Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym - propozycje zmian

Wstęp

Wstęp

Monografię dotyczącą przestępczości komputerowej (cyberprzestępczości) należałoby zacząć od próby zdefiniowania tego zjawiska. Dotychczas żaden ustawodawca nie zdecydował się na wprowadzenie do systemu prawnego definicji legalnej z oczywistych powodów – bardzo szybko stałaby się nieaktualna. Oczywiście w nauce prawa karnego nie brakuje prób zdefiniowania tego terminu. Jako jedną z pierwszych można wskazać niezwykle szeroką i pojemną definicję „nadużycia komputerowego", sformułowaną przez *Ulricha Siebera* w 1983 r., przyjętą przez grupę ekspertów OECD[1] na spotkaniu w Paryżu, zgodnie z którą „za przestępstwo komputerowe uważa się wszelkie bezprawne, nieetyczne i nieupoważnione zachowania odnoszące się do procesu przetwarzania i (lub) przekazywania danych"[2]. Generalnie jednak kładziono nacisk na wskazanie katalogu przestępstw komputerowych, a nie na tworzenie wyczerpującej definicji[3].

Na X Kongresie ONZ w Sprawie Zapobiegania Przestępczości i Postępowania z Przestępcami (ang. *The Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders*), który odbył się w dniach 10–17.4.2000 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): wszelkie 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): wszelkie nielegalne działanie dokonane za pomocą lub dotyczące systemów komputerowych lub sieci komputerowych, włączając w to m.in. nielegalne po-

[1] Organizacja Współpracy Gospodarczej i Rozwoju (ang. *Organization for Economic Co-operation and Development*, fr. *Organisation de Coopération et de Développement Economiques*).

[2] *U. Sieber*, Legal Aspects of Computer-Related Crime, s. 20–21.

[3] Zob. szerzej np. *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 119–127.

siadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[4].

Powyższa kategoryzacja stanowi punkt wyjścia dla najpopularniejszej obecnie klasyfikacji, obowiązującej zarówno w doktrynie, jak i legislacji, dzielącej przestępstwa komputerowe (cyberprzestępstwa) na trzy grupy – czyny, w których:

1) komputer, dane komputerowe lub sieć są celem przestępstwa (niejako „ofiarą"; ang. *computer as a target*), inaczej po prostu „przestępstwa komputerowe" (ang. *computer crimes*), np. haking, podsłuch komputerowy, zakłócanie pracy sieci – nazywane również „nowymi przestępstwami komputerowymi", gdyż pojawiły się wraz z pojawieniem się i rozwojem komputerów i sieci komputerowych;
2) komputer lub sieć są narzędziem przestępstwa (ang. *computer as an instrument or a tool*), inaczej „przestępstwa dotyczące komputerów" (ang. *computer related crimes*), np. rozpowszechnianie pornografii dziecięcej, oszustwo. Często spotykane jest rozbicie tej kategorii na dwie grupy: przestępstwa związane z użyciem komputera [ang. *computer assisted* (*related*) *crimes*], np. oszustwo komputerowe, oraz cyberprzestępstwa związane z treścią przetwarzanej informacji (ang. *computer content crimes*), np. rozpowszechnianie pornografii dziecięcej[5] czy piractwo komputerowe; w odróżnieniu od przestępstw z pierwszej grupy nazywane są również „starymi przestępstwami" – są to bowiem przestępstwa pospolite, które dzięki rozwojowi komputerów i sieci komputerowych uzyskały jedynie nową formę czy medium (np. rozpowszechnianie pornografii dziecięcej)[6];
3) komputer lub sieć użyte są do zadań dodatkowych, związanych z popełnieniem przestępstwa (np. do przechowywania danych o nielegalnej sprzedaży narkotyków)[7]. Grupa ta nie jest przedmiotem zainteresowania prawa karnego materialnego, a raczej procesowego, a zwłaszcza dowodowego[8].

Powyższa klasyfikacja została przyjęta w Konwencji Rady Europy o cyberprzestępczości otwartej do podpisu w Budapeszcie 23.11.2001 r.[9] – pierwszej wielostronnej 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" (Rozdział II – „Środki, jakie należy podjąć na szczeblu krajowym",

[4] Por. *M. Smarzewski*, Cyberprzestępczość (red. *I. Sepioło-Jankowska*), s. 267; *D.L. Shinder*, *E. Tittel*, Cyberprzestępczość, s. 35–36.

[5] Zob. np. *B.J. Koops*, *T. Robinson*, Cybercrime Law (red. *E. Casey*), s. 130–133; *D. Wall*, Cybercrime, s. 49–50.

[6] Por. *P. Grabosky*, Electronic Crime, s. 12–14.

