INSTYTUT WYMIARU SPRAWIEDLIWOŚCI

dr Konrad Buczkowski

Skuteczność zwalczania przestępstw przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji na podstawie badań aktowych przestępstwa z art. 287 k.k.

Warszawa 2015

Spis treści

Wprowadzenie

Ostatnie ćwierćwiecze to okres niezwykle szybkiego rozwoju technik komputerowych oraz rozprzestrzenienia się dostępu do sieci Internetu. Przez okres 12 lat – pomiędzy rokiem 1990 a 2002 liczba osób korzystających z Internetu wzrosła 224-krotnie i w 2002 r. wyniosła ponad 631 milionów[1]. Szacuje się również, że pomiędzy rokiem 2000 a 2010 liczba osób korzystających z zasobów Internetu wzrosła pięciokrotnie, zbliżając się do dwóch miliardów. Największe procentowe przyrosty liczby użytkowników Internetu miały miejsce na obszarze Afryki – 2357% wzrostu pomiędzy rokiem 2000 a 2010, Bliskiego Wschodu – 1825%, Ameryki Południowej – ponad 1033% oraz Azji – 622%. Oczywiście przyrost taki był wynikiem niskiej bazy w roku 2000 dla tych kontynentów. Dla porównania wzrost liczby użytkowników Internetu w Ameryce Północnej wyniósł tylko 146%, a w Europie – 352%, przy czym oba te kontynenty w 2000 r. miały podobną liczbę osób korzystających z sieci[2].

Powyższe dane posłużyć mają jako ilustracja zjawiska, które stało się obecnie dla ogromnej części mieszkańców naszego globu czymś tak oczywistym jak jedzenie czy sen. Internet zmienił nasze codzienne życie, ma również wpływ na upowszechnianie się nowych zjawisk społecznych, politycznych czy prawnych[3]. Wystarczy wskazać, że w trzecim kwartale 2015 r. tylko użytkowników sieci społecznościowej Facebook było ponad 1,5 mld., prawie trzykrotnie tyle, ile wszystkich użytkowników Internetu w 2000 r.[4].

Stały postęp techniczny spowodował, że współcześnie w zasadzie wszystkie przejawy życia społecznego i gospodarczego powiązane są z wykorzystaniem komputerów i dostępem do Internetu. Część zarówno profesjonalnych, jak i prywatnych zasobów (dokumentów, zdjęć) istnieje tylko w postaci zapisu

---

[1] Za: http://www.worldmapper.org/posters/worldmapper_map336_ver5.pdf (dostęp dnia 17 listopada 2015 r.).

[2] Za: http://royal.pingdom.com/2010/10/22/incredible-growth-of-the-internet-since-2000/ (dostęp dnia 17 listopada 2015 r.).

[3] Zob. J. Janowski, *Globalna cyberkultura polityki i prawa*, por. http://www.bibliotekacyfrowa.pl/Content/46512/23_Jacek_Janowski.pdf (dostęp dnia 17 listopada 2015 r.).

[4] Za: http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (dostęp dnia 17 listopada 2015 r.).

elektronicznego na dyskach komputerowych. Duża grupa użytkowników przechowuje je nie tylko we własnych (czy użytkowanych przez siebie) komputerach, lecz wykorzystuje do tego celu tzw. chmury (*cloud*) oferowane przez wielu dostawców. Przykładowo liczba użytkowników takiego rozwiązania oferowanego przez Dropbox w maju 2014 r. przekroczyła 300 mln[5]. Również coraz większa grupa użytkowników zaczyna korzystać z kompleksowych rozwiązań, które pozwalają na rezygnację z utrzymywania bardzo kosztownej infrastruktury w zamian za miesięczną opłatę za dostęp do oprogramowania i danych umieszczonych na serwerach producenta.

Zarządzanie ruchem lotniczym, nadzór nad prawidłowymi dostawami prądu, gazu czy wody, czy korzystanie z różnego rodzaju usług telekomunikacyjnych, bankowych, dokonywanie zakupów przez strony WWW, to tylko kilka kolejnych przykładów wskazujących na coraz silniejsze uzależnienie nowoczesnego społeczeństwa od sieci komputerowych i bardzo szybkiego przesyłu danych na znaczne odległości.

Tym wszystkim – pozytywnym – zmianom towarzyszą jednak również zjawiska niekorzystne. Im bardziej świat jest uzależniony od techniki komputerowej oraz treści przesyłanych i zamieszczonych w sieci internetowej, tym bardziej jest narażony na działalność grup czy jednostek, których celem jest przejęcie kontroli nad systemami komputerowymi lub wejście w posiadanie informacji poufnych czy osobistych. W ostatnich latach istotnie wzrasta zagrożenie tzw. cyberterroryzmem[6].

Przestępczość komputerowa, która pojawiła się wraz z rozwojem systemów teleinformatycznych i wzrastającą liczbą operacji za pośrednictwem Internetu, to ta grupa czynów, której liczba będzie stale rosła. Jest to przestępczość trudna do wykrycia i zwalczania, pomimo istnienia jej śladów na nośnikach danych, wymagająca zaawansowanych metod analitycznych i znacznych środków na jej

[5] Za: https://www.quora.com/How-many-users-does-Dropbox-have (dostęp dnia 17 listopada 2015 r.).

[6] Zob. M. Czyżak, *Wybrane aspekty zjawiska cyberterroryzmu*, Telekomunikacja i techniki informacyjne 2010, nr 1–2, s. 45. W *Raporcie o stanie bezpieczeństwa w Polsce w roku 2014* stwierdza się: „Cyberprzestrzeń jest także wykorzystywana przez organizacje terrorystyczne (szczególnie Państwo Islamskie) – zarówno do prowadzenia bezpośrednich ataków (np. na serwery rządowe), uzyskiwania nieautoryzowanego dostępu do baz danych instytucji państwowych, dezinformacji, jak też do komunikacji, upowszechnienia radykalnej ideologii, pozyskiwania zwolenników czy prowadzenia instruktażu w zakresie podejmowania indywidualnych aktów terroru. Portale internetowe bywają również miejscem publikowania gróźb przeprowadzenia zamachu terrorystycznego", MSWiA, Warszawa 2014, s. 284, por. http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html (dostęp dnia 17 listopada 2015 r.).

zwalczanie. W dobie społeczeństwa informacyjnego, uzależnionego od „świata wirtualnego" będziemy coraz bardziej narażeni na stanie się ofiarą któregoś z przestępstw z tej grupy.

W literaturze przedmiotu brak zgody co do terminu, jakim powinno się określać czyny zabronione polegające na posługiwaniu się elektronicznymi systemami przetwarzania informacji do naruszania dóbr prawnie chronionych przez prawo karne. Oprócz określenia „przestępczość komputerowa" używa się takich określeń jak: przestępczość związana z komputerami, przestępczość przy użyciu zaawansowanych technologii, przestępczość internetowa czy wreszcie cyberprzestępczość.

Jak zauważa M. Siwicki: „Początkowo termin przestępczość komputerowa był rozumiany dwojako. Po pierwsze, jako przestępstwa komputerowe określano grupę czynów, polegających na posługiwaniu się komputerem do naruszenia jakiegokolwiek dobra prawnego chronionego przez prawo karne. W tym ujęciu komputer stanowił przedmiot lub środowisko zamachu. Po drugie, termin ten służył dla określenia przestępstw, które były popełniane przez osoby o wysokich umiejętnościach i wiedzy z zakresu elektroniki lub informatyki. W tym drugim ujęciu posiadanie przez sprawcę szczególnej wiedzy i umiejętności było traktowane jako istotny element przestępczości komputerowej"[7].

