PRAWO W DZIAŁANIU
SPRAWY KARNE
13/2013

Filip Radoniewicz*

Odpowiedzialność karna za przestępstwo hackingu

WSTĘP

Niniejszy raport prezentuje wyniki przeprowadzonych w 2012 r. badań dotyczących szeroko pojętego hackingu (czynów zabronionych określonych w przepisach art. 267–269b kodeksu karnego[1]). Składa się z czterech zasadniczych części.

W części pierwszej przeprowadzona została analiza ustawowych znamion czynów zabronionych stypizowanych w przepisach art. 267 § 1–4, art. 268 § 1–3, art. 268a § 1–2, art. 269 § 1–2, art. 269a oraz art. 269b § 1 k.k. Omówiona również została problematyka zbiegów powyższych przepisów, wymiaru kary oraz trybu ścigania.

W części drugiej zaprezentowane zostały wyniki ogólnokrajowych badań empirycznych dotyczących hackingu, w ramach których przeanalizowano akta postępowań przygotowawczych zarejestrowanych w powszechnych jednostkach organizacyjnych prokuratury w latach 2009–2010.

W części trzeciej zawarto wnioski płynące zarówno z analizy ustawowych znamion czynów zabronionych będących przedmiotem niniejszego raportu, jak i przeprowadzonych badań.

W części czwartej przedstawione zostały wybrane stany faktyczne.

CZĘŚĆ 1. ANALIZA DOGMATYCZNA

1.1. Uwagi wprowadzające

O początkach hackingu można w zasadzie mówić już w momencie powstania pierwszych sieci telefonicznych, wtedy bowiem pojawili się tzw. phreakerzy (od ang. *phone freak* – „telefoniczny maniak"). Włamywali się oni do sieci telekomunikacyjnych, by móc nawiązywać darmowe połączenia. Inną grupą przestępców, którzy pojawili się w tym czasie byli tzw. crackerzy (od ang. *crack* – łupać), specjalizujący się w łamaniu zabezpieczeń systemów telekomunikacyjnych. Obecnie tego terminu

* Mgr Filip Radoniewicz jest doktorantem na Wydziale Prawa i Administracji Uniwersytetu Marii Curie-Skłodowskiej w Lublinie.

[1] Ustawa z 6.06.1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 ze zm.), dalej jak k.k.

używa się głównie w stosunku do „łamaczy" haseł i zabezpieczeń. Obie wyżej wskazane grupy można uznać za poprzedników dzisiejszych hackerów[2] (zresztą wielu z nich zaczynało właśnie w ten sposób swoją działalność). Początkowo termin „hacker" miał trochę inne znaczenie niż obecnie – oznaczał po prostu zdolnego programistę. Później, po zlaniu się w latach 70. XX w. subkultury hackerów z phreakerami, zaczął nabierać dzisiejszego znaczenia – kogoś działającego w podziemiu, włamującego się do komputerów i sieci, często ze szlachetnych pobudek, a czasami po prostu dla zabawy i zdobycia sławy. Taki obraz w kulturze utrwaliły filmy (zwłaszcza *Gry wojenne* Johna Badhama z 1983 r. czy *Hackerzy* Iaina Softleya z 1995 r.)[3]. Obecnie pod terminem „hacker" często rozumie się osobę, która „sieje zamęt" w Internecie, czyli zarówno włamuje się do sieci komputerowych i komputerów, jak i działa w celu zakłócenia ich pracy[4]. W języku potocznym często określenie to używane jest dla generalnego określenia przestępców działających w Internecie, w tym internetowych oszustów.

W związku z powyższym pojęcie „hacking" można rozumieć na kilka sposobów: *sensu stricto*, czyli zachowanie polegające na uzyskaniu dostępu do systemu informatycznego lub danych komputerowych, *sensu largo*, a więc jako wszelkie zamachy na bezpieczeństwo systemów i danych informatycznych (czyli również np. zakłócenie pracy systemu informatycznego, modyfikację lub zniszczenie danych komputerowych), oraz w znaczeniu najszerszym, potocznym – jako zbiorcze określenie praktycznie wszystkich przestępstw popełnianych w sieci (oczywiście z wyjątkiem np. rozpowszechniania pornografii). Przedmiotem niniejszego opracowania jest hacking *sensu largo*.

1.2. Wyjaśnienie podstawowych pojęć

Przed przejściem do analizy dogmatycznej znamion poszczególnych typów czynów zabronionych wskazane jest wyjaśnienie pewnych podstawowych terminów użytych przez ustawodawcę w treści omawianych przepisów, a mianowicie danych komputerowych (informatycznych), systemu informatycznego (oraz komputerowego), sieci telekomunikacyjnej, sieci teleinformatycznej oraz informatycznego nośnika danych. Jednocześnie konieczne jest określenie stosunku między pojęciem danych a pojęciem informacji.

Polska regulacja hackingu, czyli tzw. przestępstw komputerowych przeciwko ochronie informacji (zgrupowanych w rozdziale XXXIII k.k. „Przestępstwa przeciwko ochronie informacji", w przepisach art. 267–269b k.k.), zawdzięcza swój

[2] Termin „hacker" pochodzi od ang. *hack*, którego używali w latach 60. studenci Massachusetts Institute of Technology na określenie wyróżniających się pomysłowością żartów przez nich płatanych, http://pl.wikipedia.org/wiki/Hacker_%28slang_komputerowy%29.

[3] Por. S. Bukowski, *Przestępstwo hackingu*, „Przegląd Sądowy" 2006/4, s. 134–137; B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 53–58; D. Littlejohn Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2005, s. 65–78; J.W. Wójcik, *Przestępstwa komputerowe*, t. 1: *Fenomen cywilizacji*, Warszawa 1999, s. 187–189.

[4] Jednocześnie mamy do czynienia ze swego rodzaju paradoksem – nie ma już konieczności, by hacker w takim rozumieniu, posiadał zaawansowane umiejętności, jak jego poprzednik z wcześniejszych lat. Wystarczy, że pobierze z sieci odpowiedni program, który wszystkie czynności wykona za niego. Ukuty został nawet termin dla określenia takich osób – *script kiddies* – czyli „dzieciaki skryptowe" (skrypt – program napisany w języku skryptowym, który wykonuje pewne działania wewnątrz innego programu; w uproszczeniu jest to niesamodzielny program, np. skrypty *JavaScript* na stronach WWW, makra w dokumentach *MS Office*).

obecny kształt nowelizacji z 2008 r.[5], mającej służyć m.in. implementacji postanowień decyzji ramowej Rady 2005/222/WSiSW w sprawie ataków na systemy informatyczne[6]. W związku z tym, że pojęcia systemu informatycznego oraz danych komputerowych są w niej zdefiniowane, właściwe jest rozumienie tych terminów zgodnie z definicjami z tego aktu.

W świetle przepisu art. 1 lit. b decyzji ramowej 2005/222 dane komputerowe[7] należy rozumieć jako „każde przedstawienie faktów, informacji lub koncepcji w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem nadającym się do spowodowania wykonania funkcji przez system". Zbliżona definicja znajduje się w konwencji Rady Europy o cyberprzestępczości[8], zgodnie z którą „dane komputerowe oznaczają każde dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem nadającym się do spowodowania wykonania funkcji przez system komputerowy". Powyższe definicje danych można uznać za tożsame (zwłaszcza że obie czerpią z definicji sformułowanej przez ISO[9]). Wyraźnie z nich wynika, że dane komputerowe są nośnikiem (medium) informacji, faktów i koncepcji, które dopiero sprowadzone do postaci danych komputerowych są czytelne dla systemu informatycznego. W tym celu muszą zostać „zakodowane" w języku binarnym – zamienione w ciąg „0" i „1", a następnie mogą zostać zapisane na nośniku (np. płycie CD, DVD lub na dysku twardym) czy przesłane za pośrednictwem sieci jako impulsy energetyczne. W świetle definicji danymi komputerowymi są też programy odpowiadające za wykonywanie funkcji przez system informatyczny.

Zgodnie z powyższym informacją jest to, co można wyinterpretować, odkodować z danych. 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[10]. Uzyskanie do nich dostępu również nie zawsze musi być równoznaczne z uzyskaniem dostępu do informacji (np. w czasie transmisji danych informatycznych, kiedy to – w dużym uproszczeniu – są „zdelokalizowane", gdyż dla potrzeb transferu dzielone są na pakiety, które przesyłane są często różnymi

[5] Ustawa z 24.10.2008 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw (Dz. U. Nr 214, poz. 1344).

[6] Decyzja ramowa Rady 2005/222/WSiSW z 24.02.2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE L 69 z 2005 r., s. 67), dalej jako decyzja ramowa 2005/222.

[7] Wprawdzie polski ustawodawca użył w kodeksie karnym pojęcia danych informatycznych, ale niewątpliwie zakres przedmiotowy tego terminu jest zbieżny z danymi komputerowymi z decyzji ramowej 2005/222.

[8] Konwencja Rady Europy nr 185 o cyberprzestępczości z 23.11.2001 r., http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Polska podpisała tę konwencję właśnie 23.11.2001 r., ale jeszcze nie ratyfikowała; przepisy kodeksu karnego do jej postanowień miała dostosować ustawa z 18.03.2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. Nr 69, poz. 626).

[9] Międzynarodowa Organizacja Standaryzacyjna (ang. *International Organization for Standarization*) to międzynarodowa organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne. Z uwagi na swój pozarządowy charakter normy przez nią tworzone nie mają charakteru wiążącego dla państw. Są przez nie jednak respektowane ze względu na autorytet ISO.

[10] Zob. szerzej A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 37 i 38.

trasami i w różnej kolejności, a następnie składane w punkcie docelowym)[11]. W związku z tym w aktach prawa międzynarodowego oraz unijnego dotyczących problematyki bezpieczeństwa sieci dla określenia przedmiotu ochrony operuje się pojęciem danych komputerowych, a nie informacji. Wskazane byłoby przyjęcie takiego rozwiązania na gruncie polskiego prawa karnego.

Wyróżnia się (i chroni) trzy główne aspekty bezpieczeństwa informacji, danych komputerowych i systemów informatycznych: dostępność, integralność oraz poufność. Za zaleceniem Rady OECD C (92) 188 dotyczącym wytycznych w zakresie bezpieczeństwa systemów informatycznych[12] możemy przyjąć, iż:

- **dostępność (ang. *availability*)** informacji, danych komputerowych i systemów informatycznych oznacza, że są one osiągalne i zdatne do użytku w każdym czasie i w wymagany sposób;
- **integralność (ang. *integrity*)** jest to cecha danych i informacji oznaczająca ich dokładność i kompletność oraz utrzymywanie ich w tym stanie[13]; odnosi się zarówno do nienaruszalności danych, jak i systemów komputerowych;
- **poufność (ang. *confidentiality*)** jest to właściwość danych i informacji polegająca na ujawnianiu ich wyłącznie uprawnionym podmiotom, w dozwolonych przypadkach i w dozwolony sposób.

Jako przykładowe formy zamachów na dostępność można wskazać sabotaż, a przede wszystkim ataki DoS[14]. Do najczęściej spotykanych zamachów skierowanych przeciw integralności należą włamanie, a następnie niszczenie lub modyfikacja danych czy zawirusowanie systemu w celu skasowania danych. Formami zamachu na poufność są np. włamanie i uzyskanie dostępu do danych, czy ich przechwycenie podczas przesyłania siecią.

Dla potrzeb decyzji ramowej 2005/222 przyjęto, że systemem informatycznym jest „każde urządzenie lub grupa połączonych lub powiązanych urządzeń, z których co najmniej jedno dokonuje zgodnie z oprogramowaniem automatycznego przetwarzania danych komputerowych, jak również danych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania w dobrym stanie" (art. 1 lit. a decyzji ramowej 2005/222)[15]. Z powyższej definicji wynika, że systemem informatycznym w świetle decyzji ramowej 2005/222 jest zarówno pojedyncze urządzenie (np. komputer), jak

[11] O przesyłaniu danych w sieci zob. np. D. Littlejohn Shinder, *Cyberprzestępczość…*, s. 201-268,F. Radoniewicz, *Formy popełniania przestępstw komputerowych przeciwko bezpieczeństwu danych i systemów informatycznych*, w: M. Wędrychowicz (red.), *IV Dni Kryminalistyki Wydziału Prawa i Administracji Uniwersytetu Rzeszowskiego*, Rzeszów 2010, s. 161-166.

[12] *Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL]*; por. A. Adamski, *Prawo karne…*, s. 41.

[13] W przypadku informacji przetwarzanych w sieci informatycznej oznacza identyczność danych wysłanych z odebranymi.

[14] Atak DoS (ang. *Denial of Service* – odmowa usług) polega na wywołaniu znacznego ruchu sieciowego w celu unieruchomienia serwera lub atakowanego komputera. Bardziej jego skomplikowaną formą jest atak dDoS (ang. *Distributed Denial of Service* – rozproszona odmowa usług) przeprowadzany przy użyciu wielu komputerów przejętych w tym celu wcześniej (tzw. komputery zombie), oczywiście bez wiedzy ich użytkowników.

[15] W polskiej wersji tekstu decyzji ramowej 2005/222 zamiast zwrotu „każde urządzenie" użyto „wszelkie urządzenia".

i grupa połączonych urządzeń, czyli sieć – zarówno mała (np. lokalna), obejmująca kilka komputerów, jak i wielka, obejmująca swoim zasięgiem np. miasta. Potwierdzenie zasadności tak szerokiego rozumienia pojęcia „systemu informatycznego" znaleźć można w treści komunikatu Komisji COM (2002) 173 final[16], w którym zawarto propozycję decyzji ramowej 2005/222. W dokumencie tym wskazano, że za systemy informatyczne uważane są w szczególności komputery, telefony komórkowe oraz sieci i serwery tworzące infrastrukturę Internetu. W definicji posłużono się sformułowaniem „połączone lub powiązane", co oznacza, że urządzenia nie muszą być połączone fizycznie (np. za pomocą przewodów), a transfer danych między nimi może odbywać się za pośrednictwem innego medium (np. fal elektromagnetycznych). Przy wyjaśnieniu pojęcia automatycznego przetwarzania danych wskazane jest sięgnięcie do konwencji Rady Europy o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych[17], do której zresztą znajduje się odwołanie w treści preambuły do decyzji ramowej 2005/222. W świetle definicji zawartej w art. 2 lit. c konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych automatycznym przetwarzaniem danych są następujące czynności, jeśli w całości lub częściowo wykonywane są za pomocą procedur zautomatyzowanych: gromadzenie danych, stosowanie do nich operacji logicznych i/lub arytmetycznych, ich modyfikowanie, usuwanie, wybieranie lub rozpowszechnianie. Natomiast za procedury zautomatyzowane należy uznać takie działania, które w całości lub częściowo dokonywane są za pomocą zautomatyzowanych środków, czyli bez ingerencji człowieka[18].

Na pozór zbliżonym do systemu informatycznego pojęciem posłużono się w konwencji o cyberprzestępczości. Użyto tam terminu „system komputerowy", rozumianego jako „każde urządzenie lub zespół połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z programem, automatycznie przetwarza dane" (art. 1 lit. a konwencji o cyberprzestępczości). Jednakże zakres przedmiotowy tego terminu jest nieporównywalnie węższy niż systemu informatycznego z decyzji ramowej 2005/222. Zgodnie bowiem z oficjalnym komentarzem sporządzonym przez autorów konwencji o cyberprzestępczości[19] systemem komputerowym jest procesor lub jednostka centralna oraz ewentualne urządzenia peryferyjne (monitor, drukarka, napęd DVD itp.). Będzie to zatem telefon komórkowy, dekoder, a przede wszystkim to, co potocznie rozumie się jako samodzielny komputer osobisty, czyli pojedynczy host. Natomiast dwa lub więcej takich niezależnych, połączonych ze sobą jednostek będzie stanowiło sieć. Dlatego nie jest poprawne posłużenie się w polskim oficjalnym tłumaczeniu[20] (sporządzonym przez polskie Ministerstwo

[16] Proposal for a Council Framework Decision on attacks against information systems (COM (2002) 173 *final*) (Dz. Urz. WE C 203E z 2002 r., s. 109).

[17] Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28.01.1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25); por. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[18] Zob. szerzej F. Radoniewicz, *Problematyka ujednolicenia terminologii informatycznej – zagadnienia wybrane*, w: M. Mazuryk, S. Jaśkiewicz (red.), *Administracja publiczna w III RP. Dwie dekady doświadczeń*, Warszawa 2011, s. 685–687.

[19] *Explanatory Report,* pkt 23 i 24, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[20] Http://bip.ms.gov.pl/pl/ministerstwo/wspolpraca-miedzynarodowa/rada-europy/konwencje-rady-europy-z-obszaru-sprawiedliwosc-i-sprawy-wewnetrzne-podpisaneratyfikowane-przez-polske/.

Sprawiedliwości) konwencji o cyberprzestępczości terminem „system informatyczny", zamiast „system komputerowy" (*computer system*).

W związku z powyższym należy przyjąć, że pojęć danych informatycznych oraz danych komputerowych można – jako pojęć tożsamych – używać zamiennie, natomiast wykluczone jest to w przypadku systemu informatycznego oraz systemu komputerowego.

Kolejnym pojęciem, które należy wyjaśnić przed przejściem do głównej części opracowania, jest „sieć telekomunikacyjna". Zgodnie z definicją zawartą w przepisie art. 2 pkt 35 prawa telekomunikacyjnego[21] 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". Wskazane w definicji systemy transmisyjne to urządzenie lub zestaw urządzeń, zapewniające przesyłanie sygnałów. W zakresie przedmiotowym tego pojęcia mieszczą się nie tylko sieci o określonych zakończeniach[22], ale wszelkie systemy transmisyjne, w tym systemy radiodyfuzyjne (nadawcze). Transmisja sygnałów dokonywana jest za pomocą różnych mediów transmisyjnych[23]. Będą to zatem np. sieci satelitarne, sieci stałe wykorzystujące komutację łączy[24] oraz komutację pakietów[25], sieci telewizji kablowej czy sieci elektryczne umożliwiające transmisję sygnałów. Urządzenia komutacyjne to urządzenia służące komutacji łączy (np. centrale telefoniczne)[26], natomiast urządzenia przekierowujące – komutacji pakietów (będą to przede wszystkim routery służące trasowaniu, czyli wyznaczaniu tras i wysyłaniu nimi pakietów danych)[27].

Sieć teleinformatyczna[28] – kolejne pojęcie, które należy wyjaśnić – nie jest obecnie zdefiniowana w żadnym akcie prawnym. Natomiast znajdziemy definicję pojęcia zbliżonego – systemu teleinformatycznego. Z uwagi na panujący chaos pojęciowy w celu uporządkowania i ujednolicenia siatki terminologicznej uchwalono ustawę o zmianie ustaw w celu ujednolicenia terminologii informatycznej[29]. Odsyła ona w przypadku użycia w którejś ze wskazanych w jej treści ustaw terminu „system teleinformatyczny" do art. 3 pkt 1–4 ustawy o informatyzacji działalności

[21] Ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.), dalej jako pr. tel.

[22] Zgodnie z art. 2 pkt 52 pr. tel. przez zakończenie sieci rozumie się fizyczny punkt, w którym abonent otrzymuje dostęp do publicznej sieci telekomunikacyjnej. W przypadku sieci stosujących komutację lub przekierowywanie (zob. dalsze uwagi) zakończenie sieci identyfikuje się za pomocą konkretnego adresu sieciowego, który może być przypisany do numeru lub nazwy abonenta.

[23] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2008, s. 101.

[24] Komutacja łączy (komutacja kanałów, komutacja obwodów) – sposób transmisji głosu lub danych polegający na utworzeniu między dwoma punktami sieci (nadawcą i odbiorcą) „stałego" połączenia na czas transmisji.

[25] Komutacja pakietów – sposób transmisji danych polegający na podziale ich na fragmenty (pakiety), z których każdy może dotrzeć inną drogą do celu. Proces przesyłania pakietów nazywa się routowaniem (trasowaniem) i odbywa się pomiędzy węzłami sieci (routerami).

[26] A. Krasuski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2008, s. 63–64.

[27] Zob. szerzej np. S. Piątek, *Prawo telekomunikacyjne*…, s. 100–106; F. Radoniewicz, *Problematyka ujednolicenia*…, s. 682–684.

[28] Sieć teleinformatyczna była zdefiniowana na gruncie nieobowiązującej już ustawy z 22.01.1999 r. o ochronie informacji niejawnych (tekst jedn.: Dz. U. z 2005 r. Nr 196, poz. 1631) w jej art. 2 ust. 1 pkt 9 jako organizacyjne i techniczne połączenie systemów teleinformatycznych.

[29] Ustawa z 4.09.2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. Nr 171, poz. 1056).

podmiotów realizujących zadania publiczne[30]. Zdefiniowane w nim jest pojęcie systemu teleinformatycznego jako zespołu współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniającego 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[31]. Wynika z powyższego, iż sieć teleinformatyczna jest zespołem 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[32].

Ostatnim pojęciem, jakie należy zdefiniować, jest „informatyczny nośnik danych". W świetle przepisu art. 3 pkt 1 u.i.d.p.p. jest to „materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej". Z uwagi na to, iż definicja ta, w swoim obecnym brzmieniu, jest precyzyjna i klarowna, nie budzi w zasadzie wątpliwości zakres przedmiotowy tego pojęcia[33] – mieszczą się w nim wszystkie nośniki danych, czyli dyskietki, dyski twarde (nośniki magnetyczne), płyty CD i DVD (nośniki optyczne), pamięci półprzewodnikowe (m.in. pamięci RAM – *Random Access Memory*, ROM – *Read Only Memory*, oraz pamięci zamontowane np. w drukarkach), pamięci flash itd.

1.3. Art. 267 § 1 k.k. – hacking *sensu stricto* („kradzież informacji")

W treści art. 267 § 1 k.k. przewidziano odpowiedzialność karną za uzyskanie przez sprawcę bez uprawnienia dostępu do informacji dla niego nieprzeznaczonej, przez otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia. Czyn ten zagrożony jest karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch.

Przedmiotem ochrony przepisu art. 267 § 1 k.k. jest poufność informacji. Realizuje on konstytucyjną gwarancję wolności komunikowania się i ochronę tajemnicy komunikowania się (art. 49 oraz art. 51 ust. 1 i 2 Konstytucji[34]). Odnosi się on nie tylko do sfery prywatnej jednostki, ale obejmuje swoim zakresem również „informacje będące w dyspozycji lub przeznaczone dla osoby prawnej,

[30] Ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn.: Dz. U. z 2013 r. poz. 235 ze zm.), dalej jako u.i.d.p.p.

[31] Zgodnie z art. 2 pkt 43 pr. tel. telekomunikacyjne urządzenie końcowe jest to „urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci". W przypadku podłączenia pośredniego między urządzeniem końcowym (czyli np. kartą sieciową, telefonem, odbiornikiem telewizyjnym) a zakończeniem sieci znajduje się jeszcze urządzenie końcowe pośredniczące w przekazywaniu sygnałów, np. modem, modem DSL (ang. *Digital Subscriber Line* – cyfrowa linia abonencka; rodzaj tzw. szerokopasmowego dostępu do Internetu) czy dekoder. Możliwe jest kolejne dołączanie urządzeń końcowych do zakończenia sieci.

[32] Por. X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 62–64; A. Urbanek w: *Vademecum teleinformatyka*, J. Chustecki i in., Warszawa 1999, s. 4–5.

[33] Definicja ta jest zbliżona do sformułowanej wcześniej w piśmiennictwie; zob. J. Gołaczyński, *Elektroniczne czynności procesowe*, „Monitor Prawniczy" 2004/4 (dodatek „Prawo Mediów Elektronicznych"), s. 3; E. Rudkowska-Ząbczyk, *Pisma elektroniczne wnoszone w postępowaniu cywilnym na elektronicznych nośnikach informatycznych*, „Monitor Prawniczy" 2006/16 (dodatek „Prawo Mediów Elektronicznych"), s. 33–34.

[34] Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz. U. Nr 16, poz. 93 ze zm.).

instytucji lub organizacji, której uzyskanie jest niezgodne z wolą dysponenta (nieuprawnione), w tym informacje zakodowane elektronicznie lub magnetycznie"[35]. By odpowiedzieć na pytanie, komu przysługuje prawo do dysponowania określoną informacją, trzeba sięgnąć do regulacji konstytucyjnych, przepisów kodeksu cywilnego oraz innych ustaw szczególnych, odnoszących się do szeroko rozumianego prawa do informacji[36].

Przepis art. 267 § 1 k.k. kryminalizuje trzy zachowania będące zamachami na bezpieczeństwo systemów informatycznych: podłączenie się do sieci telekomunikacyjnej, przełamanie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia, ominięcie takiego zabezpieczenia.