[7] *S.W. Brenner*, Cybercrime and the Law, s. 17–20; *J. Clough*, Principles of cybercrime, s. 10; *P. Grabosky*, Electronic Crime, s. 11; *F. Radoniewicz*, Odpowiedzialność karna za hacking, s. 119–127.

[8] Zob. też *A. Adamski*, Prawo karne komputerowe, s. 34–35.

[9] Dz.U. z 2015 r. poz. 728; dalej jako Konwencja o cyberprzestępczości.

Część l – „Prawo karne materialne"), tj.: nielegalny dostęp (haking), nielegalne przechwytywanie danych (podsłuch komputerowy), naruszenie integralności danych, naruszenie integralności systemu, tzw. niewłaściwe użycie urządzeń (tj. czyny dotyczące tzw. narzędzi hakerskich).

Przedmiotem niniejszego opracowania jest przede wszystkim propozycja nowelizacji przepisów kryminalizujących wskazane wyżej czyny, znajdujących się w rozdziale XXXIII Kodeksu karnego („Przestępstwa przeciwko ochronie informacji"). Jednak w trakcie prac zdecydowano się odnieść do innych, dodatkowych kwestii, rozszerzając zakres przedmiotowy opracowania o cyberstalking, kradzież tożsamości, cyberterroryzm, *spamming* oraz „przestępstwa przeciwko najintymniejszej sferze życia prywatnego".

Polska regulacja przestępstw przeciwko danym komputerowym i systemom informatycznym, zgrupowanych w rozdziale XXXIII Kodeksu karnego, swój obecny kształt zawdzięcza czterem nowelizacjom: pierwszej, przeprowadzonej ustawą z 18.3.2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń[10], mającej dostosować polskie przepisy do postanowień Konwencji o cyberprzestępczości; drugiej, dokonanej ustawą z 24.10.2008 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw[11], której celem była implementacja decyzji ramowej Rady Nr 2005/222/WSiSW z 24.2.2005 r. w sprawie ataków na systemy informatyczne[12] (dalej jako decyzja ramowa Nr 2005/222); trzeciej, przeprowadzonej ustawą z 23.3.2017 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw[13], której głównym celem było wdrożenie dyrektywy Parlamentu Europejskiego i Rady Nr 2014/42/UE z 3.4.2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej[14] oraz – „częściowo" (jak to określono w ustawie) – dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z 12.8.2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady Nr 2005/222/WSiSW[15] (dalej jako dyrektywa Nr 2013/40) oraz czwartej, będącej doskonałym przykładem tzw. wrzutki[16], dokonanej ustawą z 26.5.2023 r. o aplikacji mObywatel[17].

---

10 Dz.U. Nr 69, poz. 626.

11 Dz.U. Nr 214, poz. 1344.

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

13 Dz.U. z 2017 r. poz. 768.

14 Dz.Urz. UE L Nr 127, s. 39.

15 Dz.Urz. UE L Nr 218, s. 8.

16 „Wrzutka" – „zabieg legislacyjny" polegający na umieszczeniu w akcie prawnym (zwykle w ustawie lub w ustawie będącej nowelizacją ustawy) przepisu lub przepisów (zazwyczaj wśród przepisów końcowych, a przy braku takowych – po prostu na końcu aktu) dotyczących zmian aktu prawnego regulującego zupełnie inną problematykę, celem „ukrycia" ich istnienia – wpierw przed parlamentarzystami (założeniem jest, że umieszczone w takim miejscu przepisy zostaną pominięte (nieprzeczytane) przez nich w trakcie procesu prawodawczego (czyli niejako „przemycenia" ich w toku tego procesu), a następnie przed tzw. opinią publiczną. Jak wspomniano wyżej, doskona-