B. Michalski wskazuje, że „ten niezbyt precyzyjny termin obejmuje liczną kategorię szkodliwych w różnym stopniu czynów związanych z funkcjonowaniem elektronicznego gromadzenia, przetwarzania i przesyłania informacji, polegających między innymi na naruszaniu uprawnień do programu komputerowego, bezprawnej ingerencji w gromadzone, przetwarzane informacje lub w nośniki tych informacji,

[7] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 10. Wiele prób definicyjnych pojawiło się w literaturze niemieckiej. R.A.H. von Zur-Mühlen za przestępczość komputerową uważał „każde przestępcze działanie, w którym komputer stanowi albo narzędzie albo przedmiot zamachu". U. Sieber wskazywał, że przestępczość komputerowa obejmuje przestępstwa przeciwko mieniu, w których dane komputerowe zostają trwale zmienione, zniszczone, w bezprawny sposób pozyskane i wykorzystane wraz z komputerem. H.J. Schneider za przestępstwa komputerowe uważał „przestępstwa, przy których urządzenia służące do elektronicznego przetwarzania danych zostają wykorzystane jako narzędzie przestępstwa lub przy których takie urządzenia są przedmiotem zamachu". Podaję za: M. Siwicki, *Cyberprzestępczość*, s. 10–11. Na gruncie polskim próby zdefiniowania tego pojęcia podejmowali m.in. K. Jakubski i A. Adamski. Zob. K. Jakubski, *Przestępczość komputerowa – podział i definicja*, Przegląd Kryminalistyki 1997, nr 2, s. 31; A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 30.

systemy połączeń komputerowych itp., które najbardziej ogólnie określić można jako nadużywanie technologii informatycznych dla celów sprzecznych z prawem”[8].

Rozwój technologii informatycznych spowodował, że pojęcie „przestępczości komputerowej” przestało być wystarczające dla określenia wszystkich aspektów zjawiska przestępczości powiązanej z komputerami. Sieci i systemy teleinformatyczne mogą być zarówno przedmiotem zamachu, jak i środowiskiem tego zamachu, który może polegać na wykorzystaniu komputera w celu popełnienia przestępstw przeciwko bezpieczeństwu przetwarzanej informacji, czy też mogą naruszać dobra prawne tradycyjnie chronione przez prawo karne, jak rozpowszechnianie informacji zakazanych przez prawo lub pornografii z udziałem małoletnich. Pojawiło się zatem pojęcie „cyberprzestępczości”[9].

Jak zauważył A. Završnik ta zmiana terminologiczna związana jest z rozwojem nowych form popełniania cyberprzestępstw. W ramach tego rozwoju wyróżnił on trzy takie formy: pierwszą, która obejmowała zamachy skierowane na komputer, sieci komputerowe i dane (przestępczość komputerowa), drugą – związaną z działalnością hackerską oraz trzecią – obejmującą zautomatyzowane procesy popełniania cyberprzestępstw[10].

Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.[11] (dalej: Konwencja) jest pierwszym aktem prawa międzynarodowego zawierającym zbiór standardów prawnych służących ściganiu przestępczości transgranicznej,

---

[8] B. Michalski, Przestępstwa przeciwko mieniu. Rozdział XXXV kodeksu karnego. Komentarz, Warszawa 1999, s. 218.

[9] Szerzej: M. Siwicki, *Podział i definicja cyberprzestępstw*, Prokuratura i Prawo 2012, nr 7–8, s. 241–251.

[10] A. Završnik, *Cybercrime: definitional challenges and criminological particularities,* Masaryk University journal of law and technology 2008, vol. 2, no. 2, s. 4.

[11] ETS/STE No. 185 (Dz. U. z 2015 r. poz. 728); Polska przyjęła tę konwencję na podstawie ustawy z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (Dz. U., poz. 1514). Konwencja objęła Polskę od dnia 1 czerwca 2015 r. Należy jednak pamiętać, że zjawiska związane z „przestępczością komputerową” zostały opisane w Rekomendacji nr R(89)9 Komitetu Ministrów Rady Europy już w 1990 r. Wyróżniono tam dwie grupy czynów zaliczanych do tego rodzaju przestępczości. Były to: tzw. lista minimalna obejmująca takie typy przestępstw jak: oszustwo komputerowe, fałszerstwo komputerowe, włamanie do systemu komputerowego, niszczenie danych lub programów, sabotaż komputerowy, podsłuch komputerowy, piractwo komputerowe i bezprawne kopiowanie topografii półprzewodników oraz tzw. lista fakultatywna, na której znalazły się: modyfikacja danych lub programów komputerowych, szpiegostwo komputerowe, używanie komputera bez zezwolenia i używanie prawnie chronionego programu komputerowego bez upoważnienia. Zob. B. Michalski, *Przestępstwa*…, s. 219.

popełnianych z wykorzystaniem technologii informatycznych[12]. Jej celem jest zapobieganie i zwalczanie cyberprzestępczości. Konwencja wprowadza następujący podział cyberprzestępstw:

1) przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (nielegalny dostęp – art. 2, nielegalne przechwytywanie danych – art. 3, naruszenie integralności danych – art. 4, naruszenie integralności systemu – art. 5 oraz niewłaściwe użycie urządzeń – art. 6);

2) przestępstwa komputerowe (fałszerstwo komputerowe – art. 7 i oszustwo komputerowe – art. 8);

3) przestępstwa ze względu na charakter zawartych informacji (przestępstwa związane z pornografią dziecięcą – art. 9, oraz zawarte w protokole dodatkowym: rozpowszechnianie materiałów o treściach rasistowskich i ksenofobicznych przez systemy komputerowe – art. 3, groźby motywowane rasizmem lub ksenofobią – art. 5, zaprzeczanie, rewidowanie albo usprawiedliwianie ludobójstwa oraz zbrodni przeciwko ludzkości – art. 6);

4) przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Przepisy polskiego ustawodawstwa w zasadzie implementują wszystkie typy przestępstw określonych w Konwencji, zarówno w kodeksie karnym, jak i w przepisach pozakodeksowych[13].

W kodeksie karnym[14] uregulowanie znalazły następujące typy cyberprzestępstw[15]:

1) przestępstwa przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji:

---

[12] Uzasadnienie do projektu ustawy o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie, w dniu 23 listopada 2001 r., Sejm VII kadencji, druk nr 2608, s. 3.

[13] M.in. są to: ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn.: Dz. U. z 2006 r. Nr 90, poz. 631 ze zm.), ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tekst jedn.: Dz. U. z 2014 r. poz. 243 ze zm.), ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (tekst jedn. Dz. U. z 2015 r. poz. 1212 ze zm.).

[14] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 ze zm.), dalej: k.k.