Pierwsze z wyżej wskazanych znamion – podłączenie się do sieci telekomunikacyjnej – swój obecny kształt zawdzięcza nowelizacji kodeksu karnego z 2008 r. (poprzednio: „podłączenie się do przewodu służącego do przekazywania informacji"). Jak wskazano w uzasadnieniu projektu nowelizacji, zmiana ta ma rozszerzyć zakres kryminalizacji na zachowania polegające na podłączeniu się do każdej sieci, w tym bezprzewodowej, a użycie pojęcia sieci telekomunikacyjnej nawiązywać ma do prawa telekomunikacyjnego[37]. Jak słusznie wskazuje B. Kunicka-Michalska, trudno jest rozgraniczyć znamię podłączenia się od użytego w art. 267 § 3 k.k. zakładania lub posługiwania się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Z jednej strony nie jest to istotne, gdyż w obu wypadkach grozi taka sama sankcja i oba czyny ścigane są w tym samym trybie[38], ale z drugiej jednak strony jest też zasadnicza różnica – czyn z art. 267 § 1 k.k. dokonany jest tylko wtedy, gdy sprawca uzyskał dostęp do informacji, natomiast w przypadku przestępstwa z art. 267 § 3 k.k. wystarcza, by działał w celu jej uzyskania.

Zgodnie z zasługującą na aprobatę uchwałą Sądu Najwyższego z 22.01.2003 r. „działanie sprawcy, polegające na bezprawnym podłączeniu odbiornika telewizyjnego do sieci kablowej, godzi w prawa majątkowe nadawcy programu, nie wyczerpuje jednak znamion przestępstwa określonego w art. 267 § 1 k.k."[39]. W orzeczeniu tym Sąd Najwyższy trafnie podkreślił, że istotą przestępstwa z art. 267 § 1 k.k. jest uzyskanie informacji nieprzeznaczonej dla sprawcy, natomiast program emitowany w sieci kablowej przeznaczony jest dla każdego, kto opłaca abonament. Tym samym naruszone zostają jedynie prawa majątkowe operatora sieci kablowej. Ze stanowiskiem takim zgadza się B. Kunicka-Michalska[40]. Natomiast W. Wróbel odniósł się do powyższej tezy krytycznie. Uważa bowiem, że prawo do dysponowania określoną informacją związane jest także ze sposobem jej utrwalenia, a nie tylko z samą treścią[41].

Drugie z kryminalizowanych w przepisie zachowań polega na przełamaniu elektronicznego, magnetycznego, informatycznego lub innego szczególnego

[35] A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 570.
[36] W. Wróbel w: *Kodeks karny. Komentarz. Część szczególna*, t. 2: *Komentarz do artykułów 117–277 k.k.*, A. Zoll (red.), Kraków 2006, s. 1278.
[37] Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, Sejm VI kadencji, druk sejmowy nr 458, http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/458.
[38] B. Kunicka-Michalska w: *Kodeks karny. Część szczególna. Komentarz*, t. 2: *Komentarz do artykułów 222–316*, A. Wąsek, R. Zawłocki (red.), Warszawa 2010, s. 694.
[39] Uchwała SN z 22.01.2003 r. (I KPZ 40/02), OSNKW 2003/1–2, poz. 5.
[40] B. Kunicka-Michalska w: *Kodeks karny*…, s. 694–695.
[41] W. Wróbel w: *Kodeks karny*…, s. 1281–1282.

zabezpieczenia. Podkreślić należy, iż przepis art. 267 § 1 k.k. chroni tylko takie informacje przechowywane w systemach komputerowych, które zostały przez ich dysponenta zabezpieczone przed nieuprawnionym dostępem. Przez zabezpieczenia należy rozumieć „wszelkie formy utrudnienia dostępu do informacji, których usunięcie wymaga wiedzy specjalistycznej lub posiadania szczególnego urządzenia lub kodu"[42].

Dane komputerowe mogą być chronione bezpośrednio, np. przez zaszyfrowanie czy zabezpieczenie dostępu hasłem, lub pośrednio – w ramach ochrony samego systemu informatycznego – czemu służą *firewalle*[43], systemy wykrywania włamań[44] czy procedura uwierzytelniania[45]. Przez przełamanie zabezpieczeń rozumie się działanie polegające na zniwelowaniu ich funkcji ochronnej; nie musi się ono wiązać z ich zniszczeniem[46]. Dla bytu przestępstwa określonego w przepisie art. 267 § 1 k.k. niezbędne jest, by zabezpieczenie to było realne oraz aktywne w momencie ataku hackera. W przeciwnym wypadku nie dojdzie do wypełnienia znamion przestępstwa[47].

Ostatnim kryminalizowanym w przepisie art. 267 § 1 k.k. zachowaniem jest ominięcie zabezpieczeń. Znamię to zostało dodane w wyniku nowelizacji kodeksu karnego z 2008 r. W ten sposób przyjęto, że sprawca, by popełnić przestępstwo hackingu, nie musi przełamać zabezpieczenia – wystarczy, że je ominie. Pamiętać bowiem należy, że przełamanie zabezpieczeń jest tylko jedną z wielu technik (i to nawet nie najczęściej spotykaną) używanych przez hackerów do penetracji systemów komputerowych. Pozostałe sprowadzają się do ich ominięcia, a polegają na:

- wprowadzeniu w błąd człowieka (ang. *social engineering*, czyli tzw. socjotechnika, polegająca np. na podaniu się za inną osobę w celu wyłudzenia hasła albo uzyskania dostępu do pomieszczenia, gdzie jest serwer, i fizyczne podłączenie się do niego);
- wprowadzeniu w błąd systemu – wśród metod polegających na ominięciu zabezpieczeń w ten sposób należy wskazać tzw. *spoofing* (maskarada), czyli fałszowanie adresów, mające na celu wprowadzenie w błąd co do miejsca wysłania komunikatów. Najczęściej fałszowane są adresy IP

[42] W. Wróbel w: *Kodeks karny*…, s. 1282–1283.

[43] Są to urządzenia dedykowane – komputery służące ochronie sieci komputerowych wyposażone w odpowiednie oprogramowanie albo programy chroniące pojedyncze komputery, na których je zainstalowano. Ich zadaniem jest przede wszystkim filtrowanie przesyłanych danych – zwykle na kilku poziomach – w celu zablokowania potencjalnie niebezpiecznych czy – jeżeli wyposażono je w odpowiedni system – wykrywanie określonych ataków i podejmowanie odpowiednich – zdefiniowanych z góry – kroków; zob. D. Littlejohn Shinder, *Cyberprzestępczość*…, s. 368–371; J. Muszyński w: *Vademecum teleinformatyka III*, T. Janoś (red.), Warszawa 2004, s. 206–207.

[44] Zob. szerzej T. Bilski w: *Bezpieczeństwo danych w systemach informatycznych*, T. Bilski, T. Pankowski, J. Stokłosa, Warszawa 2001, s. 32–33; J. Muszyński w: *Vademecum teleinformatyka*…, s. 213–217; F. Radoniewicz, *Formy popełniania przestępstw*…, s. 177–178.

[45] Istnieje wiele metod uwierzytelniania, czyli weryfikacji tożsamości użytkownika (komputera lub procesu). Polegają one na wymogu podania jakichś danych w celu identyfikacji. W przypadku uwierzytelniania użytkowników zazwyczaj wyróżnia się następujące sposoby: „coś, co wiesz" – najczęściej polega na wymogu podania hasła lub numeru PIN, „coś, co masz" – konieczność posiadania jakiegoś przedmiotu służącego uwierzytelnianiu (np. karty chipowej), „to, kim jesteś" – jest to metoda, w którym do identyfikacji służą cechy fizyczne osoby (takie jak np. linie papilarne, tęczówka oka).

[46] 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" 2000/1, s. 71–72; P. Kozłowska-Kalisz w: *Kodeks karny. Praktyczny komentarz*, M. Mozgawa (red.), Warszawa 2012, s. 621; W. Wróbel w: *Kodeks karny*…, s. 1283.

[47] Por. S. Bukowski, *Przestępstwo hackingu*, s. 142–143; P. Kardas, *Prawnokarna ochrona*…, s. 64.

użytkowników (adres logiczny komputera nadany przez administratora sieci), ale możliwe jest fałszowanie również np. adresów WWW (celem skierowania ofiary na stronę stworzoną przez sprawcę, np. udającą witrynę banku);
- wykorzystaniu luk (błędów) w systemach operacyjnych, aplikacjach czy protokołach (są to zbiory zasad określających procesy komunikacyjne odpowiadające m.in. za identyfikację komputerów w sieci), czemu służą programy zwane *exploitami*[48].

Z popełnieniem przestępstwa z art. 267 § 1 k.k. mamy do czynienia, gdy sprawca w wyniku podłączenia się do sieci telekomunikacyjnej lub przełamania albo ominięcia zabezpieczeń bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej. Sformułowanie to zostało wprowadzone w miejsce dotychczasowego – mocno krytykowanego[49] – „kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną". Krytyka ta wynikała z dwóch zasadniczych przyczyn. Po pierwsze, nie zawsze hacker szuka informacji. Czasami dostaje się do systemu z powodów ambicjonalnych, by wykazać nieskuteczność zabezpieczeń – zdaniem brytyjskich ekspertów do spraw bezpieczeństwa systemów komputerowych taki jest cel 95% ataków[50]. Po drugie, wykazanie, że sprawca uzyskał jakiekolwiek informacje w wyniku włamania może w praktyce okazać się trudne. System operacyjny rejestruje wprawdzie wszystkie polecenia wydawane przez użytkownika (jako tzw. logi systemowe[51]), co pozwala ustalić, jakie pliki były otwierane, ale osoba posiadająca odpowiednie umiejętności jest w stanie wyłączyć rejestrację swoich działań lub wykasować po ich dokonaniu logi. Obecnie dla bytu przestępstwa z art. 267 § 1 k.k. nie jest istotne, czy uzyskana przez sprawcę informacja jest tą, której poszukiwał, a także to, czy jest dla niego w jakikolwiek sposób przydatna[52]. Karalne jest samo uzyskanie dostępu do informacji, co wiąże się z uzyskaniem dostępu do danych procedowanych przez ten system (co jest równoznaczne z uzyskaniem dostępu do systemu informatycznego lub jego części)[53]. By było możliwe postawienie sprawcy zarzutów, nie musi on ani uzyskać nad informacją władztwa (jak było przed nowelizacją z 2008 r.), ani tym bardziej się z nią zapoznać.

Przestępstwo z art. 267 § 1 k.k. ma charakter powszechny. Może je popełnić każda osoba zdolna do ponoszenia odpowiedzialności karnej, która nie jest dysponentem informacji[54]. Występek ten można popełnić tylko umyślnie, działając w zamiarze bezpośrednim, o czym świadczy sposób, w jaki ujęto znamiona wykonawcze („podłącza się do sieci telekomunikacyjnej", „przełamuje zabezpieczenie")[55].

[48] Zob. F. Radoniewicz, *Formy popełniania przestępstw*…, s. 168–176.
[49] A. Adamski, *Prawo karne*…, s. 49.
[50] A. Adamski, *Prawo karne*…, s. 48.
[51] Są to zapisy zdarzeń – zachodzących na pojedynczym komputerze lub w sieci – wraz ze wskazaniem uczestniczących w nich podmiotów; w zależności od ich umiejscowienia mogą rejestrować np. logowanie, nawiązanie połączenia, adresy odwiedzonych stron itp.
[52] M. Kalitowski w: *Kodeks karny. Komentarz*, M. Filar (red.), Warszawa 2012, s. 1207.
[53] Zob. też A. Adamski, *Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?*, „Prawo Teleinformatyczne" 2007/3, s. 6–7.
[54] W przeciwieństwie do czynu z art. 266 k.k. (czyli naruszenia tajemnicy służbowej lub zawodowej), gdzie podmiot jest określony indywidualnie (np. funkcjonariusz publiczny).
[55] Tak też A. Marek, *Kodeks karny*…, s. 571; P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 622; W. Wróbel w: *Kodeks karny*…, s. 1284.

Takie stanowisko zajął również Sąd Najwyższy w wyroku z 2.06.2003 r.[56] Inaczej uważa B. Kunicka-Michalska, według której możliwe jest popełnienie omawianego przestępstwa również w zamiarze ewentualnym[57]. Występek ten nie może być popełniony nieumyślnie. Nie sposób zatem uznać za hackera kogoś, kto przez pomyłkę zapoznaje się z informacją dla niego nieprzeznaczoną (np. korzystając w miejscu publicznym z komputera przeczyta maila osoby, która przed nim z niego korzystała i nie wylogowała się ze swojej skrzynki pocztowej) lub przypadkowo (np. w wyniku błędu systemu) „złamie" zabezpieczenia.

1.4. Art. 267 § 2 k.k. – nieuprawniony dostęp do systemu informatycznego

Nowelizacją z 2008 r. dodano do art. 267 k.k. – jako § 2 – przepis kryminalizujący działanie sprawcy polegające na uzyskaniu bez uprawnienia dostępu do całości lub części systemu informatycznego. Jego przedmiotem ochrony jest – podobnie jak przepisu art. 267 § 1 k.k. – poufność informacji. Rozwiązanie przyjęte przez ustawodawcę w przepisie art. 267 § 2 k.k. spotkało się z uzasadnioną krytyką z trzech zasadniczych powodów. Po pierwsze, jest to niejako automatyczne i dosłowne przepisanie treści art. 2 decyzji ramowej 2005/222. Należy podkreślić, że decyzje ramowe są (a w zasadzie były – w ciągu pięciu lat od wejścia w życie Traktatu Lizbońskiego[58] miały zostać uchylone lub zastąpione dyrektywami; do tego momentu jednak obowiązują[59]) instrumentami prawnymi służącymi do zbliżania przepisów porządków prawnych państw członkowskich. Określony jest w nich rezultat, jaki ma zostać osiągnięty, natomiast dobór środków ku temu prowadzących pozostawiany jest krajowym ustawodawcom. W przypadku decyzji ramowych z dziedziny prawa karnego materialnego ustawodawca krajowy ma obowiązek wprowadzenia takich zmian w porządku prawnym, by na podstawie przepisów prawa karnego możliwe było kryminalizowanie opisanych w decyzji ramowej czynów. Co za tym idzie – postanowienia decyzji ramowych sformułowane są bardzo ogólnie. Mówiąc skrótowo, ustawodawca krajowy powinien dokonać implementacji norm prawnych, a nie przepisów. W związku z tym decyzje ramowe harmonizujące prawo karne materialne nie nadają się do dosłownej transpozycji[60]. Natomiast polski ustawodawca – jak wskazano – dosłownie przepisał treść art. 2 decyzji ramowej 2005/222. A. Adamski zastosowaną „technikę legislacyjną" trafnie określił jako *copy and paste*[61].

Po drugie, w związku z powyższym przepis art. 267 § 2 k.k. jest niezwykle pojemny treściowo. Znamiona czynu w nim opisanego wypełni sprawca, który „uzyskuje nielegalny dostęp" do danych informatycznych (co nie zawsze jest jednak równoznaczne z uzyskaniem dostępu do informacji; zob. też uwagi w rozdziale 1.2), bo na tym polega – o czym była już mowa – uzyskanie dostępu do systemu,

[56] Wyrok SN z 2.06.2003 r. (II KK 232/02), LEX nr 78373.
[57] B. Kunicka-Michalska w: *Kodeks karny*…, s. 703–704.
[58] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13.12.2007 r. (Dz. Urz. UE C 306 z 1007 r., s. 1) wszedł w życie 1.12.2009 r. Ujednolicone teksty traktatów są dostępne na stronie http://eur-lex.europa.eu/pl/treaties/index.htm.
[59] Zob. szerzej J. Barcz, *Przewodnik po Traktacie z Lizbony. Traktaty stanowiące Unię Europejską. Stan obecny oraz teksty skonsolidowane w brzmieniu Traktatu z Lizbony*, Warszawa 2008, s. 64.
[60] Zob. szerzej np. A. Grzelak, *Trzeci filar Unii Europejskiej*, Warszawa 2008, s. 118–123.
[61] A. Adamski, *Nowe ujęcie cyberprzestępstw*…, s. 7–8.

przy czym by odpowiadać karnie, nie musi w tym celu ani łamać zabezpieczenia, ani go omijać. Jedyny warunek stanowi, by dostęp ów był nieuprawniony. Można by się zastanawiać, czy ustawodawca w ten sposób usiłował stworzyć swego rodzaju typ podstawowy przestępstwa hackingu (art. 267 § 2 k.k.) oraz jego typ kwalifikowany (art. 267 § 1 k.k.), wymagający działania polegającego na pokonaniu zabezpieczeń, a co za tym idzie – działania bardziej szkodliwego społecznie. Wyklucza to jednak fakt, iż oba występki zagrożone są identyczną sankcją – karą pozbawienia wolności do lat dwóch. Wydaje się w związku z tym, że najbardziej racjonalnym rozwiązaniem jest przyjęcie, iż przepis art. 267 § 2 k.k. będzie znajdował zastosowanie w przypadkach, gdy głównym elementem czynu sprawcy było samo uzyskanie dostępu do całości lub części systemu informatycznego, a nie uzyskanie dostępu do informacji. Z sytuacją taką mamy do czynienia np. w wypadku włamania się na konto w serwisie aukcyjnym w celu wykorzystania go do popełnienia przestępstwa oszustwa, uzyskaniu dostępu do profilu na portalu społecznościowym, a następnie modyfikacji zawartych w nim danych, czy włamaniu na konto użytkownika gry MMORPG w celu zaboru wirtualnych przedmiotów lub postaci (wszystkie te kwestie zostaną szczegółowo omówione w dalszej części). 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. (przy identycznym zagrożeniu sankcją)[62].

Po trzecie – jak wyżej wspomniano – jedynym warunkiem, który musi zostać spełniony, by możliwe było postawienie sprawcy zarzutu naruszenia przepisu art. 267 § 2 k.k., jest uzyskanie przez niego dostępu do systemu bez uprawnień. Natomiast kwestię uprawnień użytkowników sieci komputerowych regulują przede wszystkim takie „akty" jak regulaminy, a nie przepisy o randze ustawowej. To swego rodzaju odesłanie przez ustawodawcę do norm pozaprawnych jest niebezpieczne i trudne do pogodzenia z zasadą określoności przestępstwa[63].

1.5. Art. 267 § 3 k.k. – nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych

Przepis art. 267 § 3 k.k. sankcjonuje konstytucyjne gwarancje prawa do ochrony życia prywatnego (art. 47 Konstytucji), wolności komunikowania się i ochrony prywatności tej komunikacji (art. 49 Konstytucji), a także nienaruszalności mieszkania (art. 51 Konstytucji). Wymienione wartości są chronione również na gruncie obowiązujących Polskę umów międzynarodowych – Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[64] (art. 8: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji") oraz Międzynarodowego Paktu Praw Obywatelskich i Politycznych[65]

[62] Zob. F. Radoniewicz, *Ujęcie cyberprzestępstw w Kodeksie karnym z 1997 roku a postanowienia decyzji ramowej Rady 2005/222/WSiSW w sprawie ataków na systemy informatyczne*, „Ius Novum" 2009/1, s. 57–58.
[63] Zwraca na to uwagę A. Adamski; zob. A. Adamski, *Nowe ujęcie cyberprzestępstw*…, s. 8.
[64] Konwencja o Ochronie Praw Człowieka i Podstawowych wolności sporządzona w Rzymie 4.11.1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.).
[65] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku 19.12.1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167).

(art. 17: „Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię")[66].

Przedmiotem ochrony omawianego przepisu jest poufność informacji oraz innych form komunikacji międzyludzkiej. Ponadto na jego podstawie można karać wiele działań polegających na ingerencji w życie prywatne. Przykładowo wskazać można tu naruszenie swobodnego korzystania z mieszkania przez inwigilację za pomocą urządzeń podsłuchowych czy wizualnych bądź też przechwytywanie informacji przesyłanych siecią telekomunikacyjną[67]. Zakres informacji chronionych przez ten przepis jest bardzo szeroki. Według B. Kunickiej-Michalskiej[68] chroni on zarówno tajemnice prywatne (tj. związane z prywatną i intymną sferą życia człowieka), jak również tajemnice niechronione przez inne przepisy szczególne[69].

Przepis art. 267 § 3 k.k. penalizuje zakładanie lub posługiwanie się – w celu uzyskania informacji – podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Wprowadzenie tego ostatniego terminu jako narzędzia służącego inwigilacji ucina dywagacje na temat, czy program komputerowy można za narzędzie uznać[70]. Przepis ten również można wykorzystywać do kryminalizacji niektórych postaci hackingu. Nie ulega bowiem wątpliwości, że za zachowanie wyczerpujące znamiona przepisu art. 267 § 3 k.k. uznać można działanie hackera polegające na zainstalowaniu w komputerze osoby inwigilowanej programu do przekazywania danych[71], takiego jak:

- koń trojański (trojan) – z pozoru użyteczny program wykonujący działania nieleżące w intencji użytkownika, jednocześnie pozostające poza jego świadomością. Służy on do obejścia zabezpieczeń – po zainstalowaniu i uruchomieniu takiego programu hacker ma otwartą drogę do systemu. Jednocześnie sam trojan może wykonywać pewne działania polegające np. na modyfikacji lub usuwaniu plików, przesyłaniu danych do napastnika, instalowaniu innych programów lub wirusów. Ponieważ trojan może wykonywać zazwyczaj wszystkie czynności, do których uprawniony jest użytkownik, szczególnie niebezpieczna jest sytuacja, gdy zainstaluje go osoba z uprawnieniami administratora. Trojany mogą być zamaskowane jako niewinne programy, np. narzędzia, wygaszacze ekranu, makra w dokumentach *MS Office*. Zdarza się, że są umieszczane jako skrypty wykonywalne (np. *JavaScript*, kontrolki *ActiveX*) na stronie internetowej. Dlatego też wejście na taką witrynę może spowodować automatyczną instalację trojana w systemie (jeśli oczywiście przeglądarka użytkownika ma włączoną opcję automatycznego uruchamiania skryptów);

[66] A. Adamski, *Prawo karne*…, s. 56–57.
[67] A. Adamski, *Prawo karne*…, s. 57.
[68] B. Kunicka-Michalska w: *Kodeks karny*…, s. 698–699.
[69] Inaczej L. Gardocki, według którego służy on jedynie ochronie życia prywatnego; zob. L. Gardocki, *Prawo karne*, Warszawa 2006, s. 302–303.
[70] W pierwotnej wersji projektu nowelizacji była mowa o oprogramowaniu specjalnym. W toku prac w sejmie słusznie usunięto jednak przymiotnik „specjalne", który mógł sugerować, że chodzi o programy komputerowe stworzone wyłącznie do popełnienia przestępstwa, podczas gdy w wielu wypadkach mamy do czynienia z programami „o podwójnej naturze" – spełniającymi wiele funkcji, ale mogącymi być wykorzystanymi (często wbrew woli i zamierzeniom ich twórców) przez przestępców; zob. szerzej dalsze uwagi dotyczące art. 269b k.k.
[71] A. Adamski, *Prawo karne*…, s. 59; W. Wróbel w: *Kodeks karny*…, s. 1287.

- program należący do kategorii oprogramowania szpiegującego (ang. *spyware*), przesyłający osobie, która go umieściła, informacje na temat użytkownika, w którego systemie funkcjonuje, takie jak adresy odwiedzanych stron WWW, dane osobowe, numery kart płatniczych, hasła;
- program „tylne drzwi" (ang. *back door*) – program umożliwiający intruzowi wejście do systemu operacyjnego z pominięciem zabezpieczeń. Zazwyczaj jest instalowany przez hackera, który po włamaniu do systemu operacyjnego pozostawia sobie w ten sposób „furtkę";
- rejestrator klawiatury (ang. *keylogger*) – program przejmujący kontrolę nad procedurami systemu operacyjnego służącymi do obsługi klawiatury. W specjalnym pliku rejestruje on każde naciśnięcia klawiszy klawiatury, dzięki czemu może przechwytywać hasła. Zazwyczaj jest wyposażony w funkcję umożliwiającą przesłanie uzyskanych danych osobie, która go w systemie operacyjnym umieściła za pośrednictwem sieci.

W przepisie art. 267 § 3 k.k. ustawodawca użył znamion alternatywnych – by pociągnąć sprawcę do odpowiedzialności wystarczy, by jedynie zainstalował on urządzenie lub program (nie musi potem z niego korzystać) lub posługiwał się narzędziem (lub programem) założonym (umieszczonym w systemie informatycznym) przez kogoś innego. Dla bytu omawianego przestępstwa wystarcza dokonanie którejś z wymienionych czynności. Natomiast sama okoliczność faktycznego uzyskania w ten sposób informacji nie ma znaczenia[72].

Inwigilację systemów informatycznych często określa się mianem podsłuchu komputerowego. Wyróżnia się dwa jego rodzaje: pasywny (gdy sprawca jedynie zapoznaje się z treścią przesyłanych informacji) oraz aktywny (gdy dokonuje modyfikacji przesyłanych danych, np. poprzez przekierowanie transmisji danych do innego miejsca w sieci)[73].

Wśród sposobów infiltrowania sieci polegających na przechwytywaniu danych w czasie ich transmisji bez ingerencji w ich treść wskazać należy przede wszystkim tzw. *sniffing* (po polsku „węszenie"), czyli przechwytywanie pakietów (w uproszczeniu „porcji", na jakie dzielone są dane, by mogły być przesłane siecią) oraz ich filtrowanie pod kątem poszukiwanych danych. Sprawca może posłużyć się w tym celu specjalnym programem (tzw. *snifferem*) albo narzędziem służącym administratorom sieci do jej monitorowania (np. *NetMon* (*Network Monitor*) implementowany we wszystkich nowszych systemach Microsoftu). Przykładem podsłuchu aktywnego jest atak *man in the middle* (czyli „człowiek pośrodku"), polegający – w znacznym uproszczeniu – na „wpięciu się" w trwającą transmisję danych między dwoma komputerami i – w rezultacie – niejako pośredniczeniu w procesie wymiany wiadomości między nimi[74].

