputera, e) szpiegostwo komputerowe; 2) cyberprzestępstwo w szerokim ujęciu (przestępstwo dotyczące komputerów): każde nielegalne działanie dokonane za pomocą lub dotyczące systemów komputerowych lub sieci komputerowych, włączając w to m.in. nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[6].

4 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 32–33. Por. B. Fischer, *Przestępstwa komputerowe...*, s. 23–31; J.W. Wójcik, *Przestępstwa komputerowe. Fenomen cywilizacji*, cz. I, Warszawa 1999, s. 52–57; J. Clough, *Principles of Cybercrime*, New York 2013, s. 9.

5 J. Clough, *Principles of cybercrime...*, s. 9.

6 Por. M. Smarzewski, *Cyberprzestępczość a zmiany w polskim prawie karnym* [w:] I. Sepioło-Jankowska (red.), *Reforma prawa karnego. Księga po Zjeździe Młodych Karnistów*, Warszawa 2014, s. 267; D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004, s. 35–36.

W literaturze stworzono wiele klasyfikacji przestępstw komputerowych. Z uwagi na ograniczenia objętościowe ograniczę się do wskazania dwóch. Po pierwsze najprostszego z możliwych podziału dychotomicznego przestępstw komputerowych na „stare" i „nowe" występki. Przy czym chodzi tu o „nowość" przestępstwa w ogóle (a nie jako przestępstwa komputerowego). Pierwsza grupa to przestępstwa konwencjonalne (pospolite), które dzięki rozwojowi techniki uzyskały nową lub zmodyfikowaną postać (np. oszustwo, nękanie czy rozpowszechnianie pornografii dziecięcej). „Nowe" przestępstwa to te, które pojawiły się w związku z powstaniem komputerów, a następnie rozwojem technologii informatycznej i jej konwergencji z telekomunikacją. Klasycznym przykładem będzie uzyskanie nieuprawnionego dostępu czy nieuprawniona modyfikacja danych komputerowych[7]. Po drugie najpowszechniejszego i najbardziej praktycznego (bo najmniej wysublimowanego i najbardziej odpowiadającego rzeczywistości) podziału na przestępstwa, w których: 1) komputer lub sieć są celem przestępstwa (niejako „ofiarą"; *computer as a target*), inaczej po prostu *computer crimes*, np. hacking, podsłuch komputerowy, zakłócanie pracy sieci – przestępstwa będące przedmiotem niniejszego artykułu; 2) komputer lub sieć są narzędziem przestępstwa (*computer as an instrument or a tool*), inaczej *computer related crimes*, np. rozpowszechnianie pornografii dziecięcej, oszustwo[8]; 3) komputer lub sieć mogą być użyte do zadań dodatkowych, związanych z popełnieniem przestępstwa (np. do przechowywania danych o nielegalnej sprzedaży narkotyków)[9].

Zarówno w literaturze, jak i w ustawodawstwach można znaleźć zbliżony do powyższego „trójpodział" cyberprzestępstw[10] na: przestępstwa kompute-

7 Por. np. P. Grabosky, *Electronic Crime*, New Jersey 2006, s. 12–14.

8 Często spotykane jest rozbicie tej kategorii na dwie grupy: *computer assisted (related) crimes* – przestępstwa związane z użyciem komputera, takie jak oszustwo komputerowe, oraz *computer content crimes* – cyberprzestępstwa związane z treścią przetwarzanej informacji, takie jak np. rozpowszechnianie pornografii dziecięcej. Zob. np. B.J. Koops, T. Robinson, *Cybercrime Law: A European Perspective* [w:] E. Casey (red.), *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Waltham–San Diego–London 2011, s. 130–133; D. Wall, *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013, s. 49–50.

9 S. Brenner [w:] R.D. Clifford (red.), *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, Durham 2011, s. 17–20; J. Clough, *Principles of cybercrime...*, s. 10, P. Grabosky, *Electronic crime...*, s. 11.

10 J. Clough, *Principles of cybercrime...*, s. 10. Por. K. Dudka, *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998, s. 105. Na temat klasyfikacji przestępstw komputerowych zob. też: J. Kosiński, *Cyberprzestępczość...*, s. 463–465; M. Siwicki, *Definicje i podział cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 241–252; M. Smarzewski,

rowe (ang. *Computer crimes*), przestępstwa, których popełnienie jest umożliwiane przez komputery (ang. *Computer facilitated crimes*), i przestępstwa, których popełnienie jest wspierane przez komputery (ang. *Computer supported crimes*).

Powyższy trójpodział przyjęty jest również w Konwencji o cyberprzestępczości[11] jedynej umowie międzynarodowej dotyczącej zwalczania przestępstw popełnianych za pośrednictwem internetu oraz sieci komputerowych. Przestępstwa odpowiadające czynom zabronionym z pierwszej grupy zostały w niej zebrane w jednym tytule jako *Przestępstwa przeciwko poufności, integralności i dostępności danych komputerowych i systemów komputerowych*. Natomiast przestępstwa z drugiej grupy znalazły się w trzech kolejnych tytułach jako *Przestępstwa związane z komputerami*, *Przestępstwa związane z treścią* oraz *Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych*.

Ostatnia grupa z „trójpodziału" nie jest przedmiotem zainteresowania prawa karnego materialnego, ale raczej procesowego, a zwłaszcza dowodowego. Dlatego też omawiając problematykę przestępstw komputerowych, pozostawia się je zwykle z boku.

Przestępstwa komputerowe w kodeksie karnym z 1997 r.