[15] Typologia za: M. Siwicki, *Cyberprzestępczość*.

a) nielegalny dostęp do systemu komputerowego (*hacking*) – art. 267 § 1 i 2 k.k.,

b) naruszenie tajemnicy komunikacji – art. 267 § 3 k.k.,

c) naruszenie integralności danych komputerowych – art. 268 i 268a k.k.,

d) naruszenie integralności systemu komputerowego – art. 269 i 269a k.k.,

e) wytwarzanie, sprzedaż, oferowanie, posiadanie „narzędzi hackerskich" – art. 269b k.k.;

2) przestępstwa związane z treścią informacji:

a) przestępstwa seksualne na szkodę małoletniego – art. 200a i 202 k.k.,

b) przestępstwa przeciwko czci – art. 212 i 216 k.k.;

3) przestępstwa związane z instrumentalnym wykorzystaniem sieci i systemów teleinformatycznych:

a) przestępstwa przeciwko mieniu – art. 286, 278 § 2, art. 285 i 287 k.k.,

b) przestępstwa przeciwko wiarygodności dokumentów – np. art. 270 § 1, art. 276, 303, 310 k.k.,

c) przestępstwa przeciwko bezpieczeństwu powszechnemu – np. art. 165 § 1 pkt 4 k.k.,

d) przestępstwa przeciwko Rzeczypospolitej Polskiej – np. art. 130 § 2 i 3 k.k.,

e) przestępstwa przeciwko wolności – art. 190a k.k. (*stalking*).

O ile od strony teoretycznej poszczególne typy cyberprzestępstw zostały opisane nie tylko w komentarzach, ale i licznym piśmiennictwie[16], o tyle znacznie mniej jest badań prowadzonych nad tą problematyką[17].

[16] Przykładowo można tu wskazać: A. Adamski, *Fałszerstwo komputerowe de lege lata i de lege ferenda*, [w:] *Państwo prawa i prawo karne. Księga jubileuszowa Profesora Andrzeja Zolla*, t. 2, P. Kardas, T. Sroka, W. Wróbel (red.), Warszawa 2012; P. Janas, *Przestępstwo hackingu*, Prokuratura i Prawo 2009, nr 10; K.J. Jakubski, *Przestępczość komputerowa – zarys problematyki*,

Niniejsze opracowanie jest kolejnym o charakterze badawczym i przedstawia wyniki analizy jednego typu przestępstwa z grupy związanych z treścią informacji przetwarzanej w ramach systemów teleinformatycznych, stypizowanego w art. 287 k.k., określanego mianem oszustwa komputerowego.

Prokuratura i Prawo 1996, nr 12; J. Kędzierski, *Stalking w polskim prawie karnym – de lege lata i de lege ferenda*, Palestra 2010, nr 1–2; M. Kulik, *Przestępstwa „pornograficzne" w ujęciu porównawczym*, [w:] *Pornografia*, M. Mozgawa (red.), Warszawa 2011; J. Sadomski, *Ochrona czci (dobrego imienia) w polskim prawie cywilnym i karnym – analiza porównawcza*, [w:] *Stosowanie prawa. Księga jubileuszowa z okazji XX-lecia Instytutu Wymiaru Sprawiedliwości*, A. Siemaszko (red.), Warszawa 2011; D. Woźniakowska-Fajst, *Prawne możliwości walki ze zjawiskiem stalkingu. Analiza regulacji prawnych państw obcych oraz opinia o wprowadzeniu do polskiego porządku prawnego przepisów kryminalizujących to zjawisko*, Warszawa 2009.

[17] Zob.: B. Gruszczyńska, M. Marczewski, P. Ostaszewski, A. Siemaszko, D. Woźniakowska-Fajst, *Stalking w Polsce. Rozmiary – formy – skutki. Raport z badania nt. uporczywego nękania*, [w:] *Stosowanie prawa. Księga jubileuszowa z okazji XX-lecia Instytutu Wymiaru Sprawiedliwości*, A. Siemaszko (red.), Warszawa 2011; M. Mozgawa, P. Kozłowska, *Prawnokarne aspekty rozpowszechniania pornografii (analiza dogmatyczna i praktyka ścigania)*, Prokuratura i Prawo 2002, nr 3; M. Mozgawa, P. Kozłowska-Kalisz, *Pornografia dziecięca w świetle badań empirycznych (aspekty prawnokarne)*, [w:] *Pornografia*, M. Mozgawa (red.), Warszawa 2011; R.A. Stefański, *Oszustwa komputerowe w praktyce polskich organów ścigania*, Studia Prawnicze 2006, nr 4; F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, Warszawa 2012.

1. Kodeksowe ujęcie przestępstwa z art. 287 k.k.

1.1. Uwagi wstępne

Wprowadzenie do polskiego sytemu prawa karnego penalizacji „przestępstw komputerowych" jest następstwem konieczności wynikającej z rozwoju technologicznego oraz realizacji przez Polskę zobowiązań związanych z unifikacją systemu prawa polskiego z prawem europejskim.

Zobowiązania te zrealizowano poprzez dodanie do polskiego ustawodawstwa odpowiednich typów przestępstw, które znalazły się zarówno w kodeksie karnym, jak i ustawach pozakodeksowych, np. ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

Konwencja Rady Europy o cyberprzestępczości w art. 8 nakłada na państwa – strony zobowiązanie do „podjęcia takich środków prawnych i innych, jakie okażą się niezbędne dla uznania za przestępstwa w ich prawie wewnętrznym, umyślnego, bezprawnego spowodowania utraty majątku przez inną osobę poprzez:

1) wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych,
2) każdą ingerencję w funkcjonowanie systemu komputerowego,

z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby".

Wskazana powyżej definicja normatywna oszustwa komputerowego konstruuje typ przestępstwa materialnego, którego skutkiem działania sprawcy jest osiągnięcie korzyści majątkowych dla siebie lub innej osoby oraz spowodowanie utraty majątku przez inną osobę.

Na gruncie prawa polskiego implementację tego typu przestępstwa stanowi art. 287 k.k. określany mianem „oszustwa komputerowego".

W literaturze wskazuje się, że tym zakresie konstrukcja przepisu art. 287 k.k. nie jest w pełni zgodna z art. 8 Konwencji.

M. Siwicki określa istotę oszustwa komputerowego ujętego w Konwencji jako „ingerencję w funkcjonowanie systemu komputerowego", podczas gdy polska regulacja penalizuje jedynie „wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienianie, usuwanie albo wprowadzanie nowego zapisu danych informatycznych", co pozostawia poza zakresem normowania tego przepisu manipulacje systemami komputerowymi niezwiązane bezpośrednio z danymi informatycznymi. W konsekwencji czyny z art. 287 § 1 i 2 k.k. należy traktować raczej jako manipulację danymi informatycznymi w zakresie praw majątkowych, niż oszustwo komputerowe[18].

B. Michalski wskazuje z kolei, że opis czynu w art. 287 § 1 k.k. zawiera w zasadzie elementy definicji z art. 8 Konwencji „ma jednakże szerszy zakres, gdyż ze względu na alternatywny cel działania sprawcy („wyrządzenie innej osobie szkody") określa – obok „oszustwa komputerowego" również inny typ przestępstwa – „szkodnictwo komputerowe"[19].

Pamiętać należy, że oszustwo komputerowe pojawiło się w kodeksie karnym z 1997 r. już z chwilą jego przyjęcia i stanowiło dopełnienie penalizacji przestępstw komputerowych określonych w Rekomendacji nr R(89)9 Komitetu Ministrów Rady Europy.