Przestępstwo z art. 267 § 3 k.k. ma charakter formalny w zakresie czynności posługiwania się urządzeniem, w odniesieniu do czynności zakładania

[72] W. Wróbel w: *Kodeks karny*…, s. 1285.
[73] Por. A. Kiedrowicz, *Zagadnienie kontroli przekazów informacji w ramach telefonii internetowej*, „Prokuratura i Prawo" 2008/10, s. 126–127; zob. szerzej np. J.W. Wójcik, *Przestępstwa komputerowe*…, s. 148–152.
[74] Zob. szerzej np. http://pl.wikipedia.org/wiki/Atak_man_in_the_middle.

ma charakter materialny (skutek następuje, gdy urządzenie zostaje zainstalowane zgodnie z wolą sprawcy)[75].

Omawiane przestępstwo ma charakter powszechny. Nie może być oczywiście popełnione przez osobę uprawnioną do uzyskania informacji.

Przestępstwo określone w przepisie art. 267 § 3 k.k. można popełnić jedynie umyślnie w zamiarze bezpośrednim kierunkowym, na co wskazuje zwrot „w celu uzyskania informacji". Osoba instalująca urządzenie służące do inwigilacji ponosi odpowiedzialność na podstawie omawianego przepisu, jeżeli ma świadomość, że nie jest uprawniona do tego. Zleceniodawca takich czynności będzie odpowiadać za sprawstwo kierownicze lub polecające.

Bezprawność czynu z art. 267 § 3 zostaje uchylona, jeśli zachowanie wypełniające znamiona jest legalnym działaniem organów ścigania (wynika z odpowiednich przepisów[76]).

1.6. Art. 267 § 4 k.k. – ujawnienie informacji uzyskanej nielegalnie

W przepisie art. 267 § 4 k.k. przewidziano odpowiedzialność za czyn polegający na ujawnieniu innej osobie informacji uzyskanej w wyniku działań kryminalizowanych w przepisach art. 267 § 1–3 k.k. Jest to przestępstwo powszechne, co oznacza, że popełnić je może każdy, kto przekazuje nielegalne informacje, wiedząc o źródle ich pochodzenia (a więc nie tylko sprawca występku z art. 267 § 1, § 2 lub § 3 k.k., który bezpośrednio je uzyskał). Ujawnienie informacji może polegać zarówno na działaniu, jak i zaniechaniu. Jest to przestępstwo materialne – jego skutkiem jest dojście informacji do innej osoby (może to być jedna, konkretna osoba, a także nieokreślony krąg osób, gdy sprawca posługuje się mediami). Może być popełnione tylko umyślnie, w obu postaciach zamiaru[77]. Ustawodawca nie przewidział kwalifikowanego typu tego przestępstwa, polegającego na posłużeniu się przez sprawcę w celu ujawnienia informacji środkami masowego przekazu, jak to uczynił np. w przypadku czynu zabronionego przewidzianego w przepisie art. 212 k.k. (zniesławienie)[78].

1.7. Art. 268 k.k. – naruszenie integralności zapisu informacji

Przepis art. 268 § 2 k.k. kryminalizuje bezprawne zachowania polegające na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu istotnej informacji na informatycznym nośniku danych albo udaremnianiu lub znacznym utrudnianiu w inny sposób osobie uprawnionej zapoznania się z informacją utrwaloną na takim nośniku. Ze względu na większą szkodliwość społeczną tego czynu stanowi on typ kwalifikowany przestępstwa z art. 268 § 1 k.k.

Przedmiotem ochrony jest integralność zapisu informacji (mowa jest o całkowitym unicestwieniu zapisu – wskazują na to zwroty „niszczy", „usuwa", oraz

[75] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 622; por. A. Marek, *Kodeks karny*…, s. 572; inaczej S. Hoc w: *Kodeks karny. Komentarz*, R.A. Stefański (red.), Legalis 2012, komentarz do art. 267.

[76] Przede wszystkim należy wskazać przepisy kodeksu postępowania karnego, ustawy z 6.04.1990 r. o Policji (tekst jedn.: Dz. U. z 2011 r. Nr 287, poz. 1687 ze zm.), ustawy z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn.: Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.).

[77] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 622; W. Wróbel w: *Kodeks karny*…, s. 1289.

[78] B. Kunicka-Michalska w: *Kodeks karny*…, s. 701.

o modyfikacji bez unicestwienia, ale w stopniu znacznym – „uszkadza", „zmienia") oraz jej dostępność (czyli możliwość korzystania) dla osoby uprawnionej. Ustawodawca jednocześnie wymaga, aby była to informacja „istotna" – przede wszystkim w sensie obiektywnym (ze względu na jej treść, wagę i znaczenie[79]) – ale z uwzględnieniem interesów osoby uprawnionej do zapoznania się z nią[80], w tym celu, jakiemu służyła lub miała służyć[81].

Przedmiotem czynności wykonawczej – zgodnie z literalnym brzmieniem – są dane informatyczne zapisane na informatycznym nośniku danych. W związku z tym uważam, że przepis art. 268 § 2 k.k. nie znajdzie zastosowania do sytuacji, gdy utrudnienie w zapoznaniu się z informacją będzie rezultatem zachowań polegających na zakłócaniu pracy sieci. Zostanie on wtedy pochłonięty przez przepis art. 268a lub 269a k.k.

Działania wymienione w tym przepisie mogą być zarówno celem działania sprawcy, jak i środkiem do niego prowadzącym (np. umieszczenie w atakowanym systemie trojana lub programu „tylnych drzwi"). Mogą one również stanowić sposób zatarcia przez hackera śladów jego obecności w systemie (np. modyfikacja logów).

Pierwszą grupę czynności wykonawczych – jak wskazano wyżej – stanowią czyny godzące w integralność danych. Będą to przede wszystkim działania o charakterze logicznym, polegające np. na ich kasowaniu, usuwaniu, często za pomocą specjalnych programów takich jak wirusy, robaki, trojany. Dane na informatycznym nośniku danych można unicestwić również poprzez działania fizyczne, np. niszcząc nośnik czy uszkadzając go (np. poprzez umieszczenie w polu elektromagnetycznym).

Druga grupa czynności wykonawczych – udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznania się z informacją – ma charakter dopełniający. Użyte przez ustawodawcę sformułowanie jest bardzo pojemne[82]. Zachowanie sprawcy może polegać np. na zmianie sposobu zakodowania informacji, nawet bez zmiany jej treści, ukryciu nośnika, zamontowaniu hasła uniemożliwiającego dostęp czy zniszczeniu programu umożliwiającego zapoznanie się z informacją[83].

Przepis art. 268 § 3 k.k. jest typem kwalifikowanym przestępstwa naruszenia integralności zapisu informacji. Znamieniem kwalifikującym jest wyrządzenie przez sprawcę znacznej szkody majątkowej[84]. Niewątpliwie chodzi tu nie o wartość informatycznego nośnika danych (która może być symboliczna), ale o szkodę, jaką faktycznie ponosi dysponent informacji w następstwie czynu, np. mogą to być koszty związane z odtworzeniem zapisów księgowości czy utracony przez autora dzieła zysk związany z jego sprzedażą[85]. Jak wskazuje W. Wróbel, szkoda majątkowa może być następstwem czynu zabronionego określonego w omawianym przepisie, gdy pokrzywdzony wskutek niemożności zapoznania się z określoną informacją podejmuje decyzje majątkowe,

[79] P. Kardas, *Prawnokarna ochrona*…, s. 88.
[80] P. Kardas, *Prawnokarna ochrona*…, s. 88; P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 624; W. Wróbel w: *Kodeks karny*…, s. 1296.
[81] O. Górniok w: *Kodeks karny. Komentarz*, t. 2, O. Górniok, S. Hoc, M. Kalitowski, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, Gdańsk 2005, s. 363–364; M. Kalitowski w: *Kodeks karny*…, s. 1209.
[82] P. Kardas, *Prawnokarna ochrona*…, s. 90.
[83] W. Wróbel w: *Kodeks karny*…, s. 1293–1294.
[84] Przez znaczną szkodę majątkową rozumie się (zgodnie z przepisami art. 115 § 7 w zw. z § 5 k.k.) szkodę, której wartość w czasie popełnienia czynu zabronionego przekracza 200.000 zł.
[85] A. Marek, *Kodeks karny*…, s. 573; tak też B. Kunicka-Michalska w: *Kodeks karny*…, s. 715–716.

które przynoszą mu straty[86]. Obejmuje ona zarówno uszczerbek w majątku pokrzywdzonego (*damnum emergens*), jak i utracone korzyści (*lucrum cessans*)[87]. W związku z faktem, że Internet jest w coraz większym stopniu wykorzystywany do wszelkiego rodzaju działalności gospodarczej, problem z tego typu przestępstwami będzie wzrastał.

Omawiany czyn może popełnić każda osoba, która nie jest uprawniona do uzyskania określonej informacji, a w szczególności zaś nie jest jej dysponentem. Jest to zatem przestępstwo powszechne[88].

Według B. Kunickiej-Michalskiej pojęcie uprawnienia ma charakter konkretny, związany z określona pracą, działalnością, czynnościami. Zakres oraz istota uprawnień wynika z konkretnych przepisów, które określają zarówno rodzaj informacji, jak i jej dysponenta i sposób przekazywania kompetencji[89]. Ustawami przewidującymi takie uprawnienia są przede wszystkim ustawa o ochronie danych osobowych[90] i ustawa o ochronie informacji niejawnych[91]. Pierwsza z nich przyznaje ściśle określonym podmiotom uprawnienia do przetwarzania danych osobowych, druga zakreśla krąg osób uprawnionych do zapoznania się z informacjami objętymi klauzulami tajności. Osobą uprawnioną jest z mocy prawa administrator danych (zob. art. 7 pkt 4 u.o.d.o.) oraz osoby działające na jego polecenie, rozumiane jako przekazanie im pewnych zadań (zob. art. 31 u.o.d.o.)[92]. Uprawnienie takie może wynikać również z woli dysponenta informacji[93].

Popełnienie omawianego przestępstwa możliwe jest zarówno przez działanie, jak i przez zaniechanie[94]. Czyn zabroniony z art. 268 § 3 k.k. nie jest typem kwalifikowanym przez następstwo, stąd też art. 9 § 3 k.k. nie ma zastosowania[95]. W zasadzie panuje zgoda w doktrynie, że wchodzi tu w grę tylko wina umyślna, zarówno w postaci zamiaru bezpośredniego, jak i ewentualnego[96] – sprawca musi co najmniej godzić się na to, że jego działanie może skutkować uniemożliwieniem lub znacznym utrudnieniem zapoznania się z istotną informacją przez uprawnioną osobę. Nie jest możliwe popełnienie tego występku nieumyślnie. Przykładowo nie wypełnia znamion niezachowanie ostrożności przy korzystaniu z komputera podłączonego do sieci i przypadkowe zainfekowanie pozostałych pracujących w niej komputerów wirusem otrzymanym jako załącznik do poczty elektronicznej.

Ustalenie motywów sprawcy konieczne jest dla stwierdzenia, czy nie zostały wypełnione znamiona innych przestępstw komputerowych, np. oszustwa komputerowego (art. 287 k.k.).

---

[86] W. Wróbel w: *Kodeks karny*…, s. 1295.
[87] P. Kardas, *Prawnokarna ochrona*…, s. 92.
[88] O. Górniok w: *Kodeks karny*…, s. 363; P. Kardas, *Prawnokarna ochrona*…, s. 90–91; P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 625; B. Kunicka-Michalska w: *Kodeks karny*…, s. 716; W. Wróbel w: *Kodeks karny*…, s. 1292.
[89] B. Kunicka-Michalska w: *Kodeks karny*…, s. 716–117.
[90] Ustawa z 29.08.1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), dalej jako u.o.d.o.
[91] Ustawa z 5.08.2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).
[92] B. Kunicka-Michalska w: *Kodeks karny*…, s. 716–717.
[93] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 624.
[94] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 625.
[95] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 625; B. Kunicka-Michalska w: *Kodeks karny*…, s. 717; W. Wróbel w: *Kodeks karny*…, s. 1296; A. Marek, *Kodeks karny*…, s. 573; inaczej O. Górniok w: *Kodeks karny*…, s. 364.
[96] Odmiennie A. Marek, który uważa, że „usuwanie", „zmienianie", „udaremnianie" lub „utrudnianie" wymagają zamiaru bezpośredniego; zob. A. Marek, *Kodeks karny*…, s. 573.

1.8. Art. 268a k.k. – naruszenie integralności danych, utrudnianie dostępu do danych oraz zakłócanie ich przetwarzania

Przepis ten (podobnie jak art. 269a i art. 269b k.k.) został wprowadzony do kodeksu karnego nowelizacją z 2004 r. w związku z podpisaniem przez Polskę 23.11.2001 r. konwencji o cyberprzestępczości. Przewiduje on karę pozbawienia wolności do trzech lat za nieuprawnione niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych albo za zakłócanie w stopniu istotnym lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych.

Przedmiotem ochrony przepisu art. 268a k.k. są dane informatyczne, a dokładnie – ich integralność (w przepisie jest mowa o niszczeniu, uszkadzaniu, usuwaniu danych), ich dostępność (bezpieczne gromadzenie, przetwarzanie i przekazywanie)[97].

Ustawodawca nie użył w treści omawianego przepisu pojęcia systemu informatycznego. Nie ulega jednak wątpliwości, że środowiskiem, w którym następuje przetwarzanie, gromadzenie lub przekazywanie danych, jest właśnie system informatyczny.

Przepis art. 268a § 1 k.k. sformułowany jest niezwykle nieprecyzyjnie. Brzmi on dosłownie: „kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych". Wątpliwości powstają przy próbie odpowiedzi na pytanie, co jest przedmiotem wykonawczym kryminalizowanych zachowań polegających na „niszczeniu", „uszkadzaniu", „usuwaniu", „zmienianiu"? Czy jest to – jak wynika z literalnego brzmienia – dostęp do danych informatycznych, czy dane informatyczne? Skłaniam się ku tej drugiej interpretacji jako logiczniejszej[98].

Pierwsza część przepisu art. 268a § 1 k.k. kryminalizuje działania polegające na niszczeniu, modyfikacji danych i utrudnianiu do nich dostępu. Omówione już one zostały wcześniej. W drugiej części przepisu penalizowane są działania polegające 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 te procesy, których skutkiem jest ich nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych informatycznych[99].

Pojęcie istotnego stopnia zakłócenia jest pojęciem nieostrym. Stopień zakłócenia bowiem może być różnie oceniany. Nie chodzi tu o ocenę jedynie subiektywną, lecz także obiektywną. B. Kunicka-Michalska uważa, że taka sytuacja zachodzi, gdy w ocenie przeciętnego użytkownika nie jest możliwe szybkie i niekłopotliwe usunięcie zakłócenia[100].

---

[97] Por. P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 625; W. Wróbel w: *Kodeks karny*…, s. 1299–1300; B. Kunicka-Michalska w: *Kodeks karny*…, s. 720. Inaczej A. Adamski, który uważa, że przepis art. 268a k.k. chroni jedynie dostępność danych (zob. A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005/4, s. 58–59), oraz A. Marek, który zawęża przedmiot ochrony tego przepisu do baz danych (zob. A. Marek, *Kodeks karny*…, s. 574).

[98] Podobnie P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 626; W. Wróbel w: *Kodeks karny*…, s 1300; przeciwnie B. Kunicka-Michalska w: *Kodeks karny*…, s. 720–721; A. Adamski, *Cyberprzestępczość*…, s. 59; S. Hoc w: *Kodeks karny*…, komentarz do art. 268a.

[99] W. Wróbel w: *Kodeks karny*…, s. 1302.

[100] B. Kunicka-Michalska w: *Kodeks karny*…, s. 736.

Przepis art. 268a § 2 k.k. przewiduje typ kwalifikowany przestępstwa z art. 268a § 1 k.k. Znamieniem kwalifikującym jest spowodowanie przez sprawcę znacznej szkody majątkowej, a grożącą sankcją – kara pozbawienia wolności od trzech miesięcy do pięciu lat.

Omawiane przestępstwo ma charakter materialny. Skutkiem jest zniszczenie, uszkodzenie, usunięcie lub zmiana danych, jak również zakłócenie oraz uniemożliwienie ich przetwarzania, gromadzenia i przekazywania (art. 268a § 1 k.k.), aż wreszcie spowodowanie takim działaniem znacznej szkody majątkowej (art. 268a § 2 k.k.).

Jest to przestępstwo powszechne. Można je popełnić zarówno przez działanie, jak i zaniechanie[101].

Oba typy omawianego przestępstwa mają charakter umyślny, mogą być popełnione zarówno w zamiarze bezpośrednim, jak i ewentualnym[102]. Nietrafny jest w związku z tym pogląd spotykany w doktrynie[103], iż może tu wchodzić w grę wina kombinowana (art. 9 § 3 k.k.), gdyż przepis mówi nie o następstwach, lecz o skutku[104].

Sprawcy omawianego przestępstwa kierują się różnymi motywami. Często są to ambicje hackerów pragnących zaprezentować swoje umiejętności. Przykładowo tak właśnie m.in. powstały wirusy wykorzystujące wiadomości pocztowe HTML, wirusy wieloplatformowe (infekujące zarówno systemy Windows, jak i Linuks) czy wirusy-pliki graficzne.

Czasami można mówić wręcz o podłożu ideologicznym – jako przykłady można podać ataki dokonywane na izraelskie serwery przez hackerów palestyńskich czy atakowanie witryny WWW Telekomunikacji Polskiej, uważanej przez wielu polskich użytkowników Internetu za monopolistę utrudniającego rozwój usług internetowych.

Ustalenie motywów sprawcy – podobnie jak w przypadku art. 268 § 2 i 3 k.k. – jest niezbędne dla stwierdzenia, czy nie zostały wypełnione znamiona innych przestępstw komputerowych, np. oszustwa komputerowego (art. 287 k.k.).

1.9. Art. 269 k.k. – sabotaż informatyczny

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.

[101] S. Hoc w: *Kodeks karny*…, komentarz do art. 268a.
[102] J. Piórkowska-Flieger w: *Kodeks karny. Komentarz*, T. Bojarski (red.), Warszawa 2012, s. 709. Według A. Marka formy wykonawcze wymagają zamiaru bezpośredniego, natomiast istotność zakłócenia w art. 268a § 1 k.k. oraz wielkość szkody w art. 268a § 2 k.k. mogą być objęte zamiarem ewentualnym (A. Marek, *Kodeks karny*…, s. 574).
[103] M. Kalitowski w: *Kodeks karny*…, s. 1210.
[104] S. Hoc w: *Kodeks karny*…, komentarz do art. 268a.

Zagrożone jest ono wysoką sankcją – karą pozbawienia wolności od sześciu miesięcy do ośmiu lat.

Przedmiotem ochrony przepisów art. 269 § 1 i 2 k.k. jest integralność oraz dostępność danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. Omawiane przepisy chronią zatem szczególne informacje, ponadto – pośrednio – obronność kraju (termin ten odnosi się zarówno do bezpieczeństwa zewnętrznego, jak i – jak się zdaje – wewnętrznego), bezpieczeństwo w komunikacji (w ruchu lądowym, morskim i powietrznym) oraz funkcjonowanie szeroko pojętej administracji państwowej. Według B. Kunickiej-Michalskiej właśnie te wartości są ich podstawowym przedmiotem ochrony[105].

Sabotaż informatyczny uważa się za typ kwalifikowany w stosunku do przestępstw z art. 268 § 2, art. 268a i art. 269a k.k. Znamieniem kwalifikującym jest tu rodzaj chronionych danych. Są to dane informatyczne mające szczególne znaczenie dla wymienionych w przepisie art. 269 § 1 k.k. wartości, czyli – jak była mowa wyżej – obronność kraju, bezpieczeństwo w komunikacji oraz niezakłócone funkcjonowanie administracji państwa.

Konstruując typ przestępstwa z art. 269 § 1 k.k., ustawodawca posłużył się alternatywnymi znamionami[106]. Pierwsza ich grupa to 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. Przedmiot ochrony stanowi w tym wypadku integralność danych należących do wskazanej w nim kategorii. Działania wymienione w dyspozycji są karalne niezależnie od tego, czy istnieje kopia zniszczonych lub zmodyfikowanych danych, czy też nie. Przedmiotem wykonawczym są dane informatyczne. Przez niszczenie, usuwanie należy rozumieć całkowite unicestwienie danych, natomiast przez zmianę, uszkodzenie – ich modyfikację w stopniu znacznym. Zamachy te mają charakter logiczny.

Na drugą grupę znamion, wymienionych w drugiej części przepisu art. 269 § 1 k.k., składa się zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania organów administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. W tym wypadku przedmiotem ochrony jest dostępność danych o szczególnym znaczeniu dla wymienionych w przepisie wartości. Znaczenie użytych w omawianym przepisie terminów oraz sposoby działań sprawcy są identyczne z poddanymi analizie przy charakterystyce czynu zabronionego określonego w art. 268a k.k.

Środowiskiem popełnienia omawianego przestępstwa może być zarówno sieć lokalna, służąca do przetwarzania chronionych informacji, jak i sieć publiczna (np. Internet), jeśli temu celowi służy[107].

[105] B. Kunicka-Michalska w: *Kodeks karny*..., s. 728.
[106] Por. A. Adamski, *Prawo karne*..., s. 77–78.
[107] Por. A. Adamski, *Prawo karne*..., s. 78–79.

Przepis art. 269 § 2 k.k. chroni określone w treści art. 269 § 1 k.k. dane informatyczne przed zamachami o charakterze fizycznym, polegającymi na niszczeniu albo wymianie informatycznego nośnika danych lub niszczeniu albo uszkadzaniu urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania takich danych informatycznych. Efektem wymienionych zachowań może być zarówno fizyczne unicestwienie danych (np. w wyniku zniszczenia dysków twardych w serwerze), jak i utrudnienie lub uniemożliwienie ich przetwarzania (np. w rezultacie uszkodzenia urządzeń sieciowych).

Nie stanowi przestępstwa sabotażu informatycznego uszkodzenie przez sprawcę samych kabli czy przewodów służących do transmisji – nie można ich uznać za urządzenia. Według W. Wróbla działania takie mogą natomiast być uznane za zakłócenie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych[108].

Przestępstwo sabotażu informatycznego ma charakter materialny[109]. Dla jego bytu konieczne jest wystąpienie skutku w postaci unicestwienia lub uszkodzenia określonych w przepisie art. 269 § 1 k.k. danych albo zakłócenia lub uniemożliwienia automatycznego ich przetwarzania, gromadzenia lub przekazywania, obojętne czy w wyniku ataku logicznego (art. 269 § 1 k.k.), czy działania fizycznego (art. 269 § 2 k.k.)[110]. Jest to przestępstwo o charakterze powszechnym.

Strona podmiotowa omawianego przestępstwa obejmuje obie odmiany umyślności – zarówno zamiar bezpośredni, jak i ewentualny. Sprawca musi chcieć popełnienia tego czynu lub przynajmniej godzić się, że swoim zachowaniem wypełni znamiona przestępstwa[111]. Musi mieć ponadto świadomość, że dane, z którymi ma do czynienia, mają lub mogą mieć szczególne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania organów administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, albo że jego zachowanie doprowadzi lub może doprowadzić do zakłócenia lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. W przypadku czynów z art. 269 § 2 k.k. sprawca musi zdawać sobie sprawę z przeznaczenia niszczonych nośników lub urządzeń (lub przynajmniej podejrzewać, do czego służą)[112].

1.10. Art. 269a k.k. – zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej

Przepis art. 269a k.k. przewiduje odpowiedzialność karną osoby, która bez uprawnienia w stopniu istotnym zakłóca pracę systemu lub sieci teleinformatycznej poprzez działania o charakterze logicznym takie jak transmisja, zniszczenie, uszkodzenie

[108] W. Wróbel w: *Kodeks karny*…, s. 1307.
[109] Por. P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 627.
[110] Por. W. Wróbel w: *Kodeks karny*…, s. 1306. Inaczej A. Adamski, który uważa, że skutek w postaci utrudnienia lub uniemożliwienia dostępu do informacji uprawnionemu nie należy do znamion przestępstwa sabotażu informatycznego (w przeciwieństwie do czynu zabronionego z art. 268 § 2 k.k.); zob. A. Adamski, *Prawo karne*…, s. 77.
[111] A. Marek uważa, że czynności sprawcze muszą być objęte zamiarem bezpośrednim, natomiast szczególne znaczenie może być objęte również zamiarem ewentualnym; zob. A. Marek, *Kodeks karny*…, s. 575.
[112] A. Adamski, *Prawo karne*…, s. 80.

lub zmiana danych informatycznych. Przewidywaną sankcją jest kara pozbawienia wolności na czas od trzech miesięcy do pięciu lat.

Przedmiotem ochrony jest bezpieczeństwo pracy systemu komputerowego, a co za tym idzie – dostępność i integralność przetwarzanych w nim danych informatycznych.