Już na wstępie należy zaznaczyć, że przestępstwa z tej grupy charakteryzują się niezwykłym zróżnicowaniem pod względem ładunku społecznej szkodliwości, a co za tym idzie, przepisy je kryminalizujące muszą przewidywać odpowiednią rozpiętość wysokości sankcji. Badania aktowe przeprowadzone w 2012 r. w Instytucie Wymiaru Sprawiedliwości pokazały, że zdecydowana większość przestępstw to czyny „drobne". Oczywiście nie należy zapominać o tym, że w przypadku przestępstw komputerowych istnieje spora ciemna liczba przestępstw – podmioty prowadzące działalność gospodarczą, zwłaszcza banki czy sklepy internetowe rzadko zgłaszają, że padły ofiarą cyberprzestępstw w trosce o swoją reputację. Badaniami, o których mowa powyżej, objęte zostały akta prokuratorskie spraw dotyczących przestępstw z art. 267 § 2, art. 268a, art. 269, art. 269a oraz art. 269b KK, które zostały zarejestrowane w powszechnych jednostkach organizacyjnych prokuratury w latach 2009–2010, czyli w zasadzie w okresie pierwszych dwóch lat obowiązywania powyższych przepisów w brzmieniu nadanym nowelizacją z 2008 r. (która weszła w życie 23.12.2008 r.). Do Instytutu Wymiaru Sprawiedliwości wpłynęło w sumie 1418 spraw (akta prokuratorskie lub ich kserokopie albo kserokopie samych postanowień, aktów oskarżenia lub wyroków). Po wstępnej selekcji polegającej na odrzuceniu spraw błędnie zakwalifikowanych (np. spraw dotyczących podsłuchu zakwalifikowanych z art. 267 § 2 KK, zamiast – jak powinno mieć to miejsce po nowelizacji z 2008 r. – art. 267 § 3 KK, art. 267b PrSpółdz[18]) lub dotyczących przestępstw niemieszczących się w zakresie badań (np. *skimming*), analizie poddano akta 1163 spraw (498 spraw z 2009 r. oraz 665 spraw z 2010 r.). Wyniki tychże badań dostępne są na stronach Instytutu Wymiaru Sprawiedliwości jako raport opublikowany w periodyku „Prawo w działaniu"[19] oraz w powoływanej już monografii „Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym". Badania te zostały przeprowadzone wprawdzie ponad dekadę temu, ale wydaje się, że można przyjąć, że obraz przestępczości komputerowej nie uległ znacznej zmianie. Tę tezę potwierdza pośrednio analiza statystyk policyjnych, które mogą w tym wypadku stanowić jedyne źródło informacji, gdyż nikt nie podjął się powtórzenia badań dotyczących problematyki przestępstw przeciwko ochronie informacji.

Niniejsze opracowanie składa się z dziesięciu rozdziałów. W rozdziale 1 i 2 zostały przedstawione w sposób krótki i zwięzły postanowienia Konwencji RE o cyberprzestępczości z 23.11.2001 r. oraz dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z 12.8.2013 r. dotyczącej ataków na systemy informatyczne, jako aktów prawnych mających decydujący wpływ na obecny kształt polskiej regulacji kwestii cyberprzestępstw.

łym przykładem zastosowania tej „procedury" jest ustawa o aplikacji mObywatel, w której zawarto przepis art. 30 przewidujący uzupełnienie zawartego w art. 269b § 1 KK katalogu przestępstw, do popełnienia których wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzeń lub programów komputerowych jest karalne – art. 270 § 1 KK (fałszerstwo materialne dokumentu) oraz 270a § 1 KK (fałszerstwo materialne faktury).

[17] Dz.U. z 2023 r. poz. 1234.

[18] T.j. Dz.U. z 2021 r. poz. 648 ze zm.

[19] *F. Radoniewicz*, Odpowiedzialność karna za przestępstwo hackingu, t. 13.

W rozdziale 3 zostały zaproponowane definicje legalne podstawowych terminów z zakresu cyberprzestępstw przeciwko ochronie informacji. Rozdział 4 zawiera propozycje nowelizacji przepisów kryminalizujących zamachy na bezpieczeństwo danych i systemów informatycznych (art. 267–269b KK). W rozdziale 5 odniesiono się do kwestii zgodności polskiej regulacji z postanowieniami Konwencji o cyberprzestępczości i dyrektywy Nr 2013/40 (a w szczególności zawartych w nich rozwiązań dotyczących „okoliczności obciążających"). Rozdział 6 poświęcony jest przestępstwu „kradzieży tożsamości" (art. 190a KK). Natomiast w 7 rozdziale przedstawiono przykłady nieumyślnych przestępstw komputerowych. Rozdział 8 poświęcony jest cyberterroryzmowi, a 9 – spammingowi. W ostatnim rozdziale 10 przedstawiono propozycję przepisów uzupełniających regulację cyberprzestępstw przeciwko prywatności. Ponadto do niniejszej publikacji dodano jako załącznik słowniczek pojęć „informatycznych" zawartych w tekście monografii (zamiast obciążać ich wyjaśnieniami tekst główny lub przypisy).

W tym miejscu pragnę podziękować Recenzentowi – Panu prof. dr. hab. *Jackowi Sobczakowi*, którego opinia utwierdziła mnie w przekonaniu, że niniejsza monografia zasługuje na publikację, oraz Panu prof. płk. dr. hab. *Tadeuszowi Zielińskiemu*, prorektorowi Akademii Sztuki Wojennej ds. dydaktycznych, bez którego życzliwej postawy zapewne nie ujrzałaby ona światła dziennego.