Jednak wówczas przepis określający jego typ podstawowy (§ 1) różnił się od brzmienia obecnego – ustalonego na podstawie art. 1 pkt 11 ustawy z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń[20], które obowiązuje od dnia 1 maja 2004 r. Zmiana konstrukcji art. 287 k.k. wynikała z konieczności dostosowania polskiego prawa do wskazywanej wyżej Konwencji o cyberprzestępczości.

[18] M. Siwicki, *Cyberprzestępczość*, s. 258. Tak również: M. Gałązka, [w:] *Kodeks karny. Komentarz*, A. Grześkowiak, K. Wiak (red.), Warszawa 2012, s. 1210. Zob. też M. Janowski, *Przestępstwo tzw. oszustwa komputerowego*, Prokuratura i Prawo 2011, nr 10, s. 52–63.

[19] B. Michalski, [w:] *Kodeks karny. Część szczególna*, t. 2: *Komentarz do artykułów 222–316*, A. Wąsek, R. Zawłocki (red.), Warszawa 2010, s. 1173. Podobnie: S. Łagodziński, *Przestępstwa przeciwko mieniu w kodeksie karnym (wybrane zagadnienia)*, Prokuratura i Prawo 1999, nr 2, s. 7–18.

[20] Dz. U. Nr 69, poz. 626.

Wprowadzone w opisie czynu zmiany polegały na zastąpieniu zawartych w pierwotnym brzmieniu tego przepisu[21] słów „przesyłanie informacji" zwrotem „przekazywanie danych informatycznych" oraz zwrotu „nowy zapis na komputerowym nośniku informacji" określeniem „nowy zapis danych informatycznych". Zmiana odnosząca się do przedmiotu bezpośredniego oddziaływania wiązała się także z modyfikacją ustawowej definicji dokumentu opisanej w art. 115 § 14 k.k., w której w miejsce „komputerowego nośnika informacji" wprowadzono „inny zapisany nośnik informacji".

Kontrowersje budzi posługiwanie się w odniesieniu do analizowanego typu przestępstwa określeniem „oszustwo komputerowe". Różni się ono bowiem od klasycznego oszustwa z art. 286 § 1 k.k. dwoma elementami:

- nie posługuje się typowym dla oszustwa znamieniem wprowadzenia w błąd albo wyzyskania czyjegoś błędu przez sprawcę czynu w celu doprowadzenia osoby do niekorzystnego rozporządzenia własnym lub cudzym mieniem;

- nie wymaga również dla dokonania przestępstwa skutku w sferze mienia w postaci niekorzystnego rozporządzenia mieniem lub uzyskania przez sprawcę lub inną osobę jakiegokolwiek przysporzenia majątkowego lub pogorszenia sytuacji podmiotu, którego prawa majątkowe odzwierciedlane są przez zapisy danych informatycznych[22].

Niekonsekwencję tę zauważył również ustawodawca, podkreślając jednak, że mimo niespełnienia przez sprawcę znamion klasycznego oszustwa, to jednak osiąga on nienależną korzyść majątkową, a tym samym wprowadzenie odrębnego typu przestępstwa oszustwa komputerowego jest niezbędne[23]. Zresztą tym określeniem

[21] Art. 287 § 1 k.k. w pierwotnej wersji brzmiał następująco: „Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5."

[22] M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks karny. Część szczególna*, t. 3: *Komentarz do art. 278–363 k.k.*, A. Zoll (red.), Warszawa 2008, s. 317.

[23] W *Uzasadnieniu rządowego projektu nowego kodeksu karnego*, [w:] *Nowe kodeksy karne z 1997 r. z uzasadnieniami,* Warszawa 1997*,* s. 206–207, stwierdza się „Wprowadzenie oszustwa komputerowego jest niezbędne, gdyż tradycyjne pojęcie oszustwa zawiera znamiona (wprowadza w błąd <<inną osobę>>, wyzyskuje jej błąd lub <<niezdolność do należytego pojmowania

posługuje się § 3 art. 287 k.k., określając typ podstawowy przestępstwa przewidziany w § 1 – oszustwem.

W efekcie – jak piszą M. Dąbrowska-Kardas i P. Kardas – „konstrukcja przestępstwa przewidzianego w art. 287 (…) sprawia, że wypadki, w których sprawca wykorzystuje automatyczne procesy przetwarzania, gromadzenia lub przekazywania danych informatycznych lub wykorzystuje dokonane przez siebie zmiany zapisów danych informatycznych, ich usunięcie lub wprowadzenie nowego zapisu, po to, by wprowadzić w błąd inną osobę i doprowadzić w ten sposób do niekorzystnego rozporządzenia mieniem, nie stanowią realizacji znamion przestępstwa określonego w art. 287 § 1, lecz wypełniają znamiona oszustwa przewidzianego w art. 286 § 1, dokonanego, jeżeli dojdzie do niekorzystnego rozporządzenia mieniem, lub usiłowanego, jeżeli do rozporządzenia mieniem nie dojdzie”[24].

1.2. Przedmiot ochrony

Co do głównego przedmiotu ochrony art. 287 k.k. należy przyjąć, że jest nim mienie. Wynika to z faktu, że przepis ten umieszczony został przez ustawodawcę w Rozdziale XXXV k.k. obejmującym przestępstwa przeciwko mieniu.

Należy uznać, że pojęcie „mienia” powinno być rozumiane w szerokim znaczeniu obejmującym każdego rodzaju mienie, o którym mowa w art. 55 kodeksu cywilnego[25], również takie, którego istnienie nie jest potwierdzone odpowiednim zapisem w postaci danych informatycznych.

Zgodzić się należy z poglądem M. Kulika, że działanie sprawcy w odniesieniu do określonych danych informatycznych może spowodować szkodę dalej idącą, obejmującą również utratę korzyści, gdy dokonanie zmian w zapisie czy wpływanie na automatyczne przetwarzanie danych informatycznych spowoduje po stronie

przedsiębranego działania>>, doprowadza ją do niekorzystnego rozporządzenia mieniem), które przy komputerowym oszustwie nie są spełniane, choć nienależna korzyść majątkowa jest osiągana”.

[24] M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 317. Zob. też: R. Korczyński, R. Koszut, *„Oszustwo” komputerowe*, Prokuratura i Prawo 2002, nr 2, s. 17.

[25] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn.: Dz. U. z 2014 r. poz. 121 ze zm.).

pokrzywdzonego konieczność poniesienia przez niego dodatkowych wydatków, które pokryje z mienia innego niż to, którego istnienie jest potwierdzone zapisem[26].

Pobocznym przedmiotem ochrony jest integralność, poufność i dostępność informacji związanych z mieniem. Ochronie podlegają te informacje (treść) i ich zapisy związane z mieniem, które podlegają automatycznemu gromadzeniu, przetwarzaniu i przesyłaniu. W przypadku braku związku takich zapisów z prawami majątkowymi, same zapisy informacji zamieszczone na odpowiednim nośniku podlegać będą ochronie na podstawie art. 268 k.k.[27].

1.3. Podmiot czynu zabronionego

Przestępstwo określone w art. 287 § 1 k.k. ma charakter powszechny. Może zatem zostać popełnione przez każdy podmiot zdolny do ponoszenia odpowiedzialności karnej.

Należy odrzucić pogląd wskazujący na indywidualny charakter tego przestępstwa, na co miałoby wskazywać określenie „bez upoważnienia" użyte w tym przepisie[28], gdyż nie odnosi się ono do charakterystyki podmiotu, a do znamion strony przedmiotowej czynu zabronionego[29].