Użyte przez ustawodawcę pojęcia „zniszczenie", „usunięcie", „uszkodzenie", „zmiana", „zakłócenie w stopniu istotnym", „system komputerowy"[113] i „sieć teleinformatyczna" zostały omówione we wcześniejszej części opracowania.

Co się natomiast tyczy pojęcia transmisji, nie jest ono zdefiniowane. Według O. Górniok jest ono bliskie lub jednoznaczne z wyrażeniem „przekazywanie", użytym w art. 268a i art. 269 k.k.[114] Uznać jednak należy, że jego zakres jest węższy i odnosi się do przekazywania na odległość danych informatycznych w postaci zakodowanej (a nie za pośrednictwem nośników fizycznych takich jak płyty CD, pendrive'y). W. Wróbel w zakres tego pojęcia włącza jeszcze wprowadzenie danych informatycznych do systemu[115].

Wymienione w treści przepisu sposoby działania sprawcy tworzą katalog zamknięty[116].

Zamach na pracę systemu komputerowego 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.

A. Adamski[117] i W. Wróbel[118] 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 komputerowego lub sieci teleinformatycznej" są w istocie tożsame. Praca systemu komputerowego oraz sieci teleinformatycznej polega właśnie na przetwarzaniu, gromadzeniu i przekazywaniu danych. A. Adamski proponuje, by przepis art. 268a k.k. traktować jako narzędzie inkryminizowania działań sprawców, które nie wypełniły znamion strony przedmiotowej art. 269a k.k.[119] W. Wróbel natomiast postuluje stosować przepis art. 269a k.k. wówczas, gdy następuje kwalifikowane zakłócenie pracy systemu lub sieci[120].

Przestępstwo z art. 269a k.k. ma charakter materialny. Jego skutkiem jest zakłócenie w istotnym stopniu pracy systemu komputerowego lub sieci informatycznej. Zanim nie dojdzie do takiego zakłócenia, można mówić co najwyżej o usiłowaniu przestępstwa[121].

Może je popełnić każdy (przestępstwo powszechne), kto nie jest uprawniony do ingerencji w dany system komputerowy lub sieć teleinformatyczną[122].

---

[113] Należy nadmienić, że chodzi w tym wypadku o system komputerowy w znaczeniu zgodnym z konwencją o cyberprzestępczości, tj. o pojedynczy komputer (czy inne samodzielne urządzenie służące przetwarzaniu danych, np. tzw. *smartphone*), a nie o system informatyczny, o którym mowa w decyzji ramowej 2005/222.
[114] O. Górniok w: *Kodeks karny*…, s. 368.
[115] W. Wróbel w: *Kodeks karny*…, s. 1309.
[116] Tak też B. Kunicka-Michalska w: *Kodeks karny*…, s. 737.
[117] A. Adamski, *Cyberprzestępczość*…, s. 58–59.
[118] W. Wróbel w: *Kodeks karny*…, s. 1309.
[119] A. Adamski, *Cyberprzestępczość*…, s. 58.
[120] W. Wróbel w: *Kodeks karny*…, s. 1309.
[121] B. Kunicka-Michalska w: *Kodeks karny*…, s. 736.
[122] A. Marek, *Kodeks karny*…, s. 576; O. Górniok w: *Kodeks karny*…, s. 368.

Omawiane przestępstwo można popełnić jedynie umyślnie, w obu postaciach zamiaru[123].

1.11. Art. 269b k.k. – tzw. bezprawne wykorzystanie programów i danych

Przedmiotem ochrony przepisu art. 269b k.k. jest szeroko rozumiane bezpieczeństwo danych komputerowych, systemów komputerowych i sieci teleinformatycznych (czyli zarówno ich poufność, jak i integralność oraz dostępność)[124].

Artykuł 269b k.k. został wprowadzony w związku z dostosowywaniem polskiego prawa do konwencji o cyberprzestępczości. Mimo że od początku był on obiektem ostrej krytyki[125] ze względu na swoje liczne wady, dotychczas nie został skorygowany.

Przepis art. 269b k.k. penalizuje szeroko pojęte czynności przygotowawcze do przestępstw wymienionych w jego dyspozycji. Kryminalizuje on wytwarzanie, pozyskiwanie, zbywanie, udostępnianie urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstw określonych w art. 165 § 1 pkt 4 k.k. (sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach), art. 267 § 3, art. 268a § 1 albo § 2 w zw. z § 1, art. 269 § 2 albo art. 269a k.k., a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub w sieci teleinformatycznej. Jak widać, ustawodawca, nowelizując powyższy przepis, z niewiadomych przyczyn nie uwzględnił w wyliczeniu zawartym w treści art. 269b k.k. przepisów art. 267 § 1 i § 2 k.k.[126]

Przedmiotem ochrony jest bezpieczeństwo informacji przetwarzanych elektronicznie, we wszystkich aspektach, tj. poufność, integralność i dostępność danych informatycznych i systemów.

Z „wytwarzaniem" mamy do czynienia wówczas, gdy sam sprawca tworzy narzędzia hackerskie lub przystosowuje w tym celu urządzenia i programy stworzone do innych, nieprzestępnych celów. „Pozyskanie" to każde działanie, wskutek którego sprawca uzyskuje dostęp do takich narzędzi (oraz możliwość użycia), a przeniesienie własności egzemplarzy narzędzi hackerskich na inne osoby stanowić będzie „zbycie". Z kolei przez „udostępnienie" rozumieć należy umożliwienie korzystania z narzędzi osobom trzecim (zarówno konkretnym, jak i innym, bliżej nieokreślonym), bez utraty władztwa nad nimi lub dostępu do nich[127]. Przykładem takiego działania będzie umieszczenie ich w witrynie internetowej lub serwerze ftp, a nawet zamieszczenie na stronie internetowej linka, czyli odnośnika do strony, z której można je uzyskać[128].

---

[123] Tak też O. Górniok w: *Kodeks karny*…, s. 368; B. Kunicka-Michalska w: *Kodeks karny*…, s. 739; P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 628; W. Wróbel w: *Kodeks karny*…, s. 1309. Natomiast według odosobnionego poglądu A. Marka jego popełnienie jest możliwe jedynie w zamiarze bezpośrednim (choć co do skutku i znamienia istotności autor ten dopuszcza zamiar ewentualny); zob. A. Marek, *Kodeks karny*…, s. 576.

[124] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 628; J. Piórkowska-Flieger w: *Kodeks karny*…, s. 713.

[125] Zob. np. A. Adamski, *Cyberprzestępczość*…, s. 60–61; K. Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b kodeksu karnego*, „Prokurator" 2005/1, s. 74-83.

[126] Uwzględniony jest przepis art. 267 § 3 k.k., kryminalizujący podsłuch komputerowy – istnieje więc możliwość postawienia hackerowi zarzutu tworzenia czy udostępniania narzędzi hackerskich, jeżeli udowodni się, że mogą one służyć również do popełnienia przestępstwa z tego przepisu.

[127] Por. P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 629; W. Wróbel w: *Kodeks karny*…, s. 1312.

[128] A. Adamski, *Cyberprzestępczość*…, s. 61; K. Gienas, *Uwagi do przestępstwa*…, s. 82. Inaczej W. Wróbel, który uważa, że działanie polegające tylko na umieszczeniu linka może być kwalifikowane jedynie jako pomocnictwo do przestępstwa z art. 269b k.k.; zob. W. Wróbel w: *Kodeks karny*…, s. 1312.

„Hasła komputerowe i kody dostępu" to przykładowe wyliczenie danych umożliwiających uzyskanie dostępu do informacji przechowywanych w systemach informatycznych i sieciach teleinformatycznych. Z tej przyczyny pod pojęciem danych należy rozumieć również dane biometryczne. Nie zawierają się w nim natomiast numery seryjne oprogramowania komputerowego[129]. Pojęcia sieci teleinformatycznej oraz systemu komputerowego zostały wyjaśnione w części wstępnej do niniejszego opracowania.

Mimo że ustawodawca użył liczby mnogiej w stosunku do przedmiotów wykonawczych, penalizacją objęte jest np. zbycie tylko jednego programu czy udostępnienie tylko jednego hasła. Odnośnie do tej kwestii panuje zgodność w doktrynie i orzecznictwie. Natomiast jak zauważa A. Marek, dyskusyjna jest interpretacja, zgodnie z którą do wypełnienia znamion czasownikowych zbywania lub udostępniania wystarcza dokonanie tych czynności wobec jednej osoby[130]. Wydaje się, iż należy się zgodzić z P. Kozłowską-Kalisz, że gdyby wystarczające było dopuszczenie się czynności sprawczej określonej w omawianym przepisie wobec jednej tylko osoby, ustawodawca posłużyłby się liczbą pojedynczą, tak jak np. w art. 267 § 4 czy art. 265 § 1 k.k.[131] W sytuacji gdy sprawca dokonuje bowiem jednej z wymienionych w dyspozycji przepisu czynności względem konkretnej osoby, co najmniej licząc się z możliwością, że wykorzysta ona dany program czy hasło do popełnienia określonego czynu zabronionego, jego zachowanie należy kwalifikować jako pomocnictwo do przestępstwa popełnionego przez kupującego (czy też osobę, której narzędzie udostępnił).

Omawiane przestępstwo można popełnić w zasadzie zarówno przez działanie, jak i zaniechanie (za wyjątkiem wytworzenia).

Jest to przestępstwo materialne. Do jego znamion należy skutek w postaci stworzenia urządzenia lub programu (przy wytwarzaniu), objęcie władztwa nad nim (lub nad nośnikiem danych, na którym jest zapisany), uzyskanie doń dostępu (w przypadku pozyskania), przeniesienie władztwa nad nim (lub nad nośnikiem danych, na którym jest zapisany) na osoby trzecie (zbycie)[132] lub uczynienie dostępnym dla osób trzecich (w przypadku zbycia za pośrednictwem sieci lub udostępniania).

Jest to przestępstwo powszechne.

Omawiany występek popełnić można tylko umyślnie. Mimo że ustawodawca zastosował podobną konstrukcję do pomocnictwa[133], strona podmiotowa obejmuje obie postaci umyślności (zob. dalsze uwagi).

Przepis art. 269b § 1 k.k. stanowić miał panaceum na problem powszechnej dostępności w Internecie narzędzi hackerskich, umożliwiającej dokonywanie ataków i innych działań destrukcyjnych nawet osobom dysponującym zaledwie elementarną wiedzą z dziedziny informatyki. Jednak – jak już wskazano – jest wadliwie skonstruowany. Pierwsza z wad została wyżej wspomniana – jest nią brak w katalogu zawartym w jego treści wskazania hackingu. Co się tyczy innych – po pierwsze, w przepisie tym mowa jest o programach „przystosowanych" do określonych działań. Istnieje zatem problem,

[129] W. Wróbel w: *Kodeks karny*…, s. 1312.
[130] A. Marek, *Kodeks karny*…, s. 576.
[131] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 629.
[132] Por. P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 629.
[133] Por. O. Górniok w: *Kodeks karny*…, s. 369–370.

jak ocenić działanie twórcy programu spełniającego kilka funkcji (tzw. programy o podwójnej naturze)[134], użytego następnie przez osobę trzecią w celach przestępczych, których autor by sobie nie życzył[135]. 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.[136], wymagając tym samym od sprawcy wytwarzającego lub pozyskującego wymienione w przepisie narzędzia zamiaru bezpośredniego[137]. Większość przedstawicieli doktryny uważa jednak (za wyjątkiem właśnie W. Wróbla, o czym była mowa wyżej, oraz B. Kunickiej-Michalskiej[138], A. Marka[139] oraz J. Piórkowskiej-Flieger[140]), że dla przypisania sprawcy winy wystarczy – jak sygnalizowano – by działał on w zamiarze ewentualnym[141]. Przyjęcie takiego rozwiązania stwarza możliwość ścigania zarówno osób, które wytwarzają i udostępniają w Internecie programy służące do działań destrukcyjnych (ich autorów, webmasterów umieszczających na swoich witrynach internetowych owe narzędzia lub linki do stron, na których są takowe dostępne), jak i administratorów oraz osób zajmujących się bezpieczeństwem systemów informatycznych, które wymieniają się w sieci wiedzą na ten temat czy używają tego typu programów do testowania zabezpieczeń systemów[142]. B. Kunicka-Michalska stoi na stanowisku, że wobec takich osób, jako działających w ramach praw i obowiązków, ma miejsce wyłączenie odpowiedzialności karnej[143], a W. Wróbel podkreśla, że brak w treści przepisu art. 269b § 1 k.k. klauzuli wskazującej, że sprawca podlega karze tylko wówczas, gdy podejmuje wymienione w nim działania bez uprawnienia, należy uznać za przeoczenie ustawodawcy[144]. Zwłaszcza że wprowadzanie takowej przewiduje art. 6 konwencji o cyberprzestępczości, którego postanowienia ma realizować omawiany przepis. Należy przy okazji zaznaczyć, że w artykule tym przewiduje się, by sprawca „miał zamiar popełnienia przestępstw", a więc by działał w zamiarze bezpośrednim.

Według W. Wróbla w zakresie, w jakim art. 296b § 1 k.k. przewiduje w istocie karalność za czynności przygotowawcze do popełnienia przestępstw z art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w zw. z § 1, art. 269 § 2 albo art. 269a k.k., możliwe jest na zasadzie dopuszczalnej analogii na korzyść sprawcy stosowanie art. 17 k.k., przewidującego instytucje czynnego żalu wyłączającego karalność[145].

---

[134] Np. monitory sieciowe, inaczej nazywane analizatorami protokołów, umożliwiające administratorom analizę ruchu w sieci, mogą zostać wykorzystane przez hackerów jako sniffery.
[135] Por. A. Adamski, *Cyberprzestępczość…*, s. 60.
[136] W. Wróbel w: *Kodeks karny…*, s. 1311–1312.
[137] W. Wróbel w: *Kodeks karny…*, s. 1313.
[138] B. Kunicka-Michalska uważa, że trudno wyobrazić sobie wytwarzanie, pozyskiwanie czy zbywanie bez zamiaru bezpośredniego sprawcy; zob. B. Kunicka-Michalska w: *Kodeks karny…*, s. 748.
[139] 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…*, s 576.
[140] J. Piórkowska-Flieger, która wskazuje, że pozyskiwanie i wytwarzanie możliwe jest jedynie z zamiarem bezpośrednim; zob. J. Piórkowska-Flieger w: *Kodeks karny…*, s. 713.
[141] Zob. np. A. Adamski, *Cyberprzestępczość…*, s. 61; K. Gienas, *Uwagi do przestępstwa…*, s. 81–82; O. Górniok w: *Kodeks karny…*, s. 369–370; M. Kalitowski w: *Kodeks karny…*, s. 1214; P. Kozłowska-Kalisz w: *Kodeks karny…*, s. 629.
[142] Art. 6 konwencji o cyberprzestępczości przewiduje wyłączenie w takim wypadku karalności. Podobną klauzulę należałoby wprowadzić w tym przepisie.
[143] B. Kunicka-Michalska w: *Kodeks karny…*, s. 749.
[144] W. Wróbel w: *Kodeks karny…*, s. 1313.
[145] W. Wróbel w: *Kodeks karny…*, s. 1313–1314.

1.12. Zbiegi przepisów i przestępstw

Według W. Wróbla możliwy jest rzeczywisty właściwy zbieg przepisów pomiędzy art. 267 § 1 oraz art. 278 § 2 k.k. (uzyskanie cudzego programu w celu osiągnięcia korzyści majątkowej bez zgody uprawnionej osoby), gdyż pierwszy z tych przepisów nie odnosi się bezpośrednio do praw majątkowych, eksponując jednocześnie sposób uzyskania informacji, jakim jest przełamanie szczególnego jej zabezpieczenia[146]. Zbieg taki może również zachodzić między przepisami art. 267 § 1 i art. 275 § 1 k.k., gdy sprawca przełamuje specjalne zabezpieczenia w celu kradzieży dokumentu zawierającego informacje, do których uzyskania nie jest uprawniony[147]. Do rzeczywistego właściwego zbiegu przepisów ustawy pomiędzy art. 267 § 1 k.k. a przepisami z rozdziału XXXV k.k. (przestępstwa przeciwko mieniu) dochodzi wówczas, gdy przedmiot stanowiący nośnik danych posiada określoną wartość majątkową, będąc jednocześnie rzeczą ruchomą (np. komputer). Konieczne jest zatem zaistnienie dwóch przesłanek: czyn musi naruszać prawa majątkowe pokrzywdzonego oraz prawo do dysponowania informacją[148]. Powyższe uwagi można odnieść odpowiednio do przepisu art. 267 § 2 k.k. (zob. uwagi dotyczące stosunku między zakresem przedmiotowym przepisów zawarte we wcześniejszej części raportu). Według B. Kunickiej-Michalskiej możliwa jest sytuacja, że sprawca wypełni jednocześnie znamiona czynu z art. 267 k.k. opisane w różnych paragrafach tego przepisu kodeksu karnego – czyn ujęty w jednym paragrafie, najbardziej odpowiadającym zachowaniu sprawcy, pochłonie wówczas czynności poprzednie jako współukarane czynności uprzednie[149]. Należy przyjąć, że sytuacja taka może zaistnieć w przypadku zbiegu przepisów art. 267 § 1 lub art. 267 § 2 z art. 267 § 3 k.k. (przepis art. 267 § 1 lub art. 267 § 2 może na zasadzie *lex consumens* wyłączyć zastosowanie art. 267 § 3 k.k.). Natomiast między powyższymi przepisami a przepisem art. 267 § 4 k.k. zachodzi zbieg kumulatywny. Możliwy jest rzeczywisty właściwy zbieg przepisu art. 267 § 4 k.k. z przepisami kryminalizującymi ujawnienie informacji, które stanowią tajemnicę: państwową (art. 265 § 1 i 2 k.k.), prywatną (art. 266 § 1 k.k.), służbową (266 § 2 k.k.), przedsiębiorstwa (art. 23 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji[150]), skarbową (art. 293 ordynacji podatkowej[151]), bankową (art. 171 ust. 5 prawa bankowego[152])[153].

Jak wskazują wyniki badań, bardzo częstym zjawiskiem jest przejmowanie kont na serwisach aukcyjnych w celu ich użycia do popełniania oszustw polegających na oferowaniu towarów na licytacji i w ten sposób wyłudzaniu pieniędzy tytułem zapłaty za wylicytowany od sprawcy nieistniejący produkt. Wydaje się

[146] W. Wróbel w: *Kodeks karny*…, s. 1290. Podobnie P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 622–623.
[147] W. Wróbel w: *Kodeks karny*…, s. 1290.
[148] W. Wróbel w: *Kodeks karny*…, s. 1290.
[149] B. Kunicka-Michalska w: *Kodeks karny*…, s. 705.
[150] Ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jedn.: Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.), dalej jako u.z.n.k.
[151] Ustawa z 29.08.1997 r. – Ordynacja podatkowa (tekst jedn.: Dz. U. z 2012 r. poz. 749 ze zm.).
[152] Ustawa z 29.08.1997 r. – Prawo bankowe (tekst jedn.: Dz. U. z 2012 r. poz. 1376 ze zm.).
[153] Por. A. Adamski, *Prawo karne*…, s. 52–53. Podobnie P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 622–623. Odmienne stanowisko zajmuje B. Kunicka-Michalska, która uważa, że w przypadku zbiegu przepisu art. 267 § 4 k.k. z przepisami art. 266 k.k. lub art. 265 k.k. przepis art. 265 k.k.(lub art. 266 k.k.) pochłonie art. 267 § 4; zob. B. Kunicka-Michalska w: *Kodeks karny*…, s. 705.

– jak wskazywano w pierwszej części raportu – iż czyny takie należy kwalifikować z art. 267 § 2 k.k., czyli jako nieuprawnione uzyskanie dostępu do konta (pod warunkiem oczywiście, że pokrzywdzony użytkownik konta złoży wniosek o ściganie) w kumulatywnym zbiegu z czynem z art. 286 § 1 k.k. (oszustwo). Innym bardzo często popełnianym przestępstwem jest przejmowanie kont na portalach społecznościowych (przede wszystkim na *Naszej klasie*). Sprawcy tych czynów zwykle działają „dla żartu". Zdarza się też, że motywem jest zemsta. Uzyskując dostęp do takiego konta, swoim działaniem wypełniają znamiona przestępstwa z art. 267 § 2 k.k. (w przypadku jednak, gdy działają przede wszystkim w celu uzyskania dostępu do informacji – zgodnie z tym, co wcześniej stwierdzono – w grę wchodzi raczej zastosowanie art. 267 § 1 k.k.). Następnie ich zachowanie może polegać na realizacji znamion całego szeregu pozostających ze sobą w zbiegu kumulatywnym występków: z art. 190 § 1 k.k. lub art. 216 § 2 k.k. (np. poprzez wysyłanie z konta wiadomości zawierających groźby, wyzwiska czy obelgi), art. 212 § 2 k.k. (np. umieszczanie komentarzy zniesławiających użytkownika) czy art. 202 § 1 lub § 2 k.k. (np. poprzez umieszczenie zdjęć pornograficznych w galeriach użytkownika). W przypadku przejmowania kont e-mailowych, gdy sprawcy zależy na uzyskaniu dostępu do informacji, zastosowanie znajdzie art. 267 § 1 k.k.

Przepis art. 268 § 3 k.k. wyłącza na zasadzie specjalności art. 268 § 2 k.k.[154] W przypadku czynu penalizowanego przez przepis art. 268 § 2 k.k. może mieć miejsce analogiczna sytuacja jak omawiana przy okazji art. 267 § 2 k.k. – rzeczywisty zbieg tego przepisu z niektórymi przepisami z rozdziału XXXV k.k. Sprawca może bowiem utrudnić uprawnionej osobie dostęp do informacji, np. poprzez zabór komputera lub informatycznego nośnika danych, co może nastąpić na drodze czynów kryminalizowanych w przepisach art. 278 k.k. (kradzież), art. 284 k.k. (przywłaszczenie) czy art. 288 k.k. (zniszczenie rzeczy będącej nośnikiem danych)[155]. Oczywiście możliwe jest to tylko w przypadku, jeśli sprawca działał z zamiarem uniemożliwienia bądź znacznego utrudnienia osobie uprawnionej zapoznania się z informacją lub godził się na nie, licząc się z możliwością wystąpienia takich następstw swoich działań (sam nośnik musi mieć przy tym wartość majątkową)[156]. P. Kozłowska-Kalisz uważa, iż możliwy jest kumulatywny zbieg pomiędzy przepisami art. 268 § 2 k.k. i art. 276 k.k.[157] Zdaniem W. Wróbla jest on wykluczony – w przypadku umyślnego zniszczenia, uszkodzenia lub usunięcia zapisu na informatycznym nośniku danych czyn sprawcy należy kwalifikować, zgodnie z zasadą specjalności, na podstawie art. 268 § 2 k.k.[158] Natomiast według R.A. Stefańskiego przepis art. 268 § 2 k.k. jako *lex specialis* wyłącza art. 276 k.k.[159]

W. Wróbel podkreśla, że ze względów kryminalno-politycznych wykluczony jest zbieg pomiędzy art. 268 § 3 k.k. oraz art. 287 § 1 k.k. Jeżeli sprawca, działając w celu wyrządzenia szkody majątkowej znacznej wartości, zmienia lub usuwa określony zapis na komputerowym nośniku informacji, powinien odpowiadać

[154] P. Kozłowska-Kalisz w: *Kodeks karny.*., s. 625; B. Kunicka-Michalska w: *Kodeks karny*…, s. 718.
[155] Por. P. Kozłowska-Kalisz w: *Kodeks karny*… s. 623; J. Piórkowska-Flieger w: *Kodeks karny*…, s. 708.
[156] Por. A. Adamski, *Prawo karne*…, s. 74; W. Wróbel w: *Kodeks karny*…, s. 1297.
[157] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 625.
[158] W. Wróbel w: *Kodeks karny*…, s. 1298.
[159] R.A. Stefański, *Przestępstwo niszczenia dokumentów (art. 276 K.K.)*, „Prokuratura i Prawo" 2002/7–8, s. 79; tak też B. Kunicka-Michalska w: *Kodeks karny*…, s. 718.

z przepisu art. 294 k.k. Natomiast kumulatywna kwalifikacja między przepisami art. 268 § 3 k.k. oraz art. 287 § 1 k.k. zachodzi wówczas, gdy sprawca dokonujący zmiany lub usunięcia zapisu na komputerowym nośniku informacji działał w celu wyrządzenia szkody majątkowej, a skutek w postaci wyrządzenia znacznej szkody obejmował zamiarem ewentualnym[160].

Możliwy jest rzeczywisty niewłaściwy zbieg przepisów art. 268a i 268 k.k. W takiej sytuacji przepis art. 268 § 2 k.k. jest wyłączany na zasadzie konsumpcji[161].

Przepis art. 269 wyłączy na zasadzie specjalności przepisy art. 268, 268a[162] i 269a k.k. Stanowi również *lex specialis* w stosunku do art. 276 k.k. (niszczenie dokumentów)[163]. Możliwy jest kumulatywny zbieg przepisów art. 269 i 165 k.k. oraz art. 269 i 174 k.k. (lub 173 k.k.)[164].