Polska regulacja czynów zabronionych określonych w dyrektywie 2013/40 znajduje się w rozdziale XXXIII Kodeksu karnego[12] „Przestępstwa przeciwko ochronie informacji", w przepisach art. 267–269c. Swój obecny kształt zawdzięcza ona trzem nowelizacjom: pierwszej, przeprowadzonej ustawą z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń[13], mającej dostosować polskie przepisy do postanowień wspomnianej Konwencji o cyberprzestępczości, drugiej, dokonanej ustawą z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw[14], której celem była implementa-

Cyberprzestępczość a zmiany w polskim prawie karnym [w:] I. Sepioło-Jankowska (red.), *Reforma prawa karnego. Księga po Zjeździe Młodych Karnistów*, Warszawa 2014, s. 264–267.

11 Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).

12 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2016 r., poz. 1137 ze zm.), dalej jako k.k.

13 Dz.U. nr 69, poz. 626.

14 Dz.U. nr 214, poz. 1344.

cja decyzji ramowej 2005/222/WSiSW w sprawie ataków na systemy informatyczne[15] oraz trzeciej, przeprowadzonej ustawą z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw[16], której głównym celem było wdrożenie dyrektywy 2014/42/UE z dnia 3 kwietnia 2014 r. w prawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej[17] oraz – „częściowo" (jak to określono w ustawie) – dyrektywy 2013/40 dotyczącej ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW[18].

W treści art. 267 § 1 k.k. przewidziano odpowiedzialność karną za uzyskanie przez sprawcę bez uprawnienia dostępu do informacji[19] dla niego nieprzeznaczonej. Dokonano w nim kryminalizacji trzech czynów, będących zamachami na bezpieczeństwo systemów informatycznych i przetwarzanych w nich danych.

15 Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69, s. 67).

16 Dz.U. z 2017 r., poz. 768.

17 Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w prawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz.Urz. UE L 127, s. 39).

18 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218, s. 8).

19 Należy już na wstępie zwrócić uwagę, iż w aktach prawa międzynarodowego oraz unijnego dotyczących problematyki bezpieczeństwa sieci komputerowych dla określenia przedmiotu ochrony operuje się pojęciem „danych komputerowych", a nie „informacji". Polski ustawodawca pojęcia informacji i danych w zasadzie utożsamia, mimo zachodzących między nimi różnic. W świetle przepisu art. 2 lit b dyrektywy 2014/30 „dane komputerowe" należy rozumieć jako „przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny". Zbliżona definicja znajduje się w Konwencji o cyberprzestępczości. Zgodnie z powyższym dane komputerowe są nośnikiem (medium) informacji, faktów i koncepcji, które dopiero sprowadzone do postaci danych komputerowych są czytelne dla systemu komputerowego (czy informatycznego). W zakres tego pojęcia wchodzą również programy komputerowe. Rozróżnienie pojęć „danych komputerowych" i „informacji" ma znaczenie z prawnego punktu widzenia. Można bowiem wejść w posiadanie danych komputerowych, ale nie móc skorzystać z zawartych w nich informacji np. z uwagi na nieznajomość algorytmu, według którego zostały one zakodowane. Zniszczenie danych nie zawsze oznacza zniszczenie informacji, podobnie jak zabór danych nie musi być kradzieżą informacji. Zob. szerzej: A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 37 i n.

Po pierwsze – podłączenia się do sieci telekomunikacyjnej[20], czyli uzyskanie fizycznego dostępu do niej np. poprzez podłączenie się przez sprawcę za jej pośrednictwem do serwera i uzyskanie dostępu do przechowywanych w nim danych (działania polegające na ich przechwytywaniu w trakcie przesyłania penalizuje art. 267 § 3 k.k.).

Po drugie – uzyskania dostępu do informacji w wyniku przełamania elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia. Chronione są zatem jedynie informacje przechowywane w systemach komputerowych, które zostały przez ich dysponenta zabezpieczone przed nieuprawnionym dostępem. Pod pojęciem elektronicznego, magnetycznego, informatycznego zabezpieczenia należy rozumieć „wszelkie formy utrudnienia dostępu do informacji, których usunięcie wymaga wiedzy specjalistycznej lub posiadania szczególnego urządzenia lub kodu"[21], natomiast „inne szczególne zabezpieczenie" jest kategorią dopełniającą, obejmującą środki niemożliwe do zakwalifikowania do któregoś z określonych w przepisie rodzajów, a których zniwelowanie sprawia sprawcy co najmniej takie trudności, jak przełamanie zabezpieczenia elektronicznego, magnetycznego lub informatycznego[22]. Dane komputerowe mogą być chronione bezpośrednio,

20 Zgodnie z definicją zawartą w przepisie art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2016 r., poz. 1489 ze zm.) przez sieć telekomunikacyjną należy rozumieć „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju". Będą to zatem np. sieci satelitarne, sieci stałe wykorzystujące komutację łączy (ang. *Circuit switching*, inaczej komutacja kanałów lub komutacja obwodów – polega na tworzeniu na żądanie między dwiema lub większą ilością punktów sieci „stałego" połączenia do ich wyłącznego użytku na czas transmisji) oraz komutację pakietów (ang. *Packet switching*– sposób transmisji danych polegający na podziale ich na pakiety, z których każdy może dotrzeć inną drogą do celu; proces przesyłania pakietów nazywa się routowaniem lub trasowaniem i odbywa się pomiędzy węzłami sieci – routerami), sieci telewizji kablowej czy sieci elektryczne umożliwiające transmisję sygnałów. Urządzenia komutacyjne to urządzenia służące komutacji łączy (np. centrale telefoniczne), natomiast urządzenia przekierowujące – komutacji pakietów (będą to przede wszystkim routery). Zob. szerzej: A. Krasuski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, s. 83–84; S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013, s. 82–83; F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko komputerowym i systemom informatycznym*, Warszawa 2016, s. 278–282.

21 W. Wróbel [w:] A. Zoll (red.), *Kodeks karny. Komentarz. Część szczególna. Komentarz do artykułów 117–277 k.k.*, t. II, Warszawa 2013, s. 1502.