M. Kulik dopuszcza jednak indywidualny charakter przestępstwa z art. 287 § 1 k.k. w wypadku popełnienia go przez zaniechanie przez tego, kto z mocy ustawy, umowy dopuścił do tego, aby kto inny wpłynął na dane informatyczne lub na ich przetwarzanie[30].

---

[26] Zob. M. Kulik, [w:] *System prawa karnego,* t. 9: *Przestępstwa przeciwko mieniu i gospodarcze.*, R. Zawłocki (red.), Warszawa 2011, s. 329. Odmiennie: M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 320.

[27] Zob. M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 321; R. Korczyński, R. Koszut, *„Oszustwo"...*, s. 20.

[28] E. Czarny-Drożdżejko, *Ochrona informacji i programów komputerowych w nowym kodeksie karnym*, [w:] *Prawo autorskie a postęp techniczny*, J. Barta, R. Markiewicz (red.), Kraków 1999, s. 206.

[29] Zob. M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 322; M. Kulik, [w:] *System*..., t. 9, s. 330.

[30] M. Kulik, [w:] *System*..., t. 9, s. 330. Jak zauważa dalej M. Kulik: „W takim wypadku, w zależności od układu sytuacyjnego w konkretnej sprawie, wystąpi on w charakterze współsprawcy lub pomocnika. (…). Należy przyjąć, że w wypadku, kiedy zaniechanie *intraneusa* będzie w przebiegu całego zdarzenia na tyle istotne, że bezeń wątpliwe będzie jego powodzenie w ogóle, uznamy go za

1.4. Strona przedmiotowa

Przedmiotem czynności wykonawczej są dane informatyczne oraz urządzenie lub nośnik informacji, wykorzystywany do zapisu, przetwarzania, przechowywania lub przesyłania danych.

Pojęcie „danych informatycznych" należy rozumieć zgodnie z art. 1 lit. b Konwencji o cyberprzestępczości jako „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny."

Przepis art. 287 § 1 k.k. przewiduje sześć możliwych rodzajów czynności sprawczej, wyliczonych enumeratywnie, które mogą przybrać postać zarówno fizycznej ingerencji, jak i destrukcji logicznej[31]:

1) wpływanie na automatyczne przetwarzanie danych informatycznych,

2) wpływanie na automatyczne gromadzenie danych informatycznych,

3) wpływanie na automatyczne przekazywanie danych informatycznych,

4) zmienianie zapisów danych informatycznych,

5) usuwanie zapisów danych informatycznych,

6) wprowadzanie nowych danych informatycznych[32].

Każde z powyższych rodzajów czynności sprawczej wyczerpuje ustawowe znamiona tego czynu zabronionego, jeżeli zostało podjęte „bez upoważnienia".

---

współsprawcę omawianego czynu zabronionego, który będzie miał charakter przestępstwa indywidualnego. Jeżeli natomiast rola jego nie była istotna, jednak ułatwił on działającemu sprawcy popełnienie czynu zabronionego, jego zaniechanie będzie stanowiło pomocnictwo" (M. Kulik, [w:] *System*..., t. 9, s. 330).

[31] Zob. R. Korczyński, R. Koszut, *„Oszustwo"...*, s. 17.

[32] Tak: M. Siwicki, *Cyberprzestępczość*, s. 253; M. Kulik, [w:] *System*..., t. 9, s. 331, M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 323. Część autorów wskazuje, że art. 287 k.k. przewiduje dwie grupy czynności sprawczych: 1) wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych (informacji); 2) zmianę, usunięcie albo wprowadzenie nowego zapisu danych informatycznych. Zob. B. Michalski, [w:] *Kodeks...*, s. 1175; M. Gałązka, [w:] *Kodeks...*, s. 1210; E. Pływaczewski, [w:] *Kodeks karny. Komentarz*, O. Górniok (red.), Warszawa 2006, s. 841.

Znamię „bez upoważnienia” należy rozumieć jako czynność polegającą na wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub czynność polegającą na zmienianiu, usuwaniu albo wprowadzaniu nowego zapisu danych informatycznych, zarówno bez wiedzy i zgody podmiotu posiadającego prawo do jej wykonywania, jak też wbrew woli tego podmiotu.

„Wpływanie” na automatyczne przetwarzanie, gromadzenie, przekazywanie danych informatycznych polega na każdym zachowaniu sprawcy, które ingeruje w prawidłowość przebiegu tych procesów.

A. Adamski wskazuje, że „wpływanie” takie może polegać na:

1) manipulacji danymi wprowadzanymi do komputera (tzw. *input manipulation*),

2) manipulacji programem (tzw. *program manipulation*),

3) manipulacji wynikiem (tzw. *output manipulation*)[33].

M. Dąbrowska-Kardas i P. Kardas jako przykłady takiego zachowania podają ponadto:

1) zmianę kodowego zapisu informacji zawartej w urządzeniu służącym do automatycznego przetwarzania, gromadzenia lub przesyłania informacji, przybierającej postać zmiany sekwencji znaków kodowych, usunięciu części z nich lub dodaniu pewnych elementów, niewystępujących w pierwotnej wersji zapisu;

2) mechaniczną ingerencję w urządzenie służące do wykonywania operacji automatycznego przetwarzania, gromadzenia lub przesyłania informacji, np. uszkodzenie serwera emitującego odpowiednio zakodowane informacje, uszkodzenie linii telefonicznej;

3) podłączenie się do systemu komunikacyjnego służącego do transmisji informacji w trakcie ich ekspedycji – pomiędzy stacją wysyłającą a stacją odbierającą, np. w odniesieniu do poczty e-mail;

[33] A. Adamski, *Prawo karne...*, s. 118–121; tak również E. Pływaczewski, [w:] *Kodeks...*, s. 841.

4) wprowadzenie do systemu gromadzącego, przetwarzającego lub przekazującego dane informacji zniekształconych, fałszywych lub uszkodzonych, co będzie powodować modyfikację procesu przetwarzania, gromadzenia lub przekazywania danych informatycznych[34].

Dla odpowiedzialności sprawcy istotne jest samo ingerowanie w procesy przetwarzania danych nawet, jeżeli nie spowoduje ono zniekształcenia ich zapisu[35]. Zachowanie sprawcy polegające na wpływaniu na procesy gromadzenia, przetwarzania lub przekazywania danych może się wiązać z uprzednim przełamaniem przez niego zabezpieczeń systemu.

Przez „automatyczne przetwarzanie danych informatycznych" należy rozumieć opracowanie za pomocą maszyn cyfrowych dużych ilości danych pomiarowych w celu uzyskania określonych informacji[36].

„Gromadzenie danych informatycznych" to z kolei ich zebranie w określonym miejscu i uporządkowane według przyjętych z góry kryteriów.

„Przekazywanie danych informatycznych" to przekaz, przesył takich danych do określonego adresata zgodnie z ustalonymi procedurami.

Kolejne czynności sprawcze określone w typie podstawowym przestępstwa oszustwa komputerowego polegają na zmianie, usunięciu albo wprowadzeniu nowego zapisu danych informatycznych. Zakresy tych czynności sprawczych nakładają się na siebie, co wynika z charakteru opracowywania i korzystania z danych informatycznych. Czynności te mogą być dokonywane bezpośrednio na komputerze, na którym informacje się znajdują, lub przez włamanie się do sieci, łączącej dany komputer z innymi urządzeniami o podobnych właściwościach[37]. W przypadku

[34] M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 325–326.