P. Ochman trafnie wskazuje, iż na etapie przesyłania dokumentu elektronicznego, choć istnieje techniczna możliwość sfałszowania go, ingerencja w jego treść nie może być traktowana jako fałsz materialny dokumentu (art. 270 § 1 k.k.), a jedynie jako uszkodzenie danych (art. 268a k.k.) czy ewentualnie jako sabotaż komputerowy (art. 269 k.k.)[165]. Związane jest to z faktem, iż dokument elektroniczny przesłany siecią traci przymiot dokumentu (nie jest zapisany, tylko przesyłany)[166].

Przepis art. 269a k.k. wyłącza na zasadzie konsumpcji przepisy art. 268 § 2 i art. 268a k.k.[167]

Możliwy jest rzeczywisty niewłaściwy zbieg przepisu art. 278 k.k. z przepisem art. 268 § 2, art. 268a lub art. 269a k.k. W takim wypadku pierwszy ze wskazanych przepisów stanowi *lex consumens* w stosunku do pozostałych[168].

Ze względu na to, że część czynności sprawczych z art. 269b k.k., a mianowicie zbycie i udostępnianie urządzeń lub programów komputerowych przystosowanych do popełnienia wyliczonych tam przestępstw, może wypełniać jednocześnie znamiona pomocnictwa, sprawca będzie odpowiadał z przepisu przewidującego wyższą sankcję[169]. Istnieje możliwość pozornego zbiegu przepisów art. 267 § 3 k.k. oraz art. 269b k.k. W tym wypadku zgodnie z zasadą *lex specialis derogat legi generali* sprawca będzie odpowiadał na podstawie przepisu art. 269b k.k.[170] Według W. Wróbla w sytuacji, gdy sprawca czyni użytek z wytworzonego lub pozyskanego wcześniej urządzenia lub programu komputerowego, popełniając przestępstwo zagrożone niższą karą (art. 267 § 3, art. 268a k.k.), wyczerpuje znamiona czynu

[160] W. Wróbel w: *Kodeks karny*…, s. 1298; por. A. Adamski, *Prawo karne*…, s. 116–117.
[161] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 626; B. Kunicka-Michalska w: *Kodeks karny*…, s. 725; S. Hoc w: *Kodeks karny*…, komentarz do art. 268a.
[162] Inaczej W. Wróbel, który uważa, że art. 269 k.k. stanowi *lex consumens* w stosunku do art. 268a k.k.; zob. W. Wróbel w: *Kodeks karny*…, s. 1303.
[163] B. Kunicka-Michalska w: *Kodeks karny*…, s. 733; R.A. Stefański, *Przestępstwo niszczenia*…, s. 80.
[164] Por. P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 627; B. Kunicka-Michalska w: *Kodeks karny*…, s. 732; J. Piórkowska-Flieger w: *Kodeks karny*…, s. 711; S. Hoc w: *Kodeks karny*…, komentarz do art. 269.
[165] P. Ochman, *Spór o pojęcie dokumentu w prawie karnym*, „Prokuratura i Prawo" 2009/1, s. 34–35.
[166] P. Ochman, *Spór o pojęcie*…, s. 34–35; por. F. Radoniewicz, *Problematyka ujednolicenia*…, s. 678–681, oraz wskazana tam literatura.
[167] P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 628; B. Kunicka-Michalska w: *Kodeks karny*…, s. 739; S. Hoc w: *Kodeks karny*…, komentarz do art. 269a.
[168] Natomiast zdaniem M. Dąbrowskiej-Kardas i P. Kardasa przepis art. 287 § 1 k.k. stanowi *lex specialis* w stosunku do przepisów art. 268, art. 268a § 1 oraz art. 269a k.k.; zob. M. Dąbrowska-Kardas, P. Kardas w: *Kodeks karny. Komentarz. Część szczególna*, t. 3: *Komentarz do art. 278–363 k.k.*, A. Zoll (red.), Kraków 2006, s. 352.
[169] W. Wróbel w: *Kodeks karny*…, s. 1314.
[170] W. Wróbel w: *Kodeks karny*…, s. 1314; P. Kozłowska-Kalisz w: *Kodeks karny*…, s. 629.

ciągłego, jeśli w ten sposób realizuje powzięty wcześniej zamiar. W innym wypadku – jak twierdzi ten Autor – sprawca popełnia dwa odrębne przestępstwa, które z uwagi na sankcje wymienione w art. 269b k.k. nie mają charakteru przestępstw współukaranych[171].

Z uwagi na postępujący proces informatyzacji zachodzący we wszystkich dziedzinach ludzkiej działalności coraz większa liczba przestępstw może pozostawać w zbiegu kumulatywnym z występkami z art. 267–269b k.k. Z uwagi na ograniczenia ramowe niniejszego opracowania problem ten zostanie jedynie zasygnalizowany. Poza wskazanymi już przestępstwami przeciwko mieniu oraz związanymi z naruszeniem tajemnicy (jako najczęstszymi przypadkami) będą to głównie przestępstwa gospodarcze (choć nie tylko), przewidziane zarówno w przepisach kodeksu karnego, jak i ustaw szczególnych. W ramach pierwszej grupy można – przykładowo – wskazać nadużycie funkcji przez funkcjonariusza publicznego (art. 231 k.k.), nadużycie zaufania przez osobę uprawnioną do zajmowania się sprawami majątkowymi lub działalnością gospodarczą osoby fizycznej, prawnej albo jednostki organizacyjnej niemającej osobowości prawnej (art. 296 k.k.), wyrządzenie szkody poprzez nieprowadzenie lub prowadzenie w sposób nierzetelny dokumentacji działalności gospodarczej (art. 303 k.k.), utrudnianie przetargu publicznego (art. 305 k.k.). Z grupy drugiej (również przykładowo) można wskazać art. 77 ustawy o rachunkowości[172] czy przepis art. 54 ustawy o statystyce publicznej[173].

1.13. Problematyka wymiaru kary

Przestępstwa będące przedmiotem badań generalnie zagrożone są stosunkowo niskimi sankcjami. Kradzież informacji (art. 267 § 1 k.k.), hacking (art. 267 § 2k.k.), zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym lub innym urządzeniem lub oprogramowaniem (art. 267 § 3 k.k.), a także ujawnianie bezprawnie uzyskanych tą drogą informacji (art. 267 § 4 k.k.), podlegają grzywnie, karze ograniczenia albo pozbawienia wolności do lat dwóch. Niewiele wyższa kara (pozbawienia wolności od miesiąca do lat trzech) przewidziana jest za typy podstawowe przestępstw udaremnienia lub uniemożliwienia zapoznania się z informacją zapisaną na informatycznym nośniku danych (art. 268 § 2 k.k.), zamachu na dane i systemy komputerowe (art. 268a k.k.) oraz „niewłaściwego użycia urządzeń" (art. 269b k.k.). W związku z tym, że w przypadku wyżej wymienionych występków zagrożenie karą pozbawienia wolności jest niższe niż trzy lata, możliwe jest stosowanie warunkowego umorzenia postępowania na podstawie art. 66 § 2 k.k. Ponadto, jeśli społeczna szkodliwość czynu nie jest znaczna, sąd może odstąpić od wymierzenia kary i poprzestać na orzeczeniu środka karnego, jeżeli cele kary zostaną przez ten środek spełnione (art. 59 k.k.). Z kolei typy kwalifikowane przestępstw z art. 268 § 1 i 2 oraz art. 268a § 1 k.k. (czyli art. 268 § 3 oraz art. 268a § 2 k.k.), jak również zakłócenie pracy systemu informatycznego przewidziane w przepisie art. 269a k.k. zagrożone są karą pozbawienia wolności od trzech miesięcy do lat

[171] W. Wróbel w: *Kodeks karny*..., s. 1314.
[172] Ustawa z 29.09.1994 r. o rachunkowości (tekst jedn.: Dz. U. z 2013 r. poz. 330 ze zm.), dalej jako u.r.
[173] Ustawa z 29.06.1995 r. o statystyce publicznej (tekst jedn.: Dz. U. z 2012 r. poz. 591 ze zm.).

pięciu, co umożliwia zastosowanie warunkowego umorzenia postępowania jedynie na zasadzie art. 66 § 3 k.k., czyli w przypadku zaistnienia dodatkowej przesłanki w postaci pojednania się pokrzywdzonego ze sprawcą, naprawienia przez niego szkody lub przynajmniej uzgodnienia sposobu jej naprawienia. Ponadto w przypadku wszystkich wskazanych wyżej występków dopuszczalne jest orzeczenie przez sąd – zamiast kary pozbawienia wolności – grzywny albo kary ograniczenia wolności do lat dwóch, w szczególności jeżeli orzekany jest równocześnie środek karny (art. 58 § 3 k.k.). Podobnie też może mieć zastosowanie instytucja prawa procesowego przewidziana w art. 11 kodeksu postępowania karnego[174] (tzw. umorzenie absorpcyjne), umożliwiająca umorzenie postępowania w sprawie o występek zagrożony karą pozbawienia wolności do lat pięciu, jeżeli orzeczenie wobec oskarżonego (podejrzanego) kary byłoby oczywiście niecelowe ze względu na rodzaj i wysokość kary prawomocnie orzeczonej za inne przestępstwo, a interes pokrzywdzonego temu się nie sprzeciwia.

Za przestępstwo sabotażu informatycznego (art. 269 k.k.), we wszystkich jego postaciach, przewidziana jest wyłącznie kara pozbawienia wolności od sześciu miesięcy do ośmiu lat. Tak wysoka sankcja (na tle innych omawianych przestępstw komputerowych) wynika ze znacznej szkodliwości społecznej tego czynu. Wyklucza ona warunkowe umorzenie postępowania oraz zastosowanie instytucji przewidzianych w art. 58 § 3, art. 59 k.k. oraz art. 11 k.p.k.

W przypadku wszystkich przestępstw będących przedmiotem badań, z uwagi na niewysokie zagrożenie karą, możliwe jest skorzystanie z trybu przewidzianego w art. 335 k.p.k., czyli umieszczenie przez prokuratora w akcie oskarżenia wniosku o wydanie wyroku skazującego i orzeczenie uzgodnionych z oskarżonym kary lub środka karnego, oczywiście o ile spełnione są pozostałe w tym przepisie warunki, tj. jeżeli okoliczności popełnienia przestępstwa nie budzą wątpliwości, a postawa oskarżonego wskazuje, że cele postępowania zostaną osiągnięte.

W przypadku skazania za omawiane przestępstwa środki karne stosowane być mogą na zasadach ogólnych. Jeżeli sąd skazuje sprawcę za występek polegający na uzyskaniu informacji (art. 267 § 1, § 2 lub § 3 k.k.), na podstawie art. 44 § 1 k.k. orzeka przypadek przedmiotów pochodzących bezpośrednio z przestępstwa, np. płyty CD ze skopiowanym zapisem informacji[175]. Nie jest to jednak zbyt dotkliwe. W. Wróbel wskazuje, że w sytuacji skazania za przestępstwo z art. 267 § 3 k.k. należy w każdym przypadku rozważyć potrzebę zastosowania instytucji wskazanej w art. 44 § 2 k.k. – przepadku urządzeń podsłuchowych, wizualnych lub innych urządzeń lub oprogramowania jako narzędzi służących lub przeznaczonych do popełnienia przestępstwa. Orzeczenie tego środka wskazane jest również w przypadku pozostałych przestępstw będących przedmiotem badań – sprawca do ich popełnienia musiał przecież korzystać z narzędzia, tj. komputera, który często stanowił jego własność.

Natomiast jeżeli sprawca swoim czynem spowodował szkodę majątkową, zastosowanie będzie miał przepis art. 46 k.k., nakładający na sąd obowiązek orzeczenia na wniosek pokrzywdzonego stosownego odszkodowania (w całości lub części).

[174] Ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 ze zm.), dalej jako k.p.k.
[175] S. Hoc w: *Kodeks karny*..., komentarz do art. 267.

Ponadto sąd powinien rozważyć zastosowanie go z urzędu (tj. bez stosownego wniosku złożonego przez pokrzywdzonego lub inną uprawnioną osobę), w szczególności w przypadkach skazania za przestępstwa z przepisu art. 268 § 3 oraz art. 268a § 2 k.k., gdyż ich dalszym przedmiotem ochrony są interesy majątkowe osoby pokrzywdzonego (w obu wypadkach znamieniem kwalifikującym jest spowodowanie znacznej szkody majątkowej).

W przypadku wszystkich omawianych przestępstw celowe wydaje się rozważenie możliwości – gdy tylko zaistnieją ku temu okoliczności – zastosowania środków przewidzianych przez przepis art. 41 k.k. (zakaz zajmowania określonego stanowiska albo wykonywania określonego zawodu), art. 45 k.k. (przepadek korzyści majątkowej osiągniętej z przestępstwa albo jej równowartości) i art. 52 k.k. (zwrot korzyści majątkowej osiągniętej przez osobę fizyczną, prawną lub jednostkę organizacyjną niemającą osobowości prawnej w wyniku popełnienia przestępstwa przez sprawcę działającego w jej imieniu lub interesie).

W art. 269b § 2 k.k. przewidziane jest ponadto obligatoryjne orzeczenie przepadku przedmiotów wymienionych w art. 269b § 1 k.k., tj. urządzeń lub programów komputerowych przystosowanych do popełnienia określonych w treści tego przepisu przestępstw. W przypadku gdy są one własnością sprawcy, orzeczenie ich przepadku ma charakter obligatoryjny, w innym wypadku – fakultatywny.

1.14. Tryb ścigania

Wszystkie omawiane przestępstwa ścigane są z oskarżenia publicznego. Część z nich ma charakter przestępstw bezwzględnie wnioskowych (dotyczy to występków z art. 267, 268, 268a k.k.). Ze względu na wysoką szkodliwość społeczną czyny penalizowane w art. 269 k.k. (sabotaż informatyczny), art. 269a k.k. (zakłócanie pracy sieci komputerowej) oraz art. 269b k.k. (tzw. bezprawne wykorzystanie programów lub danych) są ścigane z urzędu. W przypadku przestępstwa sabotażu informatycznego jest to dodatkowo uzasadnione charakterem chronionych przez ten przepis danych informatycznych.

CZĘŚĆ 2. WYNIKI BADAŃ EMPIRYCZNYCH

2.1. Uwagi wprowadzające

Badaniami objęte zostały akta prokuratorskie spraw dotyczących przestępstw z art. 267 § 2, art. 268a, art. 269, art. 269a oraz art. 269b k.k.[176], które zostały

[176] Poza zakresem badań pozostawiono sprawy o przestępstwa z art. 267 § 1 k.k. Wynikało to z dwóch zasadniczych przyczyn. Otóż – jak wspomniano – po nowelizacji kodeksu karnego przeprowadzonej w 2008 r. głównym narzędziem do walki z hackingiem (w rozumieniu wąskim) stał się nowy przepis art. 267 § 2 k.k. Jednocześnie fakt, iż przepis art. 267 § 1 k.k. kryminalizuje szeroko rozumiane naruszenie tajemnicy korespondencji, wskazywał na duże prawdopodobieństwo, iż sprawy dotyczące hackingu stanowiłyby niewielką ich część. Założenie to potwierdziły częściowo badania prowadzone równolegle na terenie apelacji lubelskiej dotyczące przestępstw kwalifikowanych z przepisu art. 267 § 1 k.k. Na 124 sprawy, które wpłynęły w 2010 r., 50 dotyczyło hackingu (40%). Oznacza to, że objęcie niniejszymi badaniami również spraw o przestępstwa z tego przepisu mogłoby wiązać się z koniecznością sprowadzenia dodatkowo do Instytutu akt ponad dwóch tysięcy spraw (należy pamiętać, że badaniami objęte były sprawy z dwóch lat), z czego ponad połowa nie mieściłaby się w zakresie przedmiotowym badań (oczywiście przy założeniu, że badania na terenie apelacji lubelskiej były miarodajne dla całego kraju).

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 kodeksu karnego z 2008 r. (która weszła w życie 23.12.2008 r.). Do Instytutu Wymiaru Sprawiedliwości wpłynęło w sumie 1418 spraw (akta prokuratorskie główne, podręczne lub zarówno podręczne, jak i główne, albo kserokopie akt lub samych postanowień, aktów oskarżenia lub wyroków). Po wstępnej selekcji, polegającej na odrzuceniu spraw błędnie zakwalifikowanych (np. spraw dotyczących podsłuchu zakwalifikowanych z art. 267 § 2 k.k., zamiast – jak powinno mieć miejsce po nowelizacji z 2008 r. – art. 267 § 3 k.k.) lub dotyczących przestępstw niemieszczących się w zakresie badań (np. *skimming*[177]), analizie poddano akta 1163 spraw (498 spraw z 2009 r. oraz 665 spraw z 2010 r.).

Ustalono, iż w latach 2009–2010 w poszczególnych apelacjach zarejestrowano następującą liczbę spraw dotyczących badanych przestępstw:

- apelacja gdańska – 143 sprawy;
- apelacja warszawska – 183 sprawy;
- apelacja krakowska – 123 sprawy;
- apelacja łódzka – 75 spraw;
- apelacja białostocka – 61 spraw;
- apelacja lubelska – 103 sprawy;
- apelacja poznańska – 134 sprawy;
- apelacja szczecińska – 57 spraw;
- apelacja wrocławska – 98 spraw;
- apelacja katowicka – 123 sprawy;
- apelacja rzeszowska – 63 sprawy.

Z powyższego zestawienia wynika, że ilość spraw zależała w zasadzie od wielkości apelacji oraz znajdujących się na ich terenie miast. Najwięcej spraw było w apelacjach warszawskiej (15,73%), gdańskiej (12,29%), poznańskiej (11,52%), krakowskiej (10,58%), katowickiej (10,58%), a najmniej – w rzeszowskiej (5,41%) i białostockiej (5,24%).

2.2. Sposób załatwienia sprawy

W skali całego kraju umorzeniem zakończyło się 750 spraw (64,49% ogólnej liczby spraw; w 2009 r. – 331, w 2010 r. – 419). Odmówiono wszczęcia postępowania w 213 przypadkach (18,31% ogólnej liczby spraw; w 2009 r. – 88, w 2010 r. – 125). W 102 sprawach (8,77% ogólnej liczby) do sądu skierowano akty oskarżenia (w 2009 r. – 41 spraw, w 2010 r. – 61). W 25 wypadkach (2,15% liczby spraw) prokurator sporządził wnioski o warunkowe umorzenie postępowania (w 2009 r. – 12, w 2010 r. – 13). W inny sposób załatwiono 68 (5,85%) spraw (w 2009 r. – 24, w 2010 r. – 44). Co do sposobu zakończenia dwóch postępowań przygotowawczych brak jest danych (oba z 2009 r.), natomiast trzy się toczą (wszystkie z 2010 r.).

[177] *Skimming* – kopiowanie zawartości paska magnetycznego (obecnie również danych z chipa) karty bankomatowej w celu jej podrobienia.

2.2.1. Odmowy wszczęcia postępowania

Tabela 1.			
Podstawa odmowy wszczęcia postępowania	**2009**	**2010**	**Suma**
art. 17 § 1 pkt 1 k.p.k. – czynu nie popełniono	1	7	8
art. 17 § 1 pkt 1 k.p.k. – brak danych dostatecznie uzasadniających podejrzenie popełnienia czynu	28	32	60
art. 17 § 1 pkt 2 k.p.k. – czyn nie zawiera znamion czynu zabronionego	30	41	71
art. 17 § 1 pkt 3 k.p.k. – znikoma społeczna szkodliwość czynu	4	1	5
art. 17 § 1 pkt 8 k.p.k. – sprawca nie podlega orzecznictwu polskich sądów karnych	0	1	1
art. 17 § 1 pkt 10 k.p.k. – brak wniosku o ściganie	40	58	98
Suma	103	140	243

Z tabeli 1 wynika, iż najczęściej pojawiającą się podstawą odmowy wszczęcia postępowania był brak wniosku o ściganie (art. 17 § 1 pkt 10 k.p.k.; 98 spraw, tj. 40,33%). Wśród przyczyn takich decyzji pokrzywdzonych należy wskazać – po pierwsze – fakt, iż wielu spośród nich było zainteresowanych jedynie złożeniem zawiadomienia o przestępstwie i otrzymaniem stosownego zaświadczenia potwierdzającego dokonanie tej czynności. Miało to miejsce np. w przypadku przejęć kont w internetowych serwisach aukcyjnych (przede wszystkim na *Allegro*). Dzięki takiemu zaświadczeniu pokrzywdzeni odzyskują konta, a serwis zwraca prowizje pobrane od transakcji zawartych za pomocą przejętego konta oraz – w przypadku pokrzywdzonych będących kupującymi, którzy nie otrzymali zamówionego towaru (lub otrzymali, ale znacznie różniący się od opisanego w ofercie) – wyrównuje straty do pewnej wysokości (10.000 zł w przypadku *Allegro*). Drugim często spotykanym powodem cofnięcia (lub niezłożenia) wniosku o ściganie było ustalenie już w toku pierwszych czynności, iż sprawcą jest osoba znana pokrzywdzonemu, która swoim zachowaniem, mającym na celu np. spłatanie żartu (często „niesmacznego"), nieświadomie dopuściła się przestępstwa (np. przejęła konto na portalu *Nasza klasa* i umieściła złośliwe komentarze). Za przykład odmowy wszczęcia postępowania z powodu braku znamion czynu zabronionego (art. 17 § 1 pkt 2 k.p.k.), która to przesłanka pojawiła się 71 razy (29,22%), może posłużyć podszywanie się pod pokrzywdzonego przez stworzenie przez sprawcę fałszywego profilu na portalu społecznościowym[178] albo randkowym[179].

2.2.2. Umorzenia postępowania

Jak wynika z zestawienia zawartego w tabeli 2, zdecydowanie najczęstszą przyczyną umorzenia postępowania przygotowawczego było niewykrycie sprawcy

[178] Zob. w ostatniej części raportu sprawa nadzorowana przez Prokuraturę Rejonową w Pruszkowie (4Ds1632/10).

[179] Obecnie zachowania polegające ma podszywaniu się pod inną osobę, wykorzystywaniu jej wizerunku lub innych jej danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej mogą być kwalifikowane jako tzw. *stalking* (art. 191a § 2 k.k.).

Tabela 2.			
Podstawa umorzenia postępowania	**2009**	**2010**	**Suma**
art. 17 § 1 pkt 1 k.p.k. – czynu nie popełniono	2	9	11
art. 17 § 1 pkt 1 k.p.k. – brak danych dostatecznie uzasadniających podejrzenie popełnienia czynu	52	71	123
art. 17 § 1 pkt 1 k.p.k. – brak danych, że podejrzany popełnił zarzucany mu czyn	0	1	1
art. 17 § 1 pkt 2 k.p.k. – czyn nie zawiera znamion czynu zabronionego	74	65	139
art. 17 § 1 pkt 2 k.p.k. – zachowanie podejrzanego nie wypełniło znamion czynu zabronionego	0	10	10
art. 17 § 1 pkt 2 k.p.k. – ustawa stanowi, że sprawca nie podlega karze	0	1	1
art. 17 § 1 pkt 3 k.p.k. – znikoma społeczna szkodliwość czynu	10	12	22
art. 17 § 1 pkt 7 k.p.k. – postępowanie karne co do tego samego czynu tej samej osoby zostało prawomocnie zakończone albo wcześniej wszczęte toczy się	1	1	2
art. 17 § 1 pkt 10 k.p.k. – brak wniosku o ściganie	48	52	100
art. 322 § 1 k.p.k. – nie wykryto sprawcy	183	261	444
art. 322 § 1 k.p.k. – brak danych uzasadniających, że podejrzany popełnił zarzucany mu czyn zabroniony	6	5	11
Suma	375	489	864

(51,39% przypadków). Paradoksalnie w wielu wypadkach nie wynikało to z jego sprytu czy przebiegłości. Oczywiście zdarzały się skomplikowane ataki typu dDoS, do których realizacji używano setek przejętych komputerów[180], co praktycznie uniemożliwiało odnalezienie źródła takiego ataku, czy sytuacje, gdy sprawca oszustw popełnianych za pomocą kont przejętych na portalu aukcyjnym świadomie uniemożliwiał zidentyfikowanie swojej osoby (np. korzystając z telefonu z kartą typu *prepaid* oraz karty kredytowej tego typu)[181]. W większości spraw niewykrycie sprawcy wynikało jednak z bardzo prozaicznych przyczyn – korzystanie przez niego z komputera w bibliotece czy szkole, łączenie się przez grupę użytkowników z Internetem za pośrednictwem jednego routera, korzystanie przez sprawcę z sieci poprzez podłączenie się do niezabezpieczonej sieci radiowej czy wreszcie po prostu użytkowanie tego samego komputera przez większą grupę osób (np. członkowie rodziny, koledzy i koleżanki ze szkoły). Duże problemy pojawiały się, gdy konto poczty elektronicznej, do którego uzyskano nieuprawniony dostęp, było założone w zagranicznym serwisie internetowym (takim jak np. niezwykle popularny *Gmail*). Polski przedstawiciel właściciela takiego serwisu (w przypadku *Gmaila* jest to Google.Inc – przedsiębiorstwo z siedzibą w Stanach Zjednoczonych) nie mógł bowiem udostępnić danych logowań do takiej skrzynki pocztowej i kierował w tej sprawie do głównej siedziby firmy.