22 P. Kardas *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, s. 71.

np. przez zaszyfrowanie czy zabezpieczenie dostępu hasłem, lub pośrednio – w ramach ochrony samego systemu informatycznego – czemu służą *firewalle*, systemy wykrywania włamań czy procedura uwierzytelniania. „Przełamaniem zabezpieczeń" jest bezpośrednie oddziaływanie sprawcy na zabezpieczenie, prowadzące do zniwelowania jego funkcji ochronnej, które nie musi się wiązać z jego zniszczeniem[23]. W doktrynie podkreśla się, że ma być ono realne oraz aktywne w momencie popełnienia czynu. W przeciwnym wypadku nie dojdzie do wypełnienia znamion przestępstwa[24].

Po trzecie – ominięcia wskazanych wyżej zabezpieczeń i uzyskanie dzięki temu dostępu do informacji. Nie należy bowiem zapominać, że przełamanie zabezpieczeń jest tylko jedną z wielu technik (i to nawet nie najczęściej stosowaną) używanych przez hackerów do penetracji systemów komputerowych. Pozostałe sprowadzają się do ich ominięcia, a polegają na wprowadzeniu w błąd człowieka (*social engineering*, czyli tzw. socjotechnika, polegająca np. na wyłudzeniu hasła), wprowadzeniu w błąd systemu (np. tzw. *IP spoofing*, czyli fałszowanie adresów, mające na celu wprowadzenie w błąd co do miejsca wysłania pakietów danych) czy wykorzystaniu luk (błędów) lub słabości w systemach operacyjnych, aplikacjach, czy protokołach (zbiorach zasad określających procesy komunikacyjne odpowiadające m.in. za identyfikację komputerów w sieci), czemu służą programy zwane *exploitami*.

W przepisie art. 267 § 2 k.k. dokonano kryminalizacji nieuprawnionego uzyskania dostępu do całości lub części systemu informatycznego[25]. Autorzy

23 P. Kardas, *Prawnokarna ochrona...*, s. 71–72; P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks karny. Praktyczny komentarz*, Warszawa 2012, s. 621; W. Wróbel [w:] A. Zoll (red.), *Kodeks*..., s. 1502–1503.

24 Por. S. Bukowski, *Przestępstwo hackingu*, „Przegląd Sądowy" 2006, nr 4, s. 142–143; P. Kardas, *Prawnokarna ochrona*..., s. 64.

25 Interpretacja tego pojęcia w zasadzie od momentu pojawienia się go w Kodeksie karnym rodziła problemy (zob. szerzej np.: F. Radoniewicz, *Odpowiedzialność karna*..., s. 275–278 oraz M. Siwicki, *Cyberprzestępczość*, Legalis 2013), które dodatkowo przybrały na sile po ratyfikacji przez Polskę Konwencji o cyberprzestępczości. Ponieważ przepis art. 267 § 2 k.k. dodany został nowelizacją z 2008 r., związaną z implementacją decyzji ramowej 2005/222, wskazane byłoby zatem rozumienie tegoż terminu, zgodnie z definicją zawartą w tym akcie oraz w zastępującej go dyrektywie 2013/40, a więc zarówno jako pojedyncze urządzenie przetwarzające dane komputerowe, jak i zespół takich urządzeń, czyli sieć (zob. wcześniejsze uwagi). Natomiast tłumacząc tekst Konwencji o cyberprzestępczości popełniono wiele błędów. Jednym z nich jest przetłumaczenie pojęcia systemu komputerowego (ang. *computer system*), jako systemu informatycznego. A jak wspominano wcześniej, zakres przedmiotowy pojęcia system komputerowy z Konwencji jest węższy niż „systemu informatycznego" z dyrektywy 2013/40. Powoduje to wątpliwości co do zakresu pojęcia systemu informatycznego na gruncie Kodeksu karnego. Należy jednocześnie zaznaczyć, że mimo

projektu nowelizacji z 2008 r. – którą dodano tenże przepis – słusznie wskazali w jej uzasadnieniu, że celem uzyskania nieuprawnionego dostępu do systemu może być nie tylko uzyskanie dostępu do informacji, których dane informatyczne są nośnikiem, ale stanowić może niejako wstęp do innych działań, np. powołanemu jako przykład w uzasadnieniu umieszczeniu w komputerze programu, umożliwiającego przejęcie nad nim kontroli, celem stworzenia botnetu[26], za pomocą którego sprawca ma zamiar przeprowadzić atak dDoS[27]. Przepis ten znajdzie zastosowanie, gdy celem sprawcy, który uzyskuje nieuprawniony dostęp jest popełnienie następnie „pospolitego" przestępstwa (zachowanie sprawcy może bowiem polegać np. na uzyskaniu dostępu do konta innego użytkownika w serwisie aukcyjnym, celem wykorzystania go do dokonywania oszustw) lub gdy działał z innych pobudek, takich jak np. sprawdzenie własnych umiejętności czy uzyskanie szacunku w „środowisku hackerskim". Tym samym cel, który sprawca miał zamiar osiągnąć czy motyw, jakim się kierował jest obojętny dla bytu przestępstwa stypizowanego w art. 267 § 2 k.k.

iż Konwencja o cyberprzestępczości w momencie jej ratyfikacji stała się częścią porządku prawnego, to definicji „systemu informatycznego" (komputerowego) nie można stosować bezpośrednio, z uwagi właśnie na omawiane problemy. Istniejący zamęt potęguje fakt, że w tłumaczeniu definicji pojęcia danych informatycznych w art. 2 lit. b Konwencji (ang. *Computer data*, przetłumaczonych jako „dane informatyczne") posłużono się pojęciem systemu komputerowego („dane informatyczne oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny"). Ponadto terminu „system komputerowy" użyto w tłumaczeniu Protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych z dnia 28 stycznia 2003 r (Dz.U. z 2015 r., poz. 730).