[35] Zob. M. Kulik, [w:] *System*..., t. 9, s. 333.

[36] Zob. B. Michalski, [w:] *Kodeks...*, s. 1176. M. Kulik (w: *System*..., t. 9, s. 333) oraz R. Kopczyński i R. Koszut (*„Oszustwo"...*, s. 28) proponują, aby w celu interpretacji znamienia „przetwarzania danych" przyjąć definicję z art. 7 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (obecnie tekst jedn.: Dz. U. z 2015 r. poz. 2135 ze zm.), która za przetwarzanie danych osobowych przyjmuje jakiekolwiek operacje wykonywane na tych danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

[37] M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 330.

przełamania lub obejścia zabezpieczeń danych informatycznych, które ma na celu umożliwienie przeprowadzenia zmiany, usunięcia lub wprowadzenia nowego zapisu, sprawca dopuszcza się ponadto czynu z art. 267 k.k., który może być uznany za czyn współukarany uprzedni lub fragment czynu ciągłego[38].

„Zmiana w zapisie danych informatycznych" to przekształcenie treści istniejącego, prawdziwego zapisu danych, o charakterze trwałym lub czasowym, znajdującego się na nośniku informacji o jakimkolwiek charakterze (dysk twardy, USB, SSD, CD, DVD itp.)[39]. Może ona, ale nie musi, wpływać na proces automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych[40]. Zmianą w zapisie danych informatycznych będzie również ich zaszyfrowanie, a tym samym uniemożliwienie lub utrudnienie dostępu do nich osobie uprawnionej[41].

„Usunięcie danych informatycznych" polega na takiej zmianie danych informatycznych, która powoduje trwałe i nieodwracalne ich zlikwidowanie lub czasowe pozbawienie możliwości dostępu i korzystania z nich, przy istnieniu możliwości odzyskania pierwotnego zapisu.

„Wprowadzenie nowego zapisu danych informatycznych" może polegać albo na uzupełnieniu istniejących danych o nowe treści albo na wprowadzeniu danych wcześniej nieistniejących[42]. Wprowadzenie nowego zapisu danych informatycznych nie może polegać na czynnościach opisanych powyżej, tj. nie może wprowadzać zmian w istniejącej treści danych w postaci usunięcia ich części i dodania nowych, jak też nie może polegać na całkowitym usunięciu takich danych[43]. Również w tym przypadku wprowadzenie nowego zapisu może być trwałe lub czasowe.

Czyn zabroniony określony w art. 287 § 1 i 2 k.k. nie ma – występującego w przypadku „klasycznego" oszustwa z art. 286 § 1 k.k. – znamienia skutku w postaci

[38] M. Gałązka, [w:] *Kodeks*..., s. 1211.

[39] „Nośnik informacji" to środek użyty do przeniesienia informacji, a „komputerowy nośnik informacji" – element komputera lub jego oprzyrządowania, zob. B. Michalski, [w:] *Kodeks…*, s. 1178.

[40] M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 328.

[41] Tak M. Kulik, [w:] *System*..., t. 9, s. 335.

[42] Warto przypomnieć, że pierwotne brzmienie art. 287 § 1 k.k. w tej części przewidywało znamiennie „nowy zapis na komputerowym nośniku informacji". Wyeliminowanie określenia „komputerowy" pozwoliło na rozszerzenie zakresu penalizacji na wszystkie nośniki danych informatycznych.

[43] M. Kulik, [w:] *System*..., t. 9, s. 335.

niekorzystnego rozporządzenia mieniem, co jednoznacznie charakteryzowałoby go jako przestępstwo materialne. Na tym tle w literaturze występują liczne rozbieżności.

Część autorów uznaje przestępstwa z art. 287 k.k., w obu typach, za mające charakter formalny. W ten sposób widzą je R. Korczyński i R. Koszut. Autorzy ci stanowisko swoje uzasadniają tym, że „skutkowe ujęcie przestępstwa <<oszustwa>> komputerowego mogłoby prowadzić do pozostawienia poza nawiasem odpowiedzialności karnej szeregu zachowań godzących bezpośrednio w urządzenia i systemy komputerowe. Zachowanie sprawcy determinowane celem osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, a nie prowadzące do przekształceń i zmian w świecie zewnętrznym (…), pozostałoby tym samym poza zakresem penalizacji art. 287 k.k. Takiego niebezpieczeństwa nie stwarza natomiast formalne ujęcie <<oszustwa>> komputerowego, wymieniony wyżej sposób działania sprawcy zostanie bowiem objęty karalnymi znamionami <<wpływania>> na automatyczne przetwarzanie informacji” [44].

Dla części (M. Siwicki, B. Michalski) czyny zabronione z art. 287 § 1 i 2 k.k. mają charakter częściowo materialny, a częściowo formalny. „Oszustwo komputerowe jest przestępstwem formalnym w odmianie polegającej na <<wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych>>. Warunkiem dokonania oszustwa komputerowego w tej odmianie nie jest już samo tylko <<wpływanie>> na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, w odmianie natomiast polegającej na zmianie, usunięciu albo wprowadzeniu nowego zapisu danych informatycznych jest przestępstwem materialnym, którego ustawowo określonymi skutkami są wymienione w tym przepisie <<zmiana>>, <<usunięcie>> albo <<wprowadzenie nowego zapisu>>”[45].

Największa grupa autorów (A. Marek, B. Kunicka-Michalska, M. Dąbrowska-Kardas, P. Kardas, M. Kulik, M. Gałązka) opowiadają się za materialnym charakterem art. 287 k.k. „Przestępstwo [z art. 287 k.k.] (…) jest znamienne skutkiem, upatrując

[44] R. Korczyński, R. Koszut, *„Oszustwo”...*, s. 35. Tak też A. Adamski, *Prawo karne..*, s. 135; E. Pływaczewski, [w:] *Kodeks...*, s. 841; R. Góral, *Kodeks karny. Praktyczny komentarz*, Warszawa 2007, s. 497.

[45] B. Michalski, [w:] *Kodeks…,* s. 1181; M. Siwicki, *Cyberprzestępczość*, s. 252.

tego skutku nie w osiągnięciu korzyści majątkowej lub w wyrządzeniu szkody, lecz w tym, że sprawca dokonuje wpływu (wpływa) na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub dokonuje zmiany, usunięcia albo wprowadzenia nowego zapisu danych informatycznych. (…) Oszustwo komputerowe jest przestępstwem materialnym, przy takim właśnie rozumieniu skutku”[46]. Należy podzielić powyższy pogląd, jako najbliższy zamysłowi ustawodawcy tego przepisu.

W przypadku gdy sprawca podjął działania zmierzające do uzyskania określonego wpływu na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub dokonania zmiany, usunięcia albo wprowadzenia nowego zapisu danych informatycznych, lecz swojego celu nie osiągnął, może odpowiadać wyłączenie za usiłowanie przestępstwa z art. 287 § 1 k.k.[47].