[180] Zob. omówioną w ostatniej części raportu sprawę nadzorowaną przez Prokuraturę Rejonową Warszawa-Praga Północ (7Ds463/10/III/IV).
[181] Zob. omówienie sprawy nadzorowanej przez Prokuraturę Rejonową w Oleśnie (1Ds1166/10).

2.2.3. „Inny sposób" załatwienia sprawy

Tabela 3.			
„Inny sposób" załatwienia sprawy	**2009**	**2010**	**Suma**
Dołączenie do innej sprawy	0	1	1
Przekazanie innej jednostce z uwagi na właściwość miejscową	11	24	35
Przekazanie innej jednostce z uwagi na dobro wymiaru sprawiedliwości	0	1	1
Przekazanie sądowi rodzinnemu	10	14	24
Zawieszenie	3	4	7
Suma	24	44	68

Z przedstawionych w tabeli 3 danych można by wyciągnąć mylne wnioski odnośnie do niewielkiej liczby nieletnich wśród sprawców – jedynie w 24 sprawach (co stanowi 2,06% badanych spraw) przekazano sprawy do sądów rodzinnych. Należy jednak pamiętać, iż – dla porównania – akty oskarżenia i wnioski o warunkowe umorzenie sporządzono w 127 sprawach. A poza sprawami, które znalazły swój finał w sądzie rodzinnym, jest wiele takich, w których z materiału dowodowego można wywnioskować, iż sprawcą była osoba nieletnia, ale nie została ona wykryta bądź cofnięto wniosek o ściganie[182].

2.3. Kwalifikacje prawne

W niniejszym podrozdziale zaprezentowane zostały kwalifikacje czynów przyjęte w postanowieniach o odmowie wszczęcia, umorzeniu, w wyrokach (lub aktach oskarżenia w przypadku braku tych ostatnich) oraz we wnioskach prokuratora o warunkowe umorzenie postępowania. Następnie przedstawione zostały wyniki ich analizy.

Ze względu na znaczną ilość przyjętych kwalifikacji oraz znaczne ich zróżnicowanie, przy jednoczesnej powtarzalności najczęściej występujących, wskazane było ograniczenie się do przedstawienia w poniższych zestawieniach właśnie tej grupy. W przypadku postanowień o odmowie wszczęcia postępowania w tabeli ujęto te kwalifikacje, które wystąpiły co najmniej pięć razy. Ze względu na znaczną liczbę spraw zakończonych umorzeniem w ich wypadku zawarto w tabeli te kwalifikacje, które odnotowano co najmniej 10 razy. Przyjęcie analogicznego rozwiązania nie było możliwe w przypadku wyroków (i aktów oskarżenia), gdyż kwalifikacje w nich przyjęte okazały się znacznie bardziej zróżnicowane. Stąd ograniczenie się jedynie do wskazania ich przykładów.

[182] W jednej z badanych spraw (Prokuratura Rejonowa w Koszalinie (DS2924/09/D)) nieznani sprawcy włamali się do szkolnych dzienników elektronicznych. Wniosek o ściganie został jednak cofnięty przez dyrektora szkoły, który uzasadnił to posunięcie decyzją rady pedagogicznej, iż najlepszym rozwiązaniem będzie wyciągnięcie konsekwencji wobec sprawców „we własnym zakresie" przez władze szkoły.

Tabela 4.			
Kwalifikacje prawne przyjęte w postanowieniu o odmowie wszczęcia postępowania	**2009**	**2010**	**Suma**
art. 267 § 1 k.k.	3	3	6
art. 267 § 2 k.k.	5	8	13
art. 268 § 1 k.k.	5	0	5
art. 268 § 1 w zw. z 268 § 2 k.k.	2	4	6
art. 268 § 2 k.k.	15	18	33
art. 268a § 1 k.k.	53	80	133
art. 269a k.k.	7	5	12
art. 269b § 1 k.k.	5	4	9
Pozostałe czyny[183]	8	18	26
Suma	103	140	243

Tabela 5.			
Kwalifikacje prawne najczęściej przyjmowane w postanowieniach o umorzeniu postępowania	**2009**	**2010**	**Suma**
art. 267 § 1 k.k.	15	8	23
art. 267 § 1 w zb. z art. 268 § 2 w zw. z art. 11 § 2 k.k.	11	10	21
art. 267 § 1 w zb. z art. 268a § 1 w zw. z art. 11 § 2 k.k.	9	8	17
art. 267 § 1 w zb. z art. 268a § 1 w zw. z art. 11 § 2 k.k.	5	6	11
art. 267 § 2 k.k.	4	18	22
art. 268 § 1 w zw. z art. 268 § 2 k.k.	8	7	15
art. 268 § 2 k.k.	41	55	96
art. 268a § 1 k.k.	165	241	406
art. 269a k.k.	15	13	28
art. 269b § 1 k.k.	11	11	22
art. 286 § 1 k.k.	9	15	24
Pozostałe[184]	82	97	179
Suma	375	489	864

[183] Kwalifikacje pominięte: art. 23 u.z.n.k., art. 190 § 1, art. 202 § 1, art. 202 § 2 w zb. z art. 268a § 1 w zw. z art. 11 § 2, art. 216 § 2, art. 231 § 1, art. 231 § 1 w zb. z art. 267 § 1 w zb. z 267 § 2 w zb. z art. 268a § 1 w zw. z art. 11 § 2, art. 266 § 1, art. 267 § 1 w zb. z art. 268 § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268 § 2 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268 § 2 w zw. z art. 11 § 2 w zw. z art. 12, art. 267 § 1 w zb. z art. 268a § 1, art. 267 § 1 w zb. z art. 268a w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 267 § 2 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 267 § 2 w zw. z art. 11 § 2 w zw. z art. 12, art. 267 § 1 w zb. z art. 267 § 3, art. 267 § 1 w zb. z art. 267 § 2 w zb. z art. 268a, art. 287 § 1 k.k.

[184] Kwalifikacje pominięte: art. 77 pkt 1 u.r., art. 23 u.z.n.k., art. 49 ust. 1 u.o.d.o. w zb. z art. 268a § 1 w zw. z art. 11 § 2, art. 13 § 1 w zw. z art. 268 § 1, art. 13 § 1 w zw. z art. 282 w zb. z art. 269a, art. 13 § 1 w zw. z art. 286 § 1, art. 13 § 1 w zw. z art. 286 § 1 w zb. z art. 267 § 2 w zw. z art. 11 § 2, art. 13 § 1 w zw. art. 286 § 1 w zw. z art. 12, art. 13 § 1 w zw. z art. 286 § 1 w zb. z art. 267 § 1 w zb. z art. 267 § 2 w zw. z art. 11 § 2 w zw. z art. 12, art. 190 § 1, art. 202 § 2, art. 202 § 4a, art. 212 § 2, art. 216 § 1, art. 216 § 2, art. 217 § 2, art. 226 § 1, art. 231 § 1, art. 231 § 1 w zb. z art. 276 w zb. z art. 278 w zb. z art. 268a § 1 w zw. z art. 11 § 2, art. 266 § 1, art. 18 § 3 w zw. z art. 267 § 1, art. 267 § 1 w zw. z art. 12, art. 267 § 1

Przed przejściem do przedstawienia wniosków, które nasuwają się po analizie powyższych kwalifikacji, konieczne jest zwrócenie uwagi na powód umieszczenia w nich przepisów dotyczących przestępstw niebędących przedmiotem badań. Wynika to stąd, że przestępstwa te albo wystąpiły w zbiegu z omawianymi w tym raporcie czynami zabronionymi, albo wręcz powinny być zakwalifikowane w zbiegu kumulatywnym z przepisów je kryminalizujących (a nie zostały, z uwagi np. na brak wniosku o ściganie).

Najczęściej przyjmowanymi kwalifikacjami prawnymi, zarówno w postanowieniach o odmowie wszczęcia, jak i o umorzeniu, były przepisy art. 268a k.k. (odpowiednio 133 czynów, tj. 54,73%, oraz 406, tj. 46,99%) i art. 268 § 2 k.k. (odpowiednio 33 czyny, tj. 13,58%, oraz 101, tj. 11,69%).

Nie przedstawiono kwalifikacji przyjętych w aktach oskarżenia i wyrokach. Jak sygnalizowano wyżej, wynika to z faktu, iż były one niezwykle zróżnicowane (w zasadzie się nie powtarzały) i niemożliwe było jakiekolwiek ich pogrupowanie i przedstawienie w uporządkowany sposób. Potwierdza się jednak w nich tendencja widoczna w przypadku postanowień o odmowie wszczęcia i o umorzeniu – przepisami, po które sięgano najczęściej, były art. 268a § 1 oraz art. 268 § 2 k.k. Jako przykładowe kwalifikacje można wskazać: art. 267 § 1 w zb. z art. 268a § 1 w zw. z art. 11 § 2 w zw. z art. 12, art. 267 § 2 w zb. z art. 267 § 1 w zb. z art. 268 § 2 w zw. z art. 11 § 2, art. 286 § 1 w zb. z art. 287 § 1 w zb. z art. 269b § 1 w zw. z art. 11 § 2 w zw. z art. 12 w zw. z art. 65 § 1, art. 269b § 1 w zb. z art. 287 § 1 w zw. z art. 11 § 2 (zastosowano art. 91 § 1 k.k.), art. 268a § 1 k.k. w zb. z art. 7 ust. 2 ustawy o dostępie warunkowym[185] (zastosowano art. 91 § 1 k.k.).

Przechodząc do analizy przedstawionych wyżej danych, w pierwszej kolejności należy zwrócić uwagę, iż czyny polegające na uzyskaniu nieuprawnionego dostępu

w zb. z art. 267 § 2 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 267 § 3, art. 267 § 1 w zb. z art. 268 § 2 w zw. z art. 11 § 2 w zw. z art. 12, art. 267 § 1 w zb. z art. 268a § 1 w zb. z art. 287 § 1 w zw. z art. 11 § 2 w zw. z art. 12, art. 267 § 1 w zb. z art. 267 § 2 w zb. z art. 286 § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268 § 2 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268a § 1, art. 267 § 1 w zb. z art. 269a, art. 267 § 1 w zb. z art. 268a § 1 w zb. z art. 269b § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268 § 2 w zb. z art. 268a § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268a § 1 w zw. z art. 284 § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 269a w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268a § 1 w zb. z art. 269b § 1 w zb. z art. 287 § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268 § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 268 § 2 w zb. z art. 13 § 1 w zw. z art. 286 § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z § 2 w zb. z § 4 w zb. z art. 268a § 1 w zw. z art. 11 § 2, art. 267 § 1 w zb. z art. 269b § 1 w zw. z art. 11 § 2, art. 267 § 2 w zw. z art. 12, art. 267 § 2 w zb. z art. 267 § 3 w zw. z art. 11 § 2 w zw. z art. 12, art. 267 § 2 w zb. z art. 279 § 1 w zw. z art. 11 § 2, art. 267 § 3, art. 268 § 1, art. 268 § 1 w zb. z art. 268 § 2 w zw. z art. 12, art. 268 § 1 w zb. z art. 268 § 2 w zb. z art. 267 § 1, art. 268 § 1 w zb. z art. 268a w zw. z art. 11 § 2, art. 268 § 2 w zw. z art. 12, art. 268 § 2 w zb. z art. 276 w zw. z art. 11 § 2, art. 268 § 2 w zb. z art. 286 § 1 w zw. z art. 11 § 2 w zw. z art. 12, art. 268 § 2 w zb. z art. 278 § 1 w zw. z art. 11 § 2 w zw. z art. 12, art. 268 § 1 i 2 w zb. z art. 267 § 1 w zw. z art. 11 § 2 w zw. z art. 12, art. 268a § 1 w zw. z art. 91, art. 268a § 1 w zw. z art. 12, art. 268a § 1 w zb. z art. 276 w zb. z art. 284 § 2 w zw. art. 11 § 2, art. 268a § 1 w zb. z art. 269b § 1 w zw. z art. 11 § 2, art. 268a § 1 w zb. z art. 284 § 2 w zw. z art. 11 § 2, art. 268a § 1 w zb. z art. 278 § 1 w zw. z art. 11 § 2, art. 268a § 1 w zb. z art. 286 § 1 w zw. z art. 11 § 2, art. 268a § 1 w zb. z art. 286 § 1 w zw. z art. 11 § 2 w zw. z art. 12, art. 268a § 1 w zb. z art. 212 § 2 w zw. z art. 11 § 2, art. 268a § 1 w zb. z art. 269a w zw. z art. 11 § 2, art. 268a § 1 w zb. z art. 257 w zw. z art. 11 § 2, art. 268a § 1 w zb. z art. 287 § 1 w zw. z art. 11 § 2, art. 268a § 2, art. 268a w zb. z art. 269b § 1, art. 269 § 1 w zw. z art. 12, art. 269a w zw. z art. 11 § 2, art. 269a w zw. z art. 12, art. 13 § 1 w zw. z art. 286 § 1 w zb. z art. 269b w zw. z art. 11 § 2, art. 269b § 1 w zw. z art. 12, art. 270 § 1, art. 275 § 1, art. 276, art. 278 § 2, art. 285 § 1 w zw. z art. 294 § 1, art. 286 w zw. z art. 12, art. 286 § 1 w zw. z art. 294 § 1 w zb. z art. 268a § 1 w zw. z art. 11 § 2, art. 286 § 1 w zb. z art. 287 § 1 w zb. z art. 269b § 1 w zw. z art. 11 § 2, art. 279 § 1 w zb. z art. 287 § 1 w zb. z art. 269b § 1 w zw. z art. 11 § 2, art. 284 § 2, art. 284 § 2 w zw. z art. 276 w zw. z art. 11 § 2, art. 287 § 1, art. 288 § 1, art. 296 § 1, art. 305 § 1 k.k.

[185] Ustawa z 5.07.2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz. U. Nr 126, poz. 1068).

do danych informatycznych (np. włamanie na konto poczty elektronicznej, profil na portalu społecznościowym) kwalifikowano zwykle na podstawie któregoś z trzech następujących przepisów: art. 267 § 2 (lub § 1), art. 268a § 1 lub art. 268 § 2 k.k. (ewentualnie jako art. 268 § 2 w zw. z art. 268 § 1 k.k.).

Pragnę zaznaczyć, że uważam, iż błędem jest stosowanie w tych wypadkach przepisu art. 268 § 2 k.k., gdyż odnosi się on – jak sygnalizowano wcześniej (zob. uwagi do przepisu art. 268 § 2 k.k. w części pierwszej raportu) – do czynów, w których przedmiotem czynności wykonawczej są dane informatyczne na informatycznym nośniku danych.

W związku z powyższym pozostaje odpowiedzieć na pytanie, czy zastosowanie w omawianym wypadku powinien znaleźć przepis art. 267 § 2 (lub § 1) k.k., czy art. 268a § 1 k.k., czy może oba. Otóż wszystko zależy od konkretnego stanu faktycznego. Jeżeli sprawca przełamał zabezpieczenia, uzyskując dostęp do informacji dla niego nieprzeznaczonej, i to było głównym elementem czynu, zgodnie z tym, co stwierdzono w części pierwszej raportu, czyn należy zakwalifikować z art. 267 § 1 k.k. Jeżeli sprawca jednocześnie utrudnił bądź uniemożliwił pokrzywdzonemu dostęp do danych informatycznych (zmienił hasło dostępu, zlikwidował konto) albo dokonał modyfikacji danych, dojdzie do zbiegu kumulatywnego z art. 268a § 1 k.k. Analogicznie sytuacja będzie się przedstawiać w przypadku, gdy sprawca uzyskał dostęp do konta w celu innym niż uzyskanie dostępu do informacji lub nie przełamał zabezpieczenia (np. znał hasło lub hasła nie było), tyle że wtedy zastosowanie znajdzie art. 267 § 2 k.k. (zob. uwagi do art. 267 § 2 k.k. w części pierwszej raportu).

Przepis art. 267 § 2 k.k. może służyć – zgodnie z tym, co wskazano w części pierwszej raportu – do kryminalizacji zachowań polegających na uzyskaniu dostępu do niezabezpieczonej bezprzewodowej sieci. Jeżeli zachowanie sprawcy będzie powodowało spadek wydajności tejże sieci na tyle, że będzie utrudniać korzystanie z niej podmiotom uprawnionym, dojdzie do zbiegu rzeczywistego właściwego z art. 268a § 1 k.k.

Znaczna ilość spośród badanych spraw dotyczyła oszustw na portalach aukcyjnych (głównie na *Allegro*) – przestępstw polegających na oferowaniu na aukcji internetowej nieistniejących (tj. niebędących w posiadaniu sprawcy) produktów z zamiarem wyłudzenia za nie zapłaty. Jeżeli sprawca korzystał z konta, które w tym celu założył, sytuacja jest jasna – swoim zachowaniem realizuje jedynie znamiona przestępstwa z art. 286 § 1 k.k. Zwykle jednak uzyskuje w tym celu dostęp do profilu użytkownika, który miał już wyrobioną dobrą opinię (sprzedawał bądź kupował za pośrednictwem danego portalu aukcyjnego jakieś towary i dał się poznać jako rzetelny kontrahent, w związku z czym zebrał pewną liczbę pozytywnych ocen i komentarzy), i podszywając się, popełnia przestępstwo. W takiej sytuacji należy przyjąć, iż ma miejsce zbieg kumulatywny art. 267 § 2 k.k. (nieuprawnione uzyskanie dostępu do konta w serwisie aukcyjnym), art. 268a § 1 k.k. (uniemożliwienie korzystania z konta jego użytkownikowi oraz modyfikacja danych) oraz art. 286 § 1 k.k. Należy przy tym pamiętać, że przestępstwa z art. 267 § 2 i art. 268a § 1 k.k. są przestępstwami wnioskowymi. Brak wniosku będzie więc skutkował przyjęciem kwalifikacji jedynie z art. 286 § 1 k.k. (co zresztą się zdarzało w badanych sprawach i jest widoczne w zestawieniach zawartych w części wcześniejszej).

Wielość zachowań może skutkować zastosowaniem konstrukcji czynu ciągłego (art. 12 k.k.) lub ciągu przestępstw (zob. przedostatni stan faktyczny omawiany w czwartej części raportu).

Istotną kwestią, która pojawiła się ostatnimi czasy, są „kradzieże" przedmiotów, pieniędzy lub postaci w wirtualnych światach, przede wszystkim w grach MMORPG[186] lub MMORLG[187]. W badanych sprawach dotyczących tego problemu zwykle skupiano się na fakcie włamania na konto użytkownika w grze lub związanym z tym utrudnianiu korzystania z niego przez pokrzywdzonego lub modyfikacji danych komputerowych, przyjmując kwalifikację z art. 267 § 1 w zb. z art. 268a § 1 w zw. z art. 11 § 2 k.k. W wielu wypadkach istotny stawał się jednak aspekt ekonomiczny związany z tym, że wirtualne przedmioty, postaci oraz wirtualne pieniądze mogą mieć realną wartość majątkową[188], a sprawca dopuszczający się czynu polegającego na zdobyciu władztwa nad nimi działał w celu uzyskania korzyści majątkowej (np. sprzedawał następnie „skradzione" przedmioty na aukcji internetowej za „realne" pieniądze), a w związku z tym jego zachowanie wypełniało również znamiona przestępstwa z art. 287 § 1 k.k. Dlatego też w takim przypadku należy stosować kumulatywną kwalifikację z art. 267 § 2 w zb. z art. 287 § 1 w zw. z art. 11 § 2 k.k. (zob. siódmy stan faktyczny omawiany w czwartej części raportu)[189].

Najmniej trudności organom ścigania sprawiały stany faktyczne polegające na zakłóceniu pracy sieci informatycznej (np. w drodze ataków typu DoS), które prawidłowo kwalifikowano z art. 268a § 1 lub art. 269a k.k. (jak wspominano w części pierwszej raportu, zakresy przedmiotowe obu tych przepisów krzyżują się, a w większości wypadków, właśnie dotyczących zamachów na sieci informatyczne, wręcz pokrywają się).

Ponadto przepis art. 268a § 1 k.k. był trafnie wykorzystywany do kwalifikacji zachowań polegających na modyfikacji treści stron internetowych.

Pewne problemy natomiast pojawiły się na tle stosowania przepisu art. 269b § 1 k.k. W większości wypadków przepis ten błędnie, moim zdaniem, stosowano do stanów faktycznych, w których sprawca uzyskiwał dostęp do poczty elektronicznej (czy profilu w portalu społecznościowym, grze on-line) po przełamaniu zabezpieczenia w postaci hasła.

---

[186] Massively multiplayer online role-playing game (MMORPG) – gra on-line, w którą może grać wielu graczy, polegająca na wcielaniu się w wirtualne postacie i rywalizacji w wirtualnym świecie (zwykle fantastycznym, np. w świecie *Gwiezdnych wojen* w przypadku *Star Wars: The Old Republic*). Inne przykłady takich gier to *World of Warcraft* czy *Metin 2*.

[187] Massively multiplayer online real-life game (MMORLG) – gra on-line, w której użytkownik tworzy postać funkcjonującą w wirtualnym świecie (niejako równoległym do rzeczywistego i kształtowanym na jego podobieństwo). Tego typu gry potocznie nazywane są po prostu wirtualnymi światami (np. *Second Life*); zob. szerzej na ten temat J. Kulesza, J. Kulesza, *Gra „Second Life" – wirtualny świat, realne przestępstwa*, „Prokuratura i Prawo" 2009/3, s. 23 i 24; zob. też http://en.wikipedia.org/wiki/Virtual_world.

[188] Gracze w toku rozgrywki „ulepszają" postać (uzyskuje ona kolejne poziomy) oraz zdobywają wspomniane przedmioty (np. znajdując je, kupując za uzyskane w trakcie gry „wirtualne" pieniądze). Funkcjonuje jednak handel tymi dobrami. Takie transakcje odbywają się za pośrednictwem portali aukcyjnych. Większość producentów gier w swoich regulaminach zabrania tego procederu, nie mają jednak żadnych możliwości egzekwowania tego zakazu.

[189] Nieujęcie w kwalifikacji prawnej przepisu art. 268a § 1 k.k. wynika z faktu, iż w większości wypadków przepis ten będzie pochłaniany przez przepis art. 287 § 1 k.k. W przypadku jednak gdy sprawca po włamaniu na konto zablokuje dostęp do niego jego użytkownikowi (zmieniając hasło) lub je skasuje, przepis art. 268a § 1 k.k. nie zostanie pochłonięty i kwalifikacja powinna się przedstawiać w sposób następujący: art. 267 § 2 w zb. z art. 268a § 1 w zb. z art. 287 § 1 w zw. z art. 11 § 2 k.k.

Odzwierciedlenie w praktyce znalazły rozważania dotyczące zbiegów przestępstw będących przedmiotem badań z przestępstwami przeciwko mieniu oraz ustaw szczególnych (por. uwagi w pierwszej części raportu).

Z analizy przyjętych kwalifikacji prawnych wynika, iż zdecydowanie dominującą formą stadialną jest dokonanie – w opisie jedynie 13 czynów pojawiło się usiłowanie (art. 13 § 1 k.k.).

Na zakończenie należy zwrócić uwagę, iż niezwykle rzadko sięgano po przepis art. 65 § 1 k.k., umożliwiający zaostrzenie odpowiedzialności karnej w przypadku sprawcy, który z popełnienia przestępstwa uczynił sobie stałe źródło dochodu. Analiza wielu stanów faktycznych pozwala wysnuć wnioski, iż sytuacja taka miała miejsce, na co wskazuje np. zakres przestępczej działalności (ilość popełnionych czynów) czy fakt, iż w czasie ich popełnienia sprawca nie miał innych źródeł dochodu.

2.4. Oskarżeni

W sumie skierowano akty oskarżenia lub wnioski o warunkowe umorzenie przeciwko 134 osobom (dalej umownie nazywani oskarżonymi).

Wiek:

- 17–20 lat – 40 (30%)
- 21–25 lat – 33 (25%)
- 26–30 lat – 26 (26%)
- 31–40 lat – 22 (16%)
- 41–50 lat – 10 (7%)
- 51–60 lat – 1 (<1%)
- <60 lat – 2 (1,5%)

Wykształcenie:

- podstawowe – 8 (6%)
- gimnazjalne – 18 (13%)
- zawodowe – 11 (8%)
- średnie – 68 (w tym 4 techników-informatyków oraz 4 techników-elektroników) (51%)
- licencjat – 2 (1,5%)
- wyższe – 27 (w tym 7 informatyków, 1 grafik komputerowy, 1 inżynier telekomunikacji) (20%)

Zatrudnienie:

- pracujący/-ca – 66 (49%)
- na utrzymaniu rodziców – 41 (30%), w tym:
  - 6 studentów/studentek (4,5%)
  - 10 uczniów/uczennic (7,5%)
- na utrzymaniu małżonka – 5 (4%)
- niepracujący/-ca (zasiłek ewentualnie prace dorywcze) – 22 (16%)

Płeć:

- kobiety – 25 (19%)
- mężczyźni – 109 (81%)

Stan cywilny:

- panna – 19 (14%)/kawaler – 74 (55%) – łącznie 83 osoby (69%)

- zamężna – 5 (3,7%)/żonaty – 31 (23%) – łącznie 36 osób (26,7%)
- rozwiedziona – 1 (<1%)/rozwiedziony – 5 (3,7%) – łącznie 6 osób (4,5%)

Dzieci:

- tak – 33 (25%)
- nie – 101 (75%)

Karalność:

- karany/-na – 15 (11%)
- niekarany/-na – 117 (87,5%)
- brak danych – 2 (1,5%)

Wśród oskarżonych dominowali ludzie bardzo młodzi – większość nie ukończyła 26. roku życia (30% stanowiły osoby w wieku 17–20 lat, a 25% – w wieku 21–25 lat; osoby w wieku powyżej 40 lat stanowiły niecałe 10%). W istotnym stopniu młody wiek rzutował na wykształcenie (większość oskarżonych miała wykształcenie średnie – 51%, a dość duży odsetek, bo 13% – gimnazjalne), stan cywilny (osoby stanu wolnego – nie licząc rozwiedzionych – stanowiły niemal 70% ogółu), sytuację rodzinną (tylko 25% posiadało dzieci) czy karalność (uprzednio karani stanowili jedynie 11%). Zdecydowaną większość oskarżonych stanowili mężczyźni – 81%. Z racji wykształcenia, związanego z informatyką bezpośrednio (7 informatyków – 5%, 4 techników-informatyków – 3%) lub pośrednio (inżynier telekomunikacji, 4 technicy-elektronicy, grafik komputerowy – łącznie 5% ogółu), 17 podejrzanych (13%) miało „wiedzę dotyczącą komputerów" większą niż przeciętny użytkownik.