26 Botnety, czyli sieci komputerów, na których sprawca (bez wiedzy ich użytkowników) zainstalował specjalne programy – tzw. zombie (stąd przejęte komputery nazywane są „komputerami-zombie"), które są zdalnie uruchamiane w określonym momencie w celu np. przeprowadzenia ataku dDoS. Ponieważ możliwe jest wykorzystanie ogromnej liczby komputerów (nawet kilkuset tysięcy, rozsianych po całym świecie), prawdziwe źródło ataku pozostaje nieznane. Obecnie w internecie można uzyskać zarówno programy do przeprowadzenia ataków DoS, jak i „gotowe" botnety do przeprowadzenia ataków dDoS. Botnety ponadto mogą być wykorzystywane np. do rozsyłania spamu (niechcianych wiadomości e-mail). Zob. szerzej np.: A. Adamski, *Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich*, „Prokuratura i Prawo" 2013, nr 1, s. 68–69.

27 Ataki DoS (ataki odmowy usług, Denial of Service) mają zazwyczaj na celu zakłócenie pracy sieci (łącznie z jej zablokowaniem). W zasadzie można przyjąć, iż polegają na wywołaniu dużego ruchu sieciowego, prowadzącego do zawieszenia serwera, przeciążenia routera lub urządzeń sieciowych. Mogą być również skierowane przeciw konkretnym komputerom, uniemożliwiając im komunikację z serwerem. Ich „wzmocnionym" wariantem są ataki DdoS (rozproszone ataki DoS, *Distributed Denial of Service*), wykorzystujące *botnety*.

Przez dostęp do całości lub części zarówno systemu informatycznego należy rozumieć uzyskanie możliwości korzystania z jego zasobów, czyli – w zasadzie – przetwarzanych w nim danych, co jednak nie jest równoznaczne z dostępem do informacji, gdyż dane mogą być np. zaszyfrowane lub całkowicie niezrozumiałe dla sprawcy.

Przez dostęp nieuprawniony w rozumieniu niniejszego przepisu należy rozumieć dostęp bez uprawnień lub z ich przekroczeniem.

Rozwiązanie przyjęte przez ustawodawcę w przepisie art. 267 § 2 k.k. spotkało się z uzasadnioną krytyką z trzech zasadniczych powodów. Po pierwsze, jest to dosłowne przekopiowanie treści art. 2 decyzji ramowej 2005/222 („Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor"). Należy podkreślić, że decyzje ramowe służyły zbliżaniu przepisów prawnych państw członkowskich. Określały rezultat, jaki ma zostać osiągnięty, dobór środków ku temu prowadzących pozostawiając państwom członkowskim. W związku z tym ich postanowienia sformułowane są bardzo ogólnie. Decyzje ramowe harmonizujące prawo karne materialne nie nadają się zatem do dosłownej transpozycji. Po drugie przepis art. 267 § 2 k.k. jest niezwykle pojemny treściowo. Znamiona czynu w nim opisanego wypełni sprawca, który „uzyskuje nielegalny dostęp" do danych, bo na tym w zasadzie polega – o czym była już mowa – uzyskanie dostępu do systemu, przy czym by odpowiadać karnie, nie musi naruszyć zabezpieczenia. Jedynym warunkiem jest, by dostęp ów był nieuprawniony. Przyjąć należy, że przepis art. 267 § 2 k.k. będzie znajdował zastosowanie w przypadkach, gdy głównym elementem czynu sprawcy było uzyskanie dostępu do systemu informatycznego, a nie uzyskanie dostępu do informacji. Z sytuacją taką mamy do czynienia np. w wypadku włamania się do komputera w celu umieszczenia w nim bota. Szeroki zakres przedmiotowy przepisu art. 267 § 2 k.k. sprawia, że również część zachowań kryminalizowanych przez przepis art. 267 § 3 k.k., określanych jako podsłuch komputerowy, będzie mogła być jednocześnie kwalifikowana z art. 267 § 2 k.k. Uzyskanie nieuprawnionego dostępu do sieci jest równoznaczne z uzyskaniem dostępu do przesyłanych nią danych, tak więc sprawca realizuje jednocześnie znamiona czynu zabronionego z art. 267 § 3 k.k.

Po trzecie jedynym warunkiem, który musi zostać spełniony, aby możliwe było postawienie sprawcy zarzutu naruszenia przepisu art. 267 § 2 k.k., jest uzyskanie przez niego dostępu do systemu bez uprawnień. Kwestia praw dostępu do zasobów systemu informatycznego regulowana jest w większości

wypadków przez przepisy „miękkiego prawa" – regulaminy wewnętrzne sieci. Natomiast o nadaniu użytkownikowi uprawnień oraz o ich zakresie, decyduje administrator systemu. Takie odesłanie do norm pozaprawnych jest niebezpieczne i trudne do pogodzenia z zasadą określoności przestępstwa[28].

Ostatnią nowelizacją dodano przepis 269c, zgodnie z którym nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Narzędziem do walki m.in. z tzw. podsłuchem komputerowym[29] jest wspominany już kilkakrotnie artykuł 267 § 3 k.k., penalizujący zakładanie lub posługiwanie się – w celu uzyskania informacji[30] – podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

Należy podkreślić, że kryminalizuje on jedynie przechwytywanie danych komputerowych w czasie ich przesyłania. W przypadku uzyskania przez sprawcę danych przechowywanych np. na serwerze czy w prywatnym komputerze właściwa będzie kwalifikacja z art. 267 § 1 k.k. lub art. 267 § 2 k.k.

Bezprawność zachowania sprawcy zostaje oczywiście uchylona, jeśli zachowanie wypełniające znamiona jest legalnym działaniem organów ścigania (wynika z odpowiednich przepisów[31]).