1.5. Strona podmiotowa

Nie budzi wątpliwości, że przestępstwo oszustwa komputerowego ma charakter umyślny. Sprawca działa w celu osiągnięcia korzyści majątkowej (w rozumieniu art. 115 § 4 k.k.) lub wyrządzenia szkody innej osobie (rozumianej jako uszczerbek w majątku albo utracone korzyści)[48]. Zatem przestępstwo to należy do tzw. przestępstw kierunkowych. Może być ono popełnione tylko z zamiarem bezpośrednim obejmującym zarówno cel działania sprawcy, jak i sposób działania zmierzającego do realizacji tego celu[49].

---

[46] B. Kunicka-Michalska, *Oszustwo komputerowe. Regulacje prawa polskiego*, Studia Prawnicze 2006, nr 4, s. 103. Zob. też. A. Marek, *Kodeks karny. Komentarz,* Warszawa 2007, s. 585; M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 330; M. Kulik, [w:] *System*..., t. 9, s. 336; M. Gałązka, [w:] *Kodeks...*, s. 1211.

[47] M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 330.

[48] M. Kulik zwraca uwagę, że korzyść majątkowa musi mieć charakter bezprawny, nie obejmuje korzyści należącej się prawnie danemu podmiotowi. „Zatem sprawca, który dokonuje określonych manipulacji polegających na wpływaniu na automatyczne przetwarzanie, gromadzenie i przesyłanie danych informatycznych lub też sprawca zmieniający, usuwający lub wprowadzający nowy zapis danych informatycznych, lecz działający w celu osiągnięcia korzyści prawnie sobie należnej, nie odpowiada za popełnienie omawianego czynu. Należy jednak zastrzec, że będzie on odpowiadał, jeżeli jego zachowanie wyrządzi pokrzywdzonemu poważną szkodę. (…) nie uznamy za szkodę uszczuplenia w majątku pokrzywdzonego, które jest adekwatną odwrotnością należnej sprawcy korzyści” (M. Kulik, [w:] *System*..., t. 9, s. 337).

[49] M. Dąbrowska-Kardas, P. Kardas, [w:] *Kodeks...,* t. 3, s. 332.

1.6. Odmiany typu czynu zabronionego

Artykuł 287 w § 2 k.k. przewiduje typ uprzywilejowany w postaci wypadku mniejszej wagi zagrożonego karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku.

Jak zauważa B. Michalski, „w wypadku oszustwa komputerowego istotne znaczenie dla uznania tego występku za <<wypadek mniejszej wagi>> może mieć wysokość korzyści majątkowej, jaką zamierzał osiągnąć sprawca, jak również – rodzaj i rozmiary szkody, jaką czyn sprawcy mógłby wyrządzić innej osobie”[50].

Dla przestępstwa określonego w art. 287 § 1 k.k. przewidziano dwie odmiany kwalifikowane, obie zagrożone karą pozbawienia wolności od roku do lat 10:

1) gdy przedmiotem tego przestępstwa jest „mienie znacznej wartości” – art. 294 § 1 k.k.,

2) gdy czynu takiego dopuszczono się w stosunku do dobra o szczególnym znaczeniu dla kultury – art. 294 § 2 k.k.

1.7. Zagrożenie karą i środkami karnymi

Typ podstawowy oszustwa komputerowego z art. 287 § 1 k.k. zagrożony jest karą pozbawienia wolności od 3 miesięcy do lat 5.

Typ uprzywilejowany, określony w art. 287 § 2 k.k., zagrożony jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku. Dolną granicę kary ograniczenia wolności i kary pozbawienia wolności stanowi miesiąc (art. 34 § 1 i art. 37 k.k.).

Taka wysokość zagrożenia karą pozbawienia wolności powoduje, że sąd zamiast niej może orzec grzywnę albo karę ograniczenia wolności, o której mowa w art. 34 § 1a pkt 1, 2 i 4, tj. obowiązek wykonywania nieodpłatnej, kontrolowanej pracy na cele społeczne (w wymiarze od 20 do 40 godzin miesięcznie), obowiązek

[50] B. Michalski, [w:] *Kodeks…,* s. 1180.

pozostawania w miejscu stałego pobytu lub w innym wyznaczonym miejscu, z zastosowaniem systemu dozoru elektronicznego albo potrącenie od 10% do 25% wynagrodzenia za pracę w stosunku miesięcznym na cel społeczny wskazany przez sąd.

Zgodnie z art. 60 § 6 pkt 4 k.k. nadzwyczajne złagodzenie kary w obu typach tego występku polega na wymierzeniu grzywny albo kary ograniczenia wolności. Natomiast w przypadku typów kwalifikowanych z art. 294 k.k. nadzwyczajne złagodzenie kary polega na orzeczeniu grzywny, kary ograniczenia wolności albo pozbawienia wolności.

W przypadku sprawcy typu uprzywilejowanego z art. 287 k.k., jeżeli społeczna szkodliwość czynu nie jest znaczna, sąd może odstąpić od wymierzenia kary, jeżeli jednocześnie orzeka środek karny, przepadek lub środek kompensacyjny, a cele kary zostaną w ten sposób spełnione (art. 59 k.k.).

Nadzwyczajne złagodzenie kary może zostać zastosowane do sprawcy występku z art. 287 k.k. również w przypadku uwzględnienia wniosku, o którym mowa w art. 335, 338a lub 387 kodeksu postępowania karnego[51]; sąd może także odstąpić od wymierzenia kary i orzec wyłącznie środek karny, przepadek lub środek kompensacyjny (art. 60a k.k.).

Ponadto, zgodnie z treścią art. 59a § 1 k.k., w przypadku zarówno typu podstawowego, jak i uprzywilejowanego przestępstwa z art. 287 k.k., umarza się postępowanie, na wniosek pokrzywdzonego, jeżeli przed rozpoczęciem przewodu sądowego w pierwszej instancji sprawca, który nie był uprzednio skazany za przestępstwo umyślne z użyciem przemocy, pojednał się z pokrzywdzonym, w szczególności w wyniku mediacji i naprawił szkodę lub zadośćuczynił wyrządzonej krzywdzie. Jeżeli czyn został popełniony na szkodę więcej niż jednego pokrzywdzonego, warunkiem zastosowania art. 59a § 1 k.k. jest pojednanie się, naprawienie przez sprawcę szkody oraz zadośćuczynienie za wyrządzoną krzywdę w stosunku do wszystkich pokrzywdzonych (art. 59a § 2 k.k.). Przepisu art. 59a § 1 k.k. nie stosuje się, jeżeli zachodzi szczególna okoliczność uzasadniająca, że

[51] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 ze zm.), dalej jako k.p.k.

umorzenie postępowania byłoby sprzeczne z potrzebą realizacji celów kary (art. 59a § 3 k.k.).

Na podstawie art. 66 k.k. w stosunku do sprawcy oszustwa komputerowego (w obu typach określonych w art. 287 k.k.) możliwe jest zastosowanie warunkowego umorzenia postępowania.

Sąd może zastosować nadzwyczajne złagodzenie kary, a nawet odstąpić od jej wymierzenia w stosunku do sprawcy przestępstwa oszustwa komputerowego określonego w art. 287 k.k. i jego typu kwalifikowanego z art. 294 k.k., który dobrowolnie naprawił szkodę w całości, a wobec sprawcy, który dobrowolnie naprawił szkodę w znacznej części – nadzwyczajne złagodzenie kary (art. 295 k.k.).

Ze względu na to, że jednym ze znamion strony podmiotowej czynu z art. 287 k.k. jest popełnienie go w celu osiągnięcia korzyści majątkowej, w stosunku do sprawcy, któremu takie działanie zostanie przypisane, możliwe jest orzeczenie obok kary pozbawienia wolności grzywny kumulatywnej (art. 33 § 2 k.k.).

W stosunku do sprawcy możliwe jest orzeczenie środka karnego w postaci zakazu zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej, w przypadku spełnienia warunków opisanych w art. 41 § 1 k.k.

Możliwe jest ponadto – w razie odstąpienia od wymierzenia kary – orzeczenie świadczenia pieniężnego na rzecz Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej w wysokości nieprzekraczającej 60 000 zł (art. 43a § 1 k.k.).

Wobec sprawcy przestępstwa oszustwa komputerowego sąd może orzec ponadto przepadek przedmiotów, które służyły lub były przeznaczone do popełnienia przestępstwa (art. 44 § 2 k.k.) oraz przepadek korzyści majątkowej lub jej równowartości, jeżeli sprawca osiągnął z popełnienia przestępstwa, chociażby pośrednio, korzyść majątkową niepodlegającą przepadkowi przedmiotów wymienionych w art. 44 § 1 lub 6 (art. 45 § 1 k.k.).

Ponadto – na podstawie art. 46 k.k. – w razie skazania sąd może orzec, a na wniosek pokrzywdzonego lub innej osoby uprawnionej orzeka, stosując przepisy prawa cywilnego, obowiązek naprawienia, w całości albo w części, wyrządzonej

przestępstwem szkody lub zadośćuczynienia za doznaną krzywdę, a jeżeli orzeczenie obowiązku naprawienia szkody jest znacznie utrudnione, sąd może orzec zamiast tego obowiązku nawiązkę w wysokości do 200 000 zł na rzecz pokrzywdzonego, a w razie jego śmierci w wyniku popełnionego przez skazanego przestępstwa nawiązkę na rzecz osoby najbliższej, której sytuacja życiowa wskutek śmierci pokrzywdzonego uległa znacznemu pogorszeniu. W razie gdy ustalono więcej niż jedną taką osobę, nawiązki orzeka się na rzecz każdej z nich.

1.8. Zbieg przepisów ustawy

Przestępstwo z art. 287 k.k. stanowi *lex specialis* w stosunku do przepisu art. 268 k.k. (naruszenie prawa do zapoznania się z informacją), art. 268a § 1 k.k. (niszczenie, uszkadzanie, usuwanie danych informatycznych) i art. 269a k.k. (zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej), co wyklucza kumulatywny zbieg tych przepisów.

Przepis art. 287 k.k. może natomiast pozostawać w kumulatywnym zbiegu z przepisem art. 269 § 2 k.k. (dywersja informatyczna) oraz art. 279 § 1 k.k. (kradzież z włamaniem).

Jak zauważył Sąd Apelacyjny w Szczecinie w wyroku z dnia 14 października 2008 r. „pogląd, zgodnie z którym przepis art. 287 § 1 k.k. nigdy nie wystąpi samodzielnie, lecz zawsze w zbiegu z art. 279 § 1 k.k. jest poprawny jedynie wówczas, gdy wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianie, usunięciu albo wprowadzeniu nowego zapisu danych informatycznych towarzyszyć będzie wyjęcie jednostek pieniężnych z władztwa dotychczasowego posiadacza i ich włączenie do majątku sprawcy. Przestępstwo z art. 287 § 1 k.k., dokonane jest tymczasem już z chwilą wprowadzenia zmian lub innej opisanej w tym przepisie ingerencji w urządzenie lub system do gromadzenia, przetwarzania lub przesyłania informacji za pomocą techniki komputerowej. Efektywna szkoda nie należy zatem do jego znamion. Dla jego bytu obojętny jest także konieczny na gruncie art. 279 § 1 k.k. zamiar przywłaszczenia”[52].

[52] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r., II AKa 120/08, LEX nr 508308.

W sytuacji gdy sprawca wpływa na m.in. automatyczne procesy przetwarzania danych informatycznych po to, aby wprowadzić w błąd inną osobę i doprowadzić w ten sposób do niekorzystnego rozporządzenia mieniem, wypełniają znamiona oszustwa z art. 286 § 1 k.k., a nie czynu określonego w art. 287 § 1 k.k.

1.9. Tryb ścigania

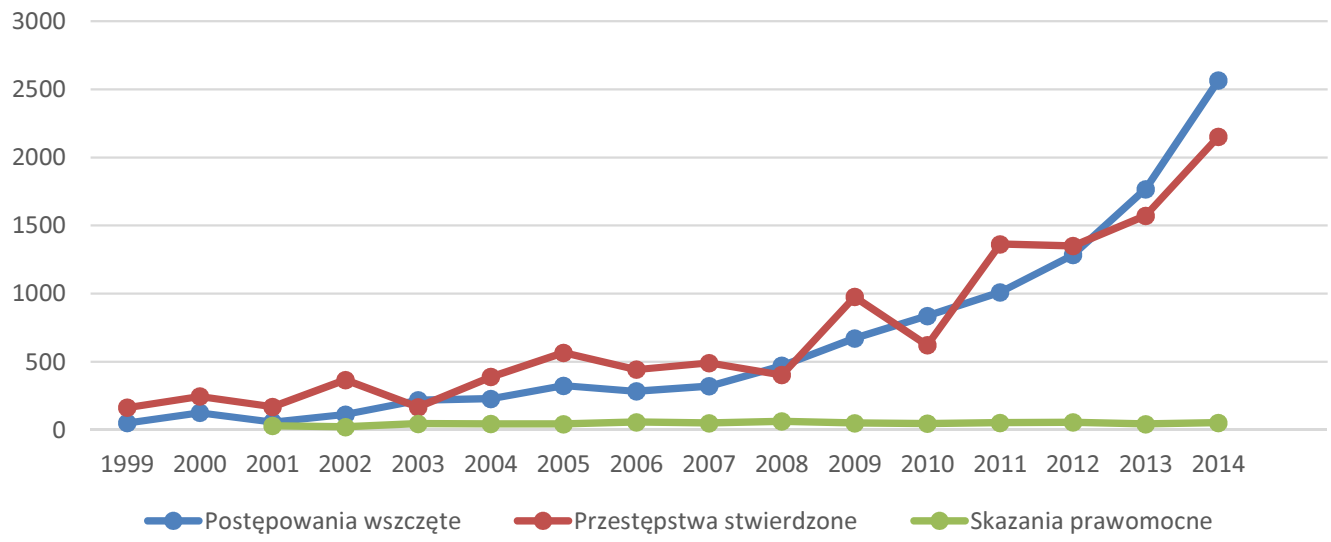
Przestępstwo z art. 287 k.k. jest przestępstwem publicznoskargowym i jest ścigane z urzędu. Jedynie w przypadku, gdy oszustwo komputerowe popełniono na szkodę osoby najbliższej, nabiera ono charakteru przestępstwa wnioskowego – ściganego na wniosek pokrzywdzonego (art. 287 § 3 k.k.).

2. Art. 287 k.k. w ujęciu statystycznym

Przestępstwo określone w art. 287 k.k. zostało wprowadzone do polskiego ustawodawstwa wraz z wejściem w życie obecnie obowiązującego kodeksu karnego z 1997 r.

Początkowe