Wśród form zjawiskowych dominowało jednosprawstwo (jedynie w dziewięciu sprawach pojawiło się współsprawstwo). Odnotowano jeden przypadek pomocnictwa[190]. W ani jednej sprawie nie wystąpiło podżeganie.

2.5. Problematyka wymiaru kary

Akty oskarżenia skierowano do sądów w 102[191] spośród badanych spraw. W 63 postępowaniach zapadły wyroki skazujące, w 9 wypadkach sąd warunkowo umorzył postępowanie, 3 zostały umorzone na podstawie art. 17 § 1 pkt 10 k.p.k., 2 skończyły się uniewinnieniem, 8 spraw jeszcze się toczyło, 1 sprawa była zawieszona, 1 zakończyła się ugodą, co do 11 – brak danych. W jednym wypadku zapadł wyrok, w którym co do dwóch czynów sąd umorzył postępowanie warunkowo, a w kwestii trzeciego – uniewinnił. W celach statystycznych został on potraktowany jako dwa orzeczenia.

W związku z powyższym wśród 81 spraw, w których znane są rozstrzygnięcia, skazaniem zakończyło się 78%, warunkowym umorzeniem – 12,34%, umorzeniem –3,7%, uniewinnieniem – 3,7%, natomiast zawarciem ugody – 1,2%.

W sumie skazano 67 sprawców, z czego jedynie wobec 3 z nich orzeczono kary bezwzględnego pozbawienia wolności, w wymiarze:

[190] Prokuratura Rejonowa Kraków-Śródmieście Zachód (2 Ds170/09).

[191] Liczba spraw jest inna niż liczba aktów oskarżenia ze względu na przekształcenia, jakie zachodziły w toku postępowań sądowych (miało miejsce zarówno łączenie postępowań, jak i wyłączenia do odrębnego rozpoznania).

– 1 rok i 2 miesiące[192];
– 2 lata i 6 miesięcy (wobec sprawcy orzeczono ponadto: grzywnę 250 stawek po 10 zł, obowiązek naprawienia szkody w całości, przepadek na podstawie art. 44 § 2 k.k.)[193];
– 3 lata (wobec sprawcy orzeczono ponadto: grzywnę 360 stawek po 30 zł, obowiązek naprawienia szkody w całości, przepadek na podstawie art. 44 § 2 k.k.)[194].

W stosunku do 40 sprawców orzeczona zastała kara pozbawienia wolności z warunkowym zawieszeniem jej wykonania w wymiarze: 3 miesiące (6 przypadków), 4 miesiące (3 przypadki), 6 miesięcy (10 przypadków), 5 miesięcy (1 przypadek), 8 miesięcy (5 przypadków), 10 miesięcy (4 przypadki), 1 rok (4 przypadki), 1 rok i 6 miesięcy (2 przypadki), 1 rok i 10 miesięcy (1 przypadek), 2 lata (3 przypadki), 3 lata (1 przypadek).

Okresy próby wynosiły: 23 razy – 3 lata, 13 razy – 2 lata, 3 razy – 5 lat, 1 raz – 4 lata. W 16 przypadkach oddano skazanego pod dozór, 4 razy orzeczono przepadek dowodów na podstawie art. 44 § 2 k.k., 2 razy nałożono obowiązek przeproszenia pokrzywdzonego, 12 razy zobowiązano skazanego do naprawienia szkody, w 19 przypadkach orzeczono grzywnę (stawki najczęściej 10 zł – w 14 wypadkach, w pozostałych niewiele wyższe: 4 razy – 20 zł, najwyższa – 50 zł, bardziej zróżnicowana była ilość stawek – od 10 do 70, w jednym wypadku – 150 i również w jednym – 300).

Jedynie 7 sprawców skazano na karę ograniczenia wolności: 3 razy na 6 miesięcy (z obowiązkiem kontrolowanej, nieodpłatnej pracy w wymiarze w 2 wypadkach 20 godzin na miesiąc, w 1 – 40), 2 razy na 8 miesięcy (z obowiązkiem pracy w jednym wypadku w wymiarze 20 godzin miesięcznie, w drugim – 30), 1 raz na 10 miesięcy (z obowiązkiem pracy w wymiarze 20 godzin miesięcznie), 1 raz na 12 miesięcy (z obowiązkiem pracy w wymiarze 20 godzin miesięcznie). Ponadto 1 sprawcę zobowiązano do naprawienia szkody, raz orzeczono przepadek dowodów na podstawie art. 44 § 2 k.k. W przypadku jednego sprawcy na wniosek kuratora zamieniono orzeczoną karę ograniczenia wolności na karę pozbawienia wolności[195].

Karę grzywny orzeczono 17 razy (w 7 wypadkach wysokość stawki dziennej ustalono na 10 zł, w 6 – 20 zł, w 2 – 30 zł, w jednym wypadku 25 zł; ilość stawek wahała się od 10 do 100, przy czym bliższa była tej pierwszej wartości). W jednym wypadku zawieszono wykonanie kary grzywny (w wymiarze 100 stawek dziennych wysokości 10 zł) na dwa lata[196].

Jedna sprawa zakończyła się ugodą, zawartą już w toku postępowania, po wniesieniu przez oskarżonego sprzeciwu od wyroku nakazowego. W treści ugody zobowiązał się on do przeproszenia pokrzywdzonego oraz zapłacenia 5000 zł tytułem zadośćuczynienia.

W 10 sprawach sąd umorzył warunkowo postępowanie (w 6 wypadkach na okres próby wynoszący 2 lata, w 4 – 1 rok; jednego sprawcę zobowiązano do naprawienia

[192] Olsztyn (połączone sprawy 1Ds894/10, 1Ds128/10, 1Ds1207/10).
[193] Gdańsk (6Ds52/09).
[194] Gdańsk (6Ds52/09).
[195] Zakopane (Ds1057/10/D).
[196] Augustów (Ds340/09).

szkody, czterech do świadczenia pieniężnego wysokości od 500 do 1000 zł).

Przeciwko 26 osobom skierowano wnioski o warunkowe umorzenie postępowania (w 25 sprawach). Sąd wobec 18 z nich warunkowo umorzył postępowanie na okres 1 roku, wobec 6 – na 2 lata. Na 20 sprawców nałożony został obowiązek świadczenia pieniężnego (jego wysokość wahała się od 100 zł do 1000 zł, średnio wynosząc 357,50 zł). W jednym wypadku umorzono postępowanie z powodu cofnięcia wniosku o ściganie (art. 17 § 1 pkt 10 k.p.k.). W jednej sprawie zawarto ugodę (sprawczyni przeprosiła pokrzywdzoną i zobowiązała się do zapłaty na jej rzecz kwoty 2000 zł tytułem zadośćuczynienia).

Z powyższego wynika, iż orzeczone kary nie były surowe. Wynikało to przede wszystkim z młodego wieku sprawców oraz ich uprzedniej niekaralności. W większości spraw podejrzani przyznawali się do zarzucanych im czynów i zgadzali się na skazanie bez przeprowadzania rozprawy w trybie art. 335 k.p.k.

Bezwzględne kary pozbawienia wolności orzeczone zostały w dwóch sprawach. W pierwszej z nich[197], dotyczącej kilku oszustw na portalu aukcyjnym *Allegro*, była to kara 1 roku i 10 miesięcy wymierzona wobec sprawcy, który wcześniej był karany za podobne przestępstwa. Druga sprawa[198] była skomplikowana (blisko 800 pokrzywdzonych w całym kraju, ponad 120 tomów akt), a dotyczyła oszustw internetowych (zarówno przy użyciu portalu *Allegro* za pomocą przejętych wcześniej kont, jak i przy wykorzystaniu innych metod, np. za pomocą spreparowanej strony internetowej służącej wyłudzaniu pieniędzy w zamian za pośrednictwo w uzyskaniu pracy w Norwegii). Trzem sprawcom postawiono w sumie 276 zarzutów (pierwszemu – 48, drugiemu – 130, a trzeciemu – 98). Ustalono, że działalność przestępcza stanowiła ich jedyne źródło dochodów, nie tworzyli jednak zorganizowanej grupy – sprawca, który pełnił rolę inicjatora popełnianych przestępstw, współpracował z każdym z pozostałych współsprawców z osobna. Wszyscy trzej byli wcześniej karani za podobne czyny. Wobec dwóch orzeczono kary bezwzględnego pozbawienia wolności (w wymiarze odpowiednio: 2 lata i 6 miesięcy oraz 3 lata), w przypadku trzeciego sąd orzekł karę 2 lat pozbawienia wolności, ale zawiesił jej wykonanie na okres 5 lat.

Stosunkowo rzadko (jedynie 7 przypadków) orzekano środek karny w postaci przepadku narzędzia służącego popełnieniu przestępstwa. Należy przyjąć, że w większości wypadków byłoby to niewspółmierne do wagi popełnionego czynu. Ponadto w wielu wypadkach nie stanowiło ono własności sprawcy.

CZĘŚĆ 3. WNIOSKI KOŃCOWE

1. Obecny kształt regulacji dotyczącej przestępstw będących przedmiotem badań, tj. tzw. przestępstw komputerowych przeciwko ochronie informacji (zgrupowanych w rozdziale XXXIII k.k. „Przestępstwa przeciwko ochronie informacji", w przepisach art. 267–269b k.k.), nadała nowelizacja dokonana ustawą z 2008 r., mająca służyć m.in. implementacji postanowień decyzji ramowej 2005/222 w sprawie ataków na systemy informatyczne.

[197] Olsztyn (połączone sprawy 1Ds894/10, 1Ds128/10, 1Ds1207/10).
[198] Gdańsk (6Ds52/09).

2. W kodeksie karnym nie zawarto definicji użytych przez ustawodawcę pojęć, tj. systemu informatycznego oraz komputerowego, sieci teleinformatycznej, sieci telekomunikacyjnej, danych informatycznych oraz informatycznego nośnika danych, co zwłaszcza w przypadku trzech pierwszych terminów rodzi trudności interpretacyjne.

3. W wyniku nowelizacji kodeksu karnego z 2008 r. pojawił się nowy przepis – art. 267 § 2 k.k., który w zamierzeniu jej twórców miał zapewne stać się głównym narzędziem walki z hackingiem. Jednocześnie jednak pozostawiono w niezmienionym kształcie art. 267 § 1 k.k. Efektem opisanej sytuacji jest fakt, że niektóre zachowania (np. uzyskanie przez sprawcę dostępu do sieci teleinformatycznej za pomocą programu komputerowego) teoretycznie mogą być kryminalizowane z trzech przepisów – art. 267 § 1, art. 267 § 2 oraz art. 267 § 3 k.k.

4. Wątpliwości budzi również sama redakcja przepisu art. 267 § 2 k.k. – przewiduje on niezwykle szeroką kryminalizację, a jednocześnie zawiera odesłanie do norm pozaprawnych, pozostawiając tym samym zbyt dużą swobodę organom ścigania.

5. Jak zaznaczono, przepisy art. 268a i art. 269a k.k. nakładają się zakresowo, w związku z tym ten ostatni przepis wydaje się zbędny.

6. Przepis art. 269b k.k. jest wadliwie skonstruowany. Przede wszystkim nie przewidziano w nim wyłączenia odpowiedzialności uprawnionych osób (np. administratorów systemów czy inspektorów bezpieczeństwa), których zachowanie – mające na celu testowanie czy zabezpieczanie systemu informatycznego – może wypełnić znamiona określonego w nim przestępstwa. Ponadto nie znajduje on zastosowania do czynności przygotowawczych do przestępstwa hackingu *sensu stricto* (art. 267 § 1 oraz art. 267 § 2 k.k.).

7. W okresie objętym ogólnopolskimi badaniami (lata 2009–2010) odnotowano w sumie 1163 spraw, z których większość (750 spraw, czyli 64,49% ich ogólnej liczby) zakończyła się umorzeniem postępowania. Odmówiono wszczęcia postępowania w 213 przypadkach (18,31% ogólnej liczby spraw), a 68 spraw (5,85%) załatwiono w inny sposób. Jedynie w 102 sprawach (8,77%) do sądu skierowano akty oskarżenia. W 25 wypadkach (2,15%) prokurator sporządził wnioski o warunkowe umorzenie postępowania.

8. Zdecydowanie najczęstszymi powodami odmowy wszczęcia postępowania był brak wniosku o ściganie (art. 17 § 1 pkt 10 k.p.k.) – 98 czynów (40,33%) oraz brak znamion czynu zabronionego (art. 17 § 1 pkt 2 k.p.k.) – 71 przypadków (29,22%), natomiast w wypadku podstaw umorzeń postępowania zdecydowanie dominowało niewykrycie sprawcy czynu (art. 322 k.p.k.) – 444 przypadki (51,34%).

9. Najczęściej przyjmowanymi kwalifikacjami prawnymi, zarówno w postanowieniach o odmowie wszczęcia, jak i o umorzeniu, były przepisy art. 268a k.k. (odpowiednio 133 czyny, tj. 54,73%, oraz 406, tj. 46,99%) i art. 268 § 2 k.k. (odpowiednio 33 czyny, tj. 13,58%, oraz 101, tj. 11,69%).

10. Jak wykazały prowadzone badania, w praktyce pojawiają się problemy ze stosowaniem przepisów kryminalizujących hacking. Dotyczy to zwłaszcza wystąpienia rzeczywistego właściwego zbiegu przepisów art. 267 § 1 (lub art. 267 § 2) z art. 268a § 1 k.k., co ma miejsce np. w przypadku zachowań polegających na uzyskaniu nieuprawnionego dostępu do cudzego konta pocztowego (czy profilu na portalu społecznościowym), przy jednoczesnym uniemożliwieniu (poprzez zmianę hasła czy usunięcia

konta lub profilu) korzystania z niego przez pokrzywdzonego. Bardzo często taki czyn kwalifikuje się jedynie z art. 267 § 1 (lub art. 267 § 2) albo art. 268a § 1 k.k., zamiast przyjmować kumulatywną kwalifikację. Przepis art. 268 § 2 k.k., który powinien mieć zastosowanie jedynie do zachowań, których przedmiotem wykonawczym jest informatyczny nośnik danych, stosowany jest jak „wytrych" do ścigania sprawców wielu innych czynów (np. przejęcia profili na portalach społecznościowych i ich modyfikacji). Kolejnym problemem jest kradzież wirtualnych przedmiotów i postaci w grach on-line. W takich sprawach często skupiano się na fakcie włamania na konto w grze lub związanym z tym utrudnianiu korzystania z niego przez pokrzywdzonego lub (ewentualnie) modyfikacji danych komputerowych. Często pomijano zupełnie aspekt ekonomiczny – wirtualne przedmioty mają wszak realną wartość majątkową, a sprawca działał w celu uzyskania korzyści majątkowej, a w związku z tym jego zachowanie wypełniało również znamiona przestępstwa z art. 287 § 1 k.k. Pewne trudności rodziły się również w związku ze stosowaniem przepisu art. 269b k.k., który w wielu wypadkach używany był w sytuacjach, gdy sprawca złamał hasło do konta czy profilu, a następnie tą drogą uzyskał do niego nieuprawniony dostęp.

11. Niezwykle rzadko w kwalifikacjach prawnych pojawiał się przepis art. 65 § 1 k.k., umożliwiający zaostrzenie odpowiedzialności karnej w przypadku sprawcy, który z popełnienia przestępstwa uczynił sobie stałe źródło dochodu.

12. Większość oskarżonych stanowili ludzie młodzi (30% stanowiły osoby w wieku 17–20 lat, a 25% – w wieku 21–25 lat) oraz – co w wielu wypadkach było konsekwencją wieku –- o wykształceniu średnim (51%), stanu wolnego (nie licząc rozwiedzionych, niemal 70%), bezdzietnych (75%). Wykształcenie 17 osób (13%) było pośrednio lub bezpośrednio związane z informatyką. Blisko 81% oskarżonych stanowili mężczyźni. Tylko 11% oskarżonych było wcześniej karane.

13. Z 81 badanych spraw, w których znane są rozstrzygnięcia, skazaniem zakończyło się 78%, warunkowym umorzeniem – 12,34%, umorzeniem – 3,7%, uniewinnieniem – 3,7%, natomiast zawarciem ugody – 1,2%. W sumie skazano 67 sprawców, z czego: 3 na karę bezwzględnego pozbawienia wolności, 40 na karę pozbawienia wolności z warunkowym zawieszeniem jej wykonania, 7 na karę ograniczenia wolności oraz 17 na karę grzywny (w tym w jednym wypadku z zawieszeniem jej wykonania). Jak widać, orzeczone kary nie były surowe, co związane było przede wszystkim z wagą czynów, wiekiem sprawców i ich wcześniejszą niekaralnością.

14. Stosunkowo rzadko (jedynie w 7 przypadkach) orzekano środek karny w postaci przepadku narzędzia służącego popełnieniu przestępstwa. Wynikało to z dwóch zasadniczych przyczyn – z zachodzącej w większości wypadków niewspółmierności tego środka do wagi popełnionego czynu oraz okoliczności, iż w wielu wypadkach narzędzie nie stanowiło własności sprawcy.

CZĘŚĆ 4. WYBRANE STANY FAKTYCZNE

4.1. Prokuratura Rejonowa Kraków-Śródmieście Wschód w Krakowie (4Ds361/09/D)

Dnia 19.02.2009 r. w Krakowie Xavier G., dyrektor generalny i jednocześnie prokurent E. Polska sp. z o.o., zgłosił fakt popełnienia przestępstwa na szkodę

reprezentowanej przez siebie spółki. Twierdził on, że 18.02.2009 r. został poinformowany przez pracowników spółki, iż Urszula D., która była managerem ds. finansowo-administracyjnych w spółce do końca stycznia 2009 r., ostatniego dnia pracy usunęła istotne dla spółki dane ze służbowego komputera. Xavier G. podejrzewał, iż Urszula D. posiadała kopie zapasowe zniszczonych danych oraz mogła mieć zamiar udostępnienia ich konkurencji.

Dnia 24.02.2009 r. wszczęto dochodzenie w sprawie zniszczenia poprzez usunięcie danych należących do E. Polska sp. z o.o., tj. o przestępstwo z art. 268 § 2 k.k.

W toku postępowania przesłuchano szereg świadków, w tym wskazaną przez dyrektora generalnego jako sprawczynię Urszulę D. Potwierdziła ona, że w październiku 2008 r. zrezygnowała z pracy w spółce E., ale zgodnie z przepisami kodeksu pracy pracowała jeszcze przez okres wypowiedzenia, tj. do końca stycznia 2009 r. Ponieważ nie uzyskała informacji, komu powinna przekazać dane znajdujące się na użytkowanym przez nią służbowym komputerze, za radą prawnika spółki zarchiwizowała je, zabezpieczyła hasłem (były to bowiem dokumenty zawierające m.in. dane osobowe i tajemnice spółki) i pozostawiła w takim stanie na tymże komputerze. Nie znajdowały się one jednak w katalogu „Moje dokumenty", w nim bowiem – jak zeznała Urszula D. – przechowywała jednie bieżące dane (tj. z bieżącego roku), ale w katalogu „Ulubione". Z uwagi na to, że w dalszym ciągu nie wskazano jej osoby, która przejmie jej obowiązki, hasła nie podała nikomu. Dyrektor generalny, po pobieżnym przejrzeniu zawartości dysku komputera i nieznalezieniu wszystkich danych, chociaż miał dane kontaktowe Urszuli D., zamiast bezpośrednio zwrócić się do niej, zgłosił się na policję.

W związku z tym, że w toku dochodzenia stwierdzono, iż żadne dane nie zostały zniszczone, 30.03.2009 r. postępowanie umorzono z uwagi na brak znamion czynu zabronionego, tj. na podstawie art. 17 § 1 pkt 2 k.p.k.

4.2. Prokuratura Rejonowa w Wadowicach (1Ds275/10/D)

Dnia 5.02.2010 r. na komisariat w Wadowicach zgłosił się Bartosz J., uczeń liceum, który zawiadomił, że nieznany mu z imienia i nazwiska sprawca, poznany za pośrednictwem komunikatora *Gadu-gadu*, podający się za dziewczynę o imieniu Sandra, przełamał w dniach między 31.01.2010 r. a 3.02.2010 r. zabezpieczenia w postaci haseł zabezpieczających dostęp do jego konta poczty elektronicznej, profilu portalu *Nasza klasa* oraz konta w komunikatorze *Gadu-gadu*, a następnie korespondował w jego imieniu z jego znajomymi. Według pokrzywdzonego sprawca dokonał tego w ten sposób, że po nawiązaniu z nim kontaktu przez komunikator *Gadu-gadu* pod pretekstem wymiany zdjęć uzyskał adres poczty elektronicznej pokrzywdzonego. Znając jego dane (przede wszystkim datę jego urodzenia), podane przez niego w tzw. katalogu publicznym *Gadu-gadu*, złamał hasło zabezpieczające do kont poczty elektronicznej za pomocą opcji „przypomnij hasło", a następnie w podobny sposób uzyskał dostęp do profilu na *Naszej klasie* oraz do konta użytkownika w komunikatorze *Gadu-gadu*.

Dnia 4.03.2010 r. wszczęto dochodzenie w sprawie zamiany haseł dostępu do kont pocztowych, konta użytkownika *Gadu-gadu*, konta użytkownika *Naszej klasy*, zarejestrowanych na osobę Bartosza J., tj. o przestępstwo z art. 268a § 1 k.k.[199]

W toku postępowania ustalono na podstawie analizy logowań do przejętych kont, że sprawca korzystał z komputera, którego użytkownikiem była 17-letnia Sandra S.

Przesłuchana 16.04.2010 r. w charakterze podejrzanego Sandra S. przyznała się do popełnienia zarzucanego jej czynu, odmówiła składania wyjaśnień, złożyła wniosek o skierowanie sprawy do mediacji oraz o warunkowe umorzenie postępowania.

W czasie spotkania mediacyjnego, które miało miejsce 28.04.2010 r., zawarto ugodę. Sandra S. przeprosiła Bartosza J. oraz zobowiązała się do przeproszenia do 1.05.2010 r. za pośrednictwem komunikatora *Gadu-gadu* znajomych pokrzywdzonego, z którymi korespondowała tą drogą, podszywając się pod niego, a także (jeszcze tego samego dnia) podania hasła do kont pocztowych, komunikatora *Gadu-gadu* oraz profilu na *Naszej klasie*. Dnia 3.05.2010 r. Bartosz J. złożył wniosek o cofnięcie wniosku o ściganie, w związku z czym dochodzenie zostało umorzone następnego dnia na podstawie art. 17 § 1 pkt 10 k.p.k.

4.3. Prokuratura Rejonowa Warszawa-Praga Północ w Warszawie (7Ds463/10/III/IV)

Prezes zarządu A. SA – firmy prowadzącej jeden z większych sklepów internetowych w Polsce – zgłosił popełnienie na szkodę reprezentowanej przez niego spółki przestępstwa polegającego na blokowaniu serwerów do niej należących, które nastąpiło od 22.05.2010 r. do 26.05.2010 r. Jego przyczyną były ponawiane rozproszone ataki odmowy dostępu usług (dDoS). Wiązało się to ze stratami finansowymi firmy rzędu kilkudziesięciu tysięcy złotych dziennie, gdyż uniemożliwiło składanie zamówień przez potencjalnych klientów sklepu. Dnia 25.05.2010 r. otrzymano wiadomość e-mailową z ofertą „pomocy" w zabezpieczeniu serwerów przed dalszymi atakami w zamian za uiszczenie kwoty 793 USD za pośrednictwem systemu Western Union.