28 Zob. szerzej: A. Adamski, *Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?*, „Prawo Teleinformatyczne" 2007, nr 3, s. 7–8; F. Radoniewicz, *Odpowiedzialność karna…*, s. 301–303.

29 Podsłuch komputerowy jest potocznym określeniem inwigilacji systemów informatycznych. Często nie w pełni poprawnie określa się to zjawisko mianem *sniffingu*, stanowiącego jedynie jedną z jego technik. Wyróżnia się dwa rodzaje podsłuchu komputerowego: pasywny – gdy sprawca jedynie zapoznaje się z treścią informacji oraz aktywny – gdy dokonuje modyfikacji przesyłanych danych, np. poprzez przekierowanie ich transmisji do innego miejsca w sieci.

30 Należy zwrócić uwagę, że dyrektywa 2013/40 nie przewiduje wymogu wystąpienia po stronie sprawcy przestępstwa nielegalnego przechwytywania danych jakichkolwiek dodatkowych wymogów dla przypisania mu odpowiedzialności karnej – np. „nieuczciwego" zamiaru, czy działania w określonym celu („Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor" – art. 6 dyrektywy 2013/40).

31 Przede wszystkim należy wskazać przepisy kodeksu postępowania karnego, ustawy z dnia 6 kwietnia 1990 r. o Policji (tj. Dz.U. z 2016 r., poz. 1782 ze zm.), ustawy z dnia 24 maja

W art. 268 § 2 k.k. dokonano kryminalizacji nieuprawnionej ingerencji w dane komputerowe, polegającej na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu istotnej informacji na informatycznym nośniku danych[32] oraz ograniczania ich dostępności dla osoby uprawnionej[33] poprzez udaremnianie lub znaczne utrudnianie w inny sposób zapoznanie się z informacją utrwaloną na takim informatycznym nośniku danych.

Informacja, będąca przedmiotem czynu sprawcy musi być „istotna", przede wszystkim w sensie obiektywnym (ze względu na jej treść, wagę i znaczenie[34]) – ale z uwzględnieniem interesów osoby uprawnionej do zapoznania się z nią[35], w tym celu, jakiemu służyła lub miała służyć[36].

Ponieważ przedmiotem ochrony jest „informacja zapisana na informatycznym nośniku danych", przepis art. 268 § 2 k.k. nie znajdzie zastosowania w sytuacji, gdy utrudnienie w zapoznaniu się z nią będzie wynikiem zakłócania pracy sieci (wówczas zachowanie sprawcy powinno zostać zakwalifikowane na podstawie art. 268a § 1 lub 2 albo 269a k.k.).

Typem kwalifikowanym tego przestępstwa jest czyn z art. 268 § 3 k.k. Znamieniem kwalifikującym jest wyrządzenie przez sprawcę znacznej szkody majątkowej.

W pierwszej części przepisu art. 268a § 1 k.k. dokonano kryminalizacji czynów, polegających na niszczeniu, modyfikacji danych i utrudnianiu do nich dostępu. Natomiast w drugiej – działań polegających na istotnym zakłócaniu (czyli utrudnianiu funkcjonowania systemu informatycznego) lub uniemożliwianiu przetwarzania, gromadzenia lub przekazywania danych informatycznych. Sformułowanie to odnosi się do wszelkich czynności oddziałujących na

2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tj. Dz.U. z 2016 r., poz. 1897 ze zm.).

32 W świetle przepisu art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2017 r., poz. 570 ze zm.), dalej jako ustawa o informatyzacji, jest to „materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej" – w zakresie tego pojęcia mieszczą się w nim wszystkie nośniki danych, czyli: niespotykane obecnie dyskietki, dyski twarde (nośniki magnetyczne), płyty CD i DVD (nośniki optyczne), pamięci półprzewodnikowe (są to m.in. pamięci RAM – *Random Access Memory*, ROM – *Read Only Memory*, jak również pamięci zamontowane, np. w drukarkach), pamięci *flash* itd.

33 Tak też: A. Adamski, *Prawo karne...*, s. 64–65.

34 P. Kardas, *Prawnokarna ochrona…*, s. 88.

35 Ibidem. Zob. także: P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks…*, s. 621; W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1296.

36 O. Górniok [w:] O. Górniok i in., *Kodeks karny. Komentarz*, t. 2, Gdańsk 2005, s. 363–364; M. Kalitowski [w:] M. Filar (red.), *Kodeks karny. Komentarz*, Warszawa 2012, s. 1209.

te procesy, których skutkiem jest ich nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych informatycznych[37].

Omawiany czyn ma swój typ kwalifikowany określony w art. 268a § 2 k.k. Znamieniem kwalifikującym jest spowodowanie przez sprawcę znacznej szkody majątkowej.

Istotą przestępstwa tzw. sabotażu informatycznego określonego art. 269 § 1 k.k. jest niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Zgodnie z przepisem art. 269 § 2 k.k. przestępstwo sabotażu informatycznego polegać może również na niszczeniu albo wymianie informatycznego nośnika danych lub niszczeniu albo uszkadzaniu urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania chronionych danych informatycznych. Zagrożone jest ono wysoką sankcją – karą pozbawienia wolności od sześciu miesięcy do ośmiu lat.

Z uwagi na znacznie wyższe znaczenie informacji chronionych przez przepis art. 269 § 1 k.k. w porównaniu z informacją podlegającą ochronie na podstawie art. 268 § 2 k.k. oraz identyczność pozostałych znamion czynów kryminalizowanych przez te przepisy, przy jednoczesnej różnicy w wysokości zagrożenia karą i środkami karnymi, przestępstwo z art. 269 § 1 k.k. uważa się za typ kwalifikowany w stosunku do przestępstwa z art. 268 § 2 k.k.[38] Z tych też względów twierdzenie takie jest moim zdaniem uzasadnione również w przypadku stosunku między przestępstwami z art. 268a k.k. lub 269a a 269 § 1 k.k.

Przepis art. 269a k.k. przewiduje odpowiedzialność karną osoby, która bez uprawnienia w stopniu istotnym zakłóca pracę systemu informatycznego,

37 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1520.

38 P. Kardas, *Prawnokarna ochrona…*, s. 96. Tak też: A. Adamski, *Prawo karne…*, s. 77; M. Kalitowski [w:] M. Filar (red.), *Kodeks…*, s. 1211.

systemu teleinformatycznego[39] lub sieci teleinformatycznej[40] poprzez działania o charakterze logicznym, takie jak transmisja, zniszczenie, uszkodzenie lub zmiana danych informatycznych. Przedmiotem ochrony jest bezpieczeństwo pracy systemu komputerowego, a co za tym idzie – dostępność przetwarzanych w nim danych informatycznych.

Zamach na pracę systemu informatycznego, teleinformatycznego i sieci teleinformatycznej jest zamachem logicznym, a nie fizycznym – zakłócenie ma być wywołane przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych. Będą to np. ataki typu DoS.

Andrzej Adamski[41] i Włodzimierz Wróbel[42] zauważają, że przepisy art. 268a i 269a k.k. nakładają się na siebie zakresowo. Określenia „w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie danych" oraz „w istotnym stopniu zakłóca pracę systemu informatycznego, teleinformatycznego i sieci teleinformatycznej" są w istocie tożsame. Praca ww. systemów oraz sieci teleinformatycznej polega właśnie na przetwarzaniu, gromadzeniu i przekazywaniu danych. A. Adamski proponuje, by przepis art. 268a k.k. traktować jako narzędzie służące ściganiu sprawców, któ-

39 Stosownie do art. 2 pkt 3 ustawy o informatyzacji, jest to 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 urządzenia końcowego w rozumieniu prawa telekomunikacyjnego (identyczna definicja znajduje się w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2016 r., poz. 1030 ze zm.). Przyjmuje się, że system informatyczny służy przetwarzaniu danych, natomiast system telekomunikacyjny przesyłaniu tych danych. Stąd system teleinformatyczny jest systemem informatycznym (w którym dane komputerowe są przetwarzane) podłączonym do sieci telekomunikacyjnej, za pośrednictwem której może wysyłać i odbierać dane. Por. X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 62–64; F. Radoniewicz, *Odpowiedzialność karna…*, s. 282–284.

40 Pojęcie to nie jest obecnie zdefiniowane w żadnym akcie prawnym. Sieć teleinformatyczna jest zespołem systemów teleinformatycznych, czyli systemów informatycznych, w których przetwarzane są dane, powiązanych ze sobą sieciami telekomunikacyjnymi, służącymi przesyłaniu danych między tymi systemami. Jest to struktura rozległa, której powstanie związane jest z procesem konwergencji technologii informatycznej i telekomunikacji. Por. X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 62–64; F. Radoniewicz, *Odpowiedzialność karna…*, s. 284; M. Świerczyński [w:] J. Gołaczyński, K. Kowalik-Bańczyk, A. Majchrowska, M. Świerczyński, *Komentarz do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*, Warszawa 2009, s. 39; A. Urbanek [w:] J. Chustecki i in., *Vademecum teleinformatyka*, Warszawa 1999, s. 4–5.

41 A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4, s. 58–59.

42 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1527.

rych zachowania nie wypełniły znamion strony przedmiotowej art. 269a k.k.[43] W. Wróbel natomiast postuluje stosować przepis art. 269a k.k. wówczas, gdy następuje kwalifikowane zakłócenie pracy systemu lub sieci[44]. Za typ kwalifikowany czynu z art. 269 a k.k. należy uznać przestępstwo z art. 269 § 1 k.k.

Podobnie jak w przypadku czynu z art. 267 § 2 k.k. zastosowanie znaleźć może instytucja z art. 269c k.k.

W artykule 269b k.k. spenalizowano czyny zabronione, których przedmiotem wykonawczym są „narzędzia hackerskie". Przepis art. 269b § 1 k.k., będący odpowiednikiem art. 7 dyrektywy 2013/40, kryminalizuje wytwarzanie, pozyskiwanie, zbywanie, udostępnianie: 1) urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4 k.k. (sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach), a także w art. 267 § 3, art. 268a § 1 albo 268 a § 2 w zw. z 268a § 1, art. 269 § 1 lub 2 albo art. 269a k.k.; 2) haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub w sieci teleinformatycznej.

Rozwiązania przyjęte w przepisie art. 269b § 1 k.k. od momentu wprowadzenia go do Kodeksu karnego nowelizacją z 2004 r. powszechnie krytykowane. Przede wszystkim wskazywano na brak klauzuli wyłączającej odpowiedzialność karną administratorów i osób zajmujących się bezpieczeństwem systemów informatycznych, którzy używają tego typu programów w procesie tworzenia zabezpieczeń systemów oraz ich testowania czy twórców oprogramowania antywirusowego[45]. Tę wadę wprawdzie w zasadzie usuwa ostatnia nowelizacja[46], ale pozostawia ona inne „niedociągnięcia". Wśród

43 A. Adamski, *Cyberprzestępczość…*, s. 58.

44 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1527.

45 P. Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b kodeksu karnego*, „Prokurator" 2005, nr 1, s. 82; F. Radoniewicz, *Odpowiedzialność karna…*, s. 336. Por. W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1530.

46 Do art. 269b dodano bowiem § 1a w brzmieniu: „Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia". Jednocześnie podwyższono górną granicę kary grożącej za to przestępstwo do 5 lat pozbawienia wolności, co uzasadniono jedynie koniecznością umożliwienia zastosowania wobec sprawcy tego czynu instytucji tzw. przepadku rozszerzonego, przewidzianego w art. 45 § 2 k.k. (Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, druk nr 1186, pkt 4.6). Spotkało się to ze słuszną krytyką (O (braku) odpowiedzialności karnej za szukanie luk w systemach i sieciach informatycznych – opinia

nich – w pierwszej kolejności – zwrócić należy uwagę na brak w zawartym w treści art. 269b § 1 k.k. katalogu przestępstw (do których popełnienia wytwarzanie, pozyskiwanie, zbywanie, udostępnianie urządzeń i programów jest kryminalizowane), wskazania hackingu, zarówno w postaci nieuprawnionego uzyskania informacji z art. 267 § 1 k.k., jak i nieuprawnionego dostępu do systemu informatycznego z art. 267 § 2 k.k.[47]

Co się tyczy innych mankamentów przepisu art. 269b § 1 k.k.– przede wszystkim mowa w nim o programach „przystosowanych" do popełnienia określonych w nim czynów. Istnieje zatem problem, jak ocenić działanie twórcy programu spełniającego kilka funkcji (chodzi o tzw. programy o podwójnej naturze)[48], użytego następnie przez osobę trzecią w celach przestępczych, czego autor by sobie nie życzył[49]. W celu zachowania *ratio legis* wprowadzenia tego przepisu i uniknięcia zbyt szerokiej kryminalizacji W. Wróbel zaproponował jego interpretację nawiązującą do definicji karalnych czynności przygotowawczych z art. 16 § 1 k.k., wymagając tym samym od sprawcy wytwarzającego lub pozyskującego wymienione w przepisie narzędzia, zamiaru bezpośredniego (w przypadku zbywania i udostępnianiu poprzestając na wymogu zamiaru ewentualnego)[50]. Jak się jednak wydaje, większość przedstawicieli doktryny uważa jednak (z wyjątkiem – właśnie W. Wróbla i Joanny Piórkowskiej-Flieger, Barbary Kunickiej-Michalskiej[51] i Andrzeja

prawna Fundacji Frank Bold i Krakowskiego Instytutu Prawa Karnego, http://blog.frankbold.pl/bug-bounty/).

47 Brak w katalogu przestępstwa z art. 268 § 2 k.k. jest mniej problematyczny – do popełnienia czynu w nim określonego będą służyć te same programy, co w przypadku czynów z art. 268a § 1 i 2 k.k. oraz art. 165 § 1 pkt 4 k.k. (np. wirusy).

48 Np. monitory sieciowe, inaczej nazywane analizatorami protokołów, umożliwiające administratorom analizę ruchu w sieci, mogą zostać wykorzystane przez hackerów jako *sniffery*.

49 Por. A. Adamski, *Cyberprzestępczość…*, s. 60.

50 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1529–1530. Podobnie J. Piórkowska-Flieger [w:] T. Bojarski (red.), *Kodeks karny. Komentarz*, Warszawa 2012, s. 713.

51 B. Kunicka-Michalska uważa, że trudno wyobrazić sobie wytwarzanie, pozyskiwanie czy zbywanie bez zamiaru bezpośredniego sprawcy; zob. B. Kunicka-Michalska [w:] A. Wąsek, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Komentarz. Komentarz do artykułów 222–316*, t. II, Warszawa 2010, s. 748.

Marka[52]), że dla przypisania sprawcy winy wystarczy, by działał on w zamiarze ewentualnym[53].

Zakończenie

Polska regulacja przestępstw komputerowych wymaga niewątpliwie zmian. W pierwszej kolejności należy ujednolicić siatkę pojęciową. Obecnie – z uwagi na ratyfikację Konwencji o cyberprzestępczości – nie zachodzi już konieczność definiowania pojęcia danych informatycznych (komputerowych), gdyż zawarta w niej definicja ma charakter normy samowykonywalnej i może być bezpośrednio stosowana. Z uwagi na omówione szeroko wątpliwości dotyczące zakresu pojęć „system informatyczny" należałoby je zdefiniować. Podobnie należy uczynić w przypadku terminu „sieć teleinformatyczna". Ewentualnie można rozważyć zastąpienie go pojęciem „sieć telekomunikacyjna".

Uważam, że należy przemyśleć ograniczenie zakresu kryminalizacji przepisu art. 267 § 1 k.k. do przypadków naruszenia tajemnicy korespondencji, przy jednoczesnym przyznaniu głównej roli w walce z *hackingiem* (uzyskania nieuprawnionego dostępu do systemu informatycznego) przepisowi art. 267 § 2 k.k., po uzupełnieniu go o wymóg, by sprawca zniwelował lub ominął magnetyczne, elektroniczne, informatyczne lub inne szczególne zabezpieczenie

52 Według A. Marka czynności sprawcze wymienione w przepisie art. 269b § 1 k.k. mogą być popełnione jedynie w zamiarze bezpośrednim, zaś zamiarem ewentualnym może być objęte przeznaczenie urządzeń, programów, haseł, kodów dostępu i innych danych; zob. A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 576. J.W. Giezek, krytycznie odnosząc się do stanowiska, iż wytwarzania i pozyskiwania dopuścić się można jedynie w zamiarze bezpośrednim, podkreśla wręcz, iż bardziej prawdopodobne wydaje się popełnienie tego przestępstwa w zamiarze ewentualnym, gdy sprawca jedynie godzi się na to, że swoim zachowaniem wypełni znamiona przestępstwa, gdyż zwykle sytuacja będzie przedstawiać się w ten sposób, iż nie tyle chce wytworzyć, pozyskać, zbyć lub udostępnić określone urządzenia lub programy komputerowe, lecz że z pewnym jedynie prawdopodobieństwem zakłada, że okażą się one przystosowane do popełnienia jednego z określonych w komentowanym przepisie przestępstw, godząc się, że tak właśnie będzie. Autor ten sugeruje wręcz, że owa „niepewność diagnozy" np. co do przystosowania urządzeń lub programów pozwala przyjąć, że mamy w takim przypadku do czynienia jedynie z zamiarem ewentualnym , J.W. Giezek [w:] J.W. Giezek (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014, s. 1007–1008.

53 Zob. np.: A. Adamski, *Cyberprzestępczość…*, s. 61; K. Gienas, *Uwagi do przestępstwa…*, s. 81–82; O. Górniok [w:] O. Górniok i in., *Kodeks…*, s. 369–370; M. Kalitowski [w:] M. Filar (red.), *Kodeks…*, s. 1214; P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks…*, s. 629.

(jednocześnie byłoby to zgodne z postanowieniami art. 3 dyrektywy 2013/40, która zaleca takie rozwiązanie[54]).

Konieczna jest modyfikacja polskiej regulacji podsłuchu komputerowego. Artykuł 267 § 3 k.k. wymaga bowiem wystąpienia po stronie sprawcy zamiaru kierunkowego, a przesłanki takiej nie przewiduje art. 6 dyrektywy 2013/40. Ewentualnie rozważyć można pozostawienie go w dotychczasowym (lub zbliżonym) brzmieniu, przy jednoczesnym dodaniu przepisu (zgodnego z art. 6 dyrektywy 2013/40), określającego czyn, w stosunku do którego występek z obecnego art. 267 § 3 k.k. stanowiłby typ kwalifikowany.

Zmian w również wymaga przepis art. 269b § 1 k.k. Konieczne jest ograniczenie odpowiedzialności do zamiaru bezpośredniego oraz wskazanie, że dotyczy on narzędzi i programów komputerowych „przede wszystkim" lub „głównie" (w angielskim tekście dyrektywy 2013/40 użyto pojęcia *„primarily"* tekście, w polskim – właśnie „głównie") służącym popełnieniu przestępstw. Ponadto należy rozszerzyć katalog przestępstw, do których popełnienia miałyby one służyć co najmniej o pozostałe omawiane czyny.

Bibliografia

Literatura

Clifford R.D. (red.), *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, Durham 2011.

Adamski A., *Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich*, „Prokuratura i Prawo" 2013, nr 1.

Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4.

Adamski A., *Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?*, „Prawo Teleinformatyczne" 2007, nr 3.

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Bojarski T. (red.), *Kodeks karny. Komentarz*, Warszawa 2012.

Bukowski S., *Przestępstwo hackingu*, „Przegląd Sądowy" 2006, nr 4.

Clough J., *Principles of Cybercrime*, New York 2013.

Czechowski R., Sienkiewicz P., *Przestępcze oblicza komputerów*, Warszawa 1993.

Dudka K., *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998.

Filar M. (red.), *Kodeks karny. Komentarz*, Warszawa 2012.

Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000.

Gienas P., *Uwagi do przestępstwa stypizowanego w art. 269b kodeksu karnego*, „Prokurator" 2005, nr 1.

Giezek J.W. (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014.

54 „Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor". Zob. także: F. Radoniewicz, *Odpowiedzialność karna…*, s. 459.

Gołaczyński J., Kowalik-Bańczyk K., Majchrowska A., Świerczyński M., *Komentarz do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*, Warszawa 2009.
Grabosky P., *Electronic Crime*, New Jersey 2006.
Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.
Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004.
Koops B.J., Robinson T., *Cybercrime Law: A European Perspective* [w:] E. Casey (red.), *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Waltham–San Diego–London 2011.
Krasuski A., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010.
Marek A., *Kodeks karny. Komentarz*, Warszawa 2010.
Mozgawa M. (red.), *Kodeks karny. Praktyczny komentarz*, Warszawa 2012.
Piątek S., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko komputerowym i systemom informatycznym*, Warszawa 2016.
Shinder D.L., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004.
Sieber U., *Legal Aspects of Computer-Related Crime in the Information Society – Comcrime – Study*, Würzburg 1998.
Siwicki M., *Definicje i podział cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.
Smarzewski M., *Cyberprzestępczość a zmiany w polskim prawie karnym* [w:] I. Sepioło-Jankowska (red.), *Reforma prawa karnego. Księga po Zjeździe Młodych Karnistów*, Warszawa 2014.
Wall D., *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013.
Wąsek A., Zawłocki R. (red.), *Kodeks karny. Część szczególna. Komentarz. Komentarz do artykułów 222–316*, t. II, Warszawa 2010.
Wójcik J.W., *Przestępstwa komputerowe. Fenomen cywilizacji*, cz. I, Warszawa 1999.
Zoll A. (red.), *Kodeks karny. Komentarz. Część szczególna. Komentarz do artykułów 117–277 k.k.*, t. II, Warszawa 2013.

Akty prawne

Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69, s. 67).
Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218, s. 8).
Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w prawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz.Urz. UE L 127, s. 39).
Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).
Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych z dnia 28 stycznia 2003 r. (Dz.U. z 2015 r., poz. 730).
Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2016 r., poz. 1489 ze zm.).
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2017 r., poz. 570 ze zm.).
Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tj. Dz.U. z 2016 r., poz. 1897 ze zm.).
Ustawa z dnia 6 kwietnia 1990 r. o Policji (tj. Dz.U. z 2016 r., poz. 1782 ze zm.).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2016 r., poz. 1137 ze zm.).

Computer crimes in the Polish Penal Code

Abstract

The aim of the paper is to analyze the provisions criminalizing the phenomenon of "computer crimes" ("cyber crimes") in the strict sense, ie acts in which a computer or network is the target of a crime ("a victim"). The paper consists of three parts – a short introduction in which the most important terminological issues are discussed in a synthetic way, the main part in which analisis of articles 267–269c of the Penal Code of 1997 (Chapter XXXIII, entitled "Offenses against the protection of information" – in which the Polish legislator defined these offenses – is carried out. The last part is the summary containing comments de legelata and de lege ferenda.

Key words: cybercime, hacking, hackingtools, surveillance, data interception