Dnia 28.06.2010 r. wszczęto śledztwo w sprawie usiłowania w dniach 22–26.05.2010 r. „doprowadzenia do niekorzystnego rozporządzenia mieniem w kwocie 793 USD groźbą zamachu na mienie poprzez przeprowadzenie ataku hackerskiego w istotny sposób zakłócającego pracę systemu komputerowego A. SA tj. o przestępstwo z art. 13 § 1 w zw. z 282 k.k. w zb. z 269a k.k."[200]. W toku

[199] Uważam, że w tym wypadku miał miejsce rzeczywisty właściwy zbieg przepisów art. 267 § 2 k.k. (sprawca uzyskał dostęp w sposób nieuprawniony do kont pokrzywdzonego) oraz art. 268a § 1 k.k. (sprawca uniemożliwił dostęp pokrzywdzonemu do kont), a w związku z tym należałoby przyjąć kwalifikację prawną z art. 267 § 2 w zb. z art. 268a § 1 w zw. z art. 11 § 2 w zw. z art. 12 k.k.

[200] Z uwagi na to, że sprawca działał w celu uzyskania korzyści majątkowej, zastosowanie powinien znaleźć przepis art. 287 § 1 k.k., który wyłączy na zasadzie konsumpcji przepis art. 269a k.k. Jednocześnie trzeba zwrócić uwagę, że sprawca nie osiągnął swojego celu (nie uzyskał korzyści majątkowej w postaci okupu), ale jednocześnie spowodował kilkudniowe zakłócenie pracy systemu informatycznego A. SA. W związku z tym wypełnił znamiona czynu zabronionego z art. 268a § 1 lub art. 269a k.k. Ponieważ zakłócenie przez niego wywołane można określić jako istotne, zastosowanie znajdzie ten drugi przepis. Stąd czyn należałoby, moim zdaniem, zakwalifikować z przepisu art. 13 § 1 w zw. z art. 282 w zb. z art. 287 § 1 w zw. z art. 11 § 2 w zb. z art. 269a w zw. z art. 11 § 2 k.k. Natomiast w wypadku, gdy działania sprawcy wyrządziłyby znaczną szkodę, z art. 13 § 1 w zw. z art. 282 w zb. z art. 294 § 1 w zw. z art. 11 § 2 w zb. z art. 269a w zw. z art. 11 § 2 k.k. lub z art. 13 § 1 w zw. z art. 282 w zb. z art. 294 § 1 w zw. z art. 11 § 2 w zb. z art. 268a § 2 w zw. z art. 11 § 2 k.k.

postępowania przesłuchano osobę odpowiedzialną za monitorowanie i zabezpieczenie serwerów, z których korzystała A. SA. Ustalono, że konto e-mail, z którego pochodziły wiadomości z żądaniem zapłaty, znajdowało się w Szwecji, a drugie konto poczty elektronicznej, z którego wysłana została wiadomość e-mail, należy do spółki z siedzibą w Krakowie, która to spółka zaprzeczyła, jakoby takie konto w ogóle istniało. W związku z powyższym śledztwo zostało umorzone na podstawie art. 322 § 1 k.p.k.

4.4. Prokuratura Rejonowa w Śremie (Ds1372/10/D)

Dnia 20.12.2010 r. Tomasz G. powiadomił policję o podejrzeniu dokonania w dniach 11–12.12.2010 r. włamania na jego konto poczty elektronicznej, a następnie skasowaniu jego profilu na portalu społecznościowym *Nasza klasa*. Dnia 22.12.2010 r. wszczęto dochodzenie w sprawie – jak to błędnie określono – „szkody w bazach danych", tj. o czyn z art. 268a § 1 w zw. z art. 12 k.k. W toku postępowania ustalono, że sprawcą przestępstwa jest Rafał S. (23 lata, wykształcenie zawodowe, zawód wyuczony: murarz, zatrudniony jako tapicer, kawaler, bezdzietny, niemający nikogo na utrzymaniu, niekarany), który przesłuchany w charakterze podejrzanego 24.01.2011 r. przyznał się do popełnienia zarzucanych mu przestępstw. Wyjaśnił, iż pokrzywdzony był niegdyś w związku z jego obecną partnerką Joanną D., a na portalu *Nasza klasa* umieścił wspólne ich zdjęcia z okresu, gdy byli jeszcze parą.

Złożono wniosek w trybie art. 335 k.p.k. o skazanie bez przeprowadzenia rozprawy. Sąd 15.02.2011 r. uznał oskarżonego za winnego popełnienia zarzucanych mu czynów, tj. przestępstw z art. 267 § 1 w zw. z art. 12 k.k. oraz art. 268a § 1 w zw. z art. 12 k.k.[201], i zgodnie z wnioskiem wymierzył mu za pierwszy czyn karę 4 miesięcy pozbawienia wolności, za drugi – 3 miesiące pozbawienia wolności. Jako karę łączną orzeczono karę 5 miesięcy pozbawienia wolności w zawieszeniu na 2 lata oraz grzywnę wysokości 20 stawek po 20 zł. Ponadto skazany został obciążony kosztami postępowania.

4.5. Prokuratura Rejonowa w Częstochowie (1Ds351/09)

Właściciel firmy PHU Z. R., będącej dostawcą usług internetowych za pośrednictwem sieci radiowej, zgłosił 23.02.2009 r. popełnienie przestępstwa polegającego na nieuprawnionym uzyskiwaniu dostępu do sieci do niego należącej i korzystania z niej bez uiszczania należnych opłat. Dnia 28.02.2009 r. wszczęto dochodzenie w sprawie „uzyskiwania informacji poprzez łącza radiowe od dnia 30.01 do 23.02.2009 r. na szkodę firmy PHU Z. R., tj. czyn z art. 267 § 2 k.k.". W wyniku prowadzonych czynności ustalono, iż sprawcą czynu był Radosław G. (20 lat, o wykształceniu średnim, zawód wyuczony: technik-handlowiec, kawaler, bezdzietny, niepracujący, pozostający na utrzymaniu rodziców, niekarany). Postawiono mu zarzut uzyskiwania od 30.01.2009 r. do 2.04.2009 r. nieuprawnionego

[201] Uważam, że w przypadku drugiego czynu należałoby przyjąć kumulatywną kwalifikację prawną z art. 267 § 2 w zb. z art. 268a § 1 w zw. z art. 11 § 2 w zw. z art. 12 k.k.

dostępu do sieci radiowej, czym spowodował straty wysokości 2000 zł na szkodę PHU Z. R. Przesłuchany w charakterze podejrzanego 2.04.2009 r. Radosław G. przyznał się do zarzucanego przestępstwa, wyjaśniając, iż niegdyś korzystał z usług firmy PHU Z. R. polegających na dostarczaniu dostępu do Internetu za pośrednictwem sieci radiowej. Z uwagi na sytuację finansową musiał jednak z nich zrezygnować. Za radą znajomego zainstalował w swoim komputerze program do wykrywania i uzyskiwania dostępu do sieci radiowych. Ponieważ sieć firmy PHU Z. R. nie była zabezpieczona przed nieuprawnionym dostępem, za pomocą posiadanego sprzętu i tegoż programu uzyskiwał do niej dostęp i łączył się z Internetem za jej pośrednictwem, nie płacąc przy tym należnych opłat (w postaci abonamentu). Prokurator złożył wniosek w trybie art. 335 k.p.k., w którym zaproponował wymierzenie kary 1 roku pozbawienia wolności w zawieszeniu na 3 lata, grzywny wysokości 20 stawek po 20 zł, oddanie na okres zawieszenia wykonania kary pod dozór kuratora, przepadek dowodu (komputera służącego sprawcy do popełnienia zarzucanego przestępstwa) oraz obciążenie kosztami postępowania. Sąd wyrokiem[202] z 9.09.2009 r. warunkowo umorzył postępowanie na okres 2 lat oraz zwolnił oskarżonego z kosztów postępowania na podstawie art. 624 § 1 k.p.k.

4.6. Prokuratura Rejonowa w Pruszkowie (4Ds1632/10)

Dnia 19.11.2010 r. aktor Radosław P. zawiadomił prokuraturę w Pruszkowie o popełnieniu przestępstwa polegającego na założeniu na portalu społecznościowym *Facebook* profilu z jego danymi osobowymi przez nieznanego sprawcę, który podszywał się pod pokrzywdzonego oraz korespondował z jego znajomymi z branży artystycznej. Ponadto sprawca dokonywał wpisów komentujących aktywność podejmowaną przez innych użytkowników na *Facebooku* (umieszczane zdjęcia, komentarze, filmy itp.), czym niejednokrotnie szkodził reputacji i dobremu imieniu pokrzywdzonego. Dnia 29.12.2010 r. wydano postanowienie o odmowie wszczęcia dochodzenia w sprawie zmiany zapisu na informatycznym nośniku danych poprzez utworzenie profilu Radosława P. na portalu społecznościowym *Facebook* bez wiedzy i zgody pokrzywdzonego, tj. o czyn z art. 268 § 2 na zasadzie art. 17 § 1 pkt 2 k.k., z uwagi na brak znamion czynu zabronionego[203].

4.7. Prokuratura Rejonowa w Zakopanem (Ds1057/10/D)

Jarosław P. zgłosił, że nieznany sprawca w nieokreślonym precyzyjnie czasie przed 22.03.2010 r. uzyskał dostęp do jego konta poczty elektronicznej, a dzięki temu do konta w grze on-line *Metin2*. Pozbawił postać należącą do pokrzywdzonego

[202] W wyroku przyjęto kwalifikację prawną identyczną jak w akcie oskarżenia (art. 267 § 2 k.k.). Natomiast z uwagi na fakt, iż na czyn sprawcy składało się więcej zachowań podjętych w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru uzyskania korzyści majątkowej (poprzez uniknięcie przez sprawcę powstania pasywów wynikających z konieczności uiszczania opłat za korzystanie z dostępu do Internetu, co sam przyznał), zasadne byłoby przyjęcie następującej kwalifikacji: art. 267 § 2 w zb. z art. 287 w zw. z art. 11 § 2 w zw. z art. 12 k.k.

[203] Obecnie – jak już sygnalizowano – zachowanie sprawcy w takim przypadku mogłoby zostać zakwalifikowane jako tzw. *stalking* (art. 190a § 2 k.k.).

ekwipunku w postaci 3 mieczy, 4 zbroi, 1 hełmu, 2 kolczyków, 2 tarcz, 6 naszyjników, 7 par butów oraz wirtualnych pieniędzy (60 milionów yang).

Dnia 2.04.2010 r. wszczęto dochodzenie w sprawie zamiany haseł dostępu do poczty elektronicznej oraz do konta w grze *Metin2*, ujawnionej 22.03.2010 r. w Zakopanem, na szkodę Jarosława P., tj. o przestępstwo z art. 269b § 1 w zb. z art. 267 § 1 w zb. z art. 268a § 1 w zw. z art. 11 § 2 k.k.

Sprawcą przestępstwa okazał się Wojciech S. (17 lat, o wykształceniu gimnazjalnym, bez zawodu, niepracujący, będący na utrzymaniu babci, kawaler), który hasła dostępowe uzyskał dzięki użyciu tzw. *keyloggera* (programu zainstalowanego w komputerze ofiary przestępstwa, przechwytującego hasła i inne dane wpisywane za pomocą klawiatury – stąd nazwa).

Dnia 14.09.2010 r. skierowano do sądu akt oskarżenia, w którym Wojciechowi S. zarzucono pozyskanie przy pomocy *keyloggerów* dostępu do gry on-line *Metin2*, czym działał na szkodę Jarosława P, tj. o czyn z art. 269b § 1 k.k., oraz o uzyskanie bez uprawnienia dostępu do konta poczty elektronicznej Jarosława P. poprzez ominięcie informatycznych zabezpieczeń, a następnie dokonanie zmiany haseł do *Metin2*, przez co utrudnił dostęp do tejże gry pokrzywdzonemu, a następnie pozbawił postać należącego do niej wirtualnego ekwipunku (tj. o czyn z art. 268a § 1 w zb. z art. 267 § 1 w zw. z art. 11 § 2)[204].

Sąd w wyroku z 28.12.2010 r. uznał oskarżonego winnym zarzucanych mu czynów. Za pierwszy z nich orzeczona została kara 4 miesięcy ograniczenia wolności oraz praca społeczna w wymiarze 20 godzin miesięcznie. Za drugi czyn wymierzona została kara identycznej wysokości. Jako karę łączną orzeczono 6 miesięcy ograniczenia wolności oraz prace społeczne w wymiarze 20 godzin na miesiąc. Skazany został zwolniony od ponoszenia kosztów postępowania. Ponieważ uchylał się on od wykonania kary, została mu ona wyrokiem z 28.02.2011 r. zamieniona na zastępczą karę 90 dni pozbawienia wolności.

4.8. Prokuratura Rejonowa w Świdnicy (1Ds2266/10/D)

Dnia 20.10.2010 r. do Komendy Wojewódzkiej we Wrocławiu wpłynęło sporządzone przez pełnomocnika banku PKO BP SA zawiadomienie o podejrzeniu popełnienia przestępstwa na szkodę jego klientów. Przestępstwo polegało na wyłudzaniu od klientów korzystających z serwisów internetowych www.ipko.pl oraz www.inteligo.pl danych służących do logowania w nich oraz numerów kart płatniczych. Służyć temu miały strony internetowe łudząco przypominające wskazane wyżej serwisy banku. Sprawcy udało się w ten sposób wprowadzić w błąd co najmniej kilku klientów banku i za pomocą uzyskanych numerów kart dokonać szeregu

[204] Uważam, że kwalifikacje czynów sprawcy powinny wyglądać odmiennie. Po pierwsze – w przypadku pierwszego czynu powinna zostać przyjęta kwalifikacja prawna z art. 267 § 1 k.k. Po drugie – w przypadku drugiego czynu wydaje się, że właściwsze byłoby zastosowanie przepisu art. 267 § 2 k.k., zamiast art. 267 § 1 k.k., gdyż sprawca owszem przełamał zabezpieczenie, ale z drugiej strony nie uzyskał dostępu do informacji – wirtualne „przedmioty" są danymi informatycznymi, ale raczej dyskusyjne jest uznanie ich za informacje. Zatem kwalifikacja powinna wyglądać następująco: art. 267 § 2 w zb. z art. 268a § 1 w zw. z art. 11 § 2 k.k. Ponadto uzyskany ekwipunek owszem był wirtualny, ale posiadał określoną wartość rynkową. Jeżeli sprawca przestępstwa działałby w celu uzyskania korzyści majątkowej (np. sprzedaży uzyskanych „przedmiotów" na aukcji internetowej), należałoby jego zachowanie zakwalifikować z art. 267 § 2 w zb. z art. 287 § 1 w zw. z art. 11 § 2 k.k.

transakcji w Internecie. Dnia 9.12.2010 r. wszczęto w tej sprawie dochodzenie w kierunku popełnienia przestępstwa z art. 267 § 1 i 2 k.k. (w sprawie nielegalnego uzyskania informacji przez nieustaloną osobę wykorzystującą w tym celu specjalne oprogramowanie)[205].

W toku postępowania podjęto szereg czynności, przede wszystkim powołano biegłego w celu dokonania ekspertyzy dysku twardego komputera jednej z pokrzywdzonych osób. Jej celem miało być przede wszystkim ustalenie, czy znajdują się na dysku programy „sczytujące i przekazujące nieuprawnionym osobom dane kart płatniczych banku PKO BP SA". Biegły w sporządzonej opinii stwierdził, iż z dostarczonego przez bank wraz z zawiadomieniem o podejrzeniu popełnienia przestępstwa wydruku kodu źródłowego fałszywej strony internetowej banku wynika, iż prawdopodobnie na dysku użytkownika znajdował się specjalnie przez sprawcę spreparowany plik *cookie*, który podczas próby zalogowania na stronie banku przekierowywał użytkownika na fałszywą stronę, za pomocą której wymuszane było podanie danych karty płatniczej. Jednocześnie przeprowadzana była weryfikacja ich poprawności. W przypadku podania niepoprawnych danych okno dialogowe nie zamykało się, uniemożliwiając korzystanie z serwisu. Plik prawdopodobnie został umieszczony w systemie pokrzywdzonego za pomocą konia trojańskiego (trojana). Przypuszczalnie za pośrednictwem tego samego konia trojańskiego dane były przekazywane sprawcy. Jednak na dysku dostarczonym do badań biegły nie znalazł ani pliku, ani trojana – plik *cookie* został prawdopodobnie usunięty automatycznie przez przeglądarkę (miała włączoną opcję kasowania tego typu plików po 20 dniach od ich zapisania), a trojan – przez program antywirusowy. Tym samym nie było już żadnych śladów przestępstwa na badanym dysku. W związku z powyższym 18.03.2011 r. dochodzenie umorzono z uwagi na niewykrycie sprawcy, tj. na podstawie art. 322 k.p.k.

4.9. Prokuratura Rejonowa w Oleśnie (1Ds1166/10/D)

Pokrzywdzony Wojciech K. 26.07.2010 r. na portalu aukcyjnym *Allegro* wylicytował telefon *Apple Iphone 3GS* za kwotę 1705 zł (1725 zł po uwzględnieniu kosztów przesyłki). Natychmiast po tym fakcie zadzwoniła do niego z telefonu komórkowego osoba podająca się za sprzedawcę. W trakcie rozmowy sprzedający podał numer rachunku bankowego, na który pokrzywdzony miał wpłacić pieniądze. Był to inny rachunek niż podany na profilu *Allegro* sprzedającego, ale został on przez niego zaproponowany, gdy okazało się, że pokrzywdzony również ma rachunek w tym banku. Umówiono się, że telefon zostanie wysłany pocztą kurierską natychmiast po wpłynięciu pieniędzy na konto sprzedającego, najpóźniej 28.07.2010 r. Dnia 2.08.2010 r. do Wojciecha K. zatelefonował Łukasz O.-W., który poinformował go, że telefon został wylicytowany z konta na *Allegro* do niego należącego, ale nie on go na aukcję wystawił. Zasugerował, że zostało ono przejęte i nieznana mu osoba posłużyła się nim. Łukasz O.-W. o całej sprawie wie stąd, że nie mógł zalogować

[205] Wydaje się, że chodzi tutaj raczej o przepis art. 267 § 3 k.k. (przed nowelizacją kodeksu karnego z 2008 r. – art. 267 § 2 k.k.). Uważam jednak, że powinna zostać przyjęta następująca kwalifikacja: art. 267 § 1 w zb. z art. 287 § 1 w zw. z art. 11 § 2 w zw. z art. 12 k.k. Sprawca bowiem po ominięciu zabezpieczenia uzyskał dostęp do informacji, do których nie był uprawniony, czyli dane kart płatniczych, a następnie przy ich użyciu skorzystał ze środków pieniężnych zgromadzonych na rachunkach pokrzywdzonych.

się na konto i skontaktował się z obsługą serwisu *Allegro*, która poinformowała go o możliwości przejęcia konta przez osobę trzecią.

Wojciech K. tego samego dnia złożył zawiadomienie o popełnieniu przestępstwa na jego szkodę. Dnia 2.09.2010 r. wszczęto dochodzenie w sprawie oszustwa na kwotę 1725 zł przy sprzedaży telefonu marki *Apple iPhone 3GS*, dokonanego 26.07.2010 r. za pośrednictwem portalu aukcyjnego *Allegro*, na szkodę Wojciecha K., tj. o czyn z art. 286 § 1 k.k.

Równolegle wszczęte dochodzenie (prowadzone przez Komendę Rejonową Policji Warszawa IV (1ds1359/10)) w sprawie nieuprawnionej ingerencji w dane informatyczne 23.07.2010 r. – konto na portalu *Allegro* zarejestrowane na Łukasz O.-W. z jednoczesnym przełamaniem zabezpieczeń informatycznych tego konta, tj. o przestępstwo z art. 268a § 1 k.k., postanowiono dołączyć do omawianego postępowania. Powodem takiej decyzji było oczywiście wysokie prawdopodobieństwo, że obu czynów dokonał ten sam sprawca. Postępowanie prowadzono w sprawie popełnienia przestępstwa z art. 268a § 1 w zb. z art. 286 § 1 w zw. z art. 11 § 2 k.k.[206]

W toku omawianego postępowania przeprowadzono szereg czynności mających na celu ustalenie osoby sprawcy. W pierwszej kolejności zwrócono się do QXL Poland sp. z o.o. (właściciela portalu *Allegro*) o podanie numeru IP, z jakiego logował się sprawca do portalu *Allegro*. Po jego uzyskaniu próbowano od dostawcy usług internetowych, do którego puli należał wskazany adres IP, uzyskać dane użytkownika, który korzystał z tego adresu. Ten jednak nie był w stanie określić, komu przypisany był ten numer w czasie popełnienia przestępstwa. Niemożliwe okazało się ustalenie, do kogo należał numer telefonu, z którego sprawca korzystał, kontaktując się z pokrzywdzonym, gdyż okazało się, że był to numer przyporządkowany do karty *prepaid*. Analogiczna sytuacja miała miejsce w przypadku numeru rachunku bankowego, którym sprawca się posłużył – z danych udostępnionych przez WBK Bank Zachodni SA wynikało, iż było to konto typu *prepaid*. W związku z powyższym dochodzenie zostało umorzone z powodu niewykrycia sprawcy, tj. na podstawie art. 322 § 1 k.p.k.

4.10. Prokuratura Rejonowa w Braniewie (Ds463/09/D)

Dnia 14.02.2009 r. na Komendę Miejską Policji w Koszalinie zgłosiła się Aneta R. w celu zgłoszenia popełnionego przestępstwa. Nieznany sprawca 30.12.2008 r. włamał się na jej konto w portalu *Nasza klasa*, zmienił dane osobowe, umieszczał zdjęcia pornograficzne oraz obraźliwe komentarze. Ponadto korespondował w jej imieniu z jej znajomymi, składając im niedwuznaczne propozycje. Dnia 16.03.2009 r. wszczęto dochodzenie w sprawie dokonania bez uprawnienia zmian w profilu użytkownika Anety R. na portalu *Nasza klasa* oraz zamieszczania tam treści ją znieważających, tj. przestępstwo określone w art. 268a § 1 w zb. z art. 216 § 2 w zw. z art. 11 § 2 w zw. z art. 12 k.k.[207]

[206] W opisie czynu pominięto fakt, że sprawca uzyskał nieuprawniony dostęp do profilu na *Allegro*. Stąd jego zachowanie należało zakwalifikować z art. 267 § 2 w zb. z art. 268a § 1 w zb. z art. 286 § 1 w zw. z art. 11 § 2 k.k.

[207] W kwalifikacji tej – podobnie jak w przypadku wcześniej omawianej sprawy – nie uwzględniono fragmentu czynu w postaci uzyskania przez sprawcę dostępu do profilu pokrzywdzonej (art. 267 § 2 k.k.). Powinna ona się przedstawiać następująco: art. 267 § 2 w zb. z art. 268a § 1 w zb. z art. 216 § 2 w zw. z art. 11 § 2 w zw. z art. 12 k.k.

W toku postępowania ustalono, że sprawca logował się do konta Anety R. z komputera należącego do Huberta P., zamieszkałego w Pieniężnie. Okazało się, że sprawczyniami włamania do konta Anety R. były jego córka Amanda P. (wiek 15 lat, uczennica gimnazjum) oraz jej koleżanka Aneta R. (wiek 15 lat, uczennica gimnazjum). W związku z tym, że obie były nieletnie, sprawę przekazano według właściwości do dalszego prowadzenia Wydziałowi Rodzinnemu i Nieletnich Sądu Rejonowego w Braniewie. W trakcie wysłuchania nieletnie zeznały, iż na konto pokrzywdzonej dostały się przez przypadek, próbując uzyskać dostęp do konta jednej z nich. Prawdopodobnie pomyliły litery, wpisując hasło. Stwierdziły, iż dokonując modyfikacji konta pokrzywdzonej, działały pod wpływem chwili, zapewne sądząc, że robią po prostu żart, działając w poczuciu bezkarności, nie zdając sobie sprawy, iż mogą grozić im jakieś konsekwencje, a tym bardziej że ich zachowanie wypełnia znamiona przestępstwa.

Dnia 29.07.2009 r. Sąd Rejonowy w Braniewie wydał postanowienie o zastosowaniu środków wychowawczych wobec Anety R. i Amandy P. w postaci upomnienia (art. 6 pkt 1 ustawy o postępowaniu w sprawach nieletnich[208]). Jednocześnie orzeczono o zwrocie dowodu rzeczowego (komputera) rodzicom nieletniej Amandy P. oraz o nieobciążaniu ich kosztami postępowania.

[208] Ustawa z 26.10.1982 r. o postępowaniu w sprawach nieletnich (tekst jedn.: Dz. U. z 2010 r. Nr 33, poz. 178 ze zm.).

Summary

Filip Radoniewicz – ***Criminal liability for the offence of hacking***

This report presents the results of research conducted in 2012 on hacking in the broad sense (prohibited acts described in the provisions of Art. 267–269b of the Criminal Code). It consists of four basic parts.

The first part contains an analysis of the statutory features of prohibited acts typified in the provisions of Art. 267 § 1–4, Art. 268 § 1–3, Art. 268a § 1–2, Art. 269 § 1–2, Art. 269a and art. 269b § 1 of the Criminal Code. It also discusses the problems of concurrence of the aforementioned provisions, the choice of penalty and the mode of prosecution.

The second part presents the results of nationwide empirical research on hacking, under which preparatory proceedings files registered in universal prosecution organization units in 2009–2010 were analysed.

The third part presents the conclusions from both analysis of statutory features of prohibited acts being the subject of this report and the conducted research.

Finally, the fourth part presents the facts of selected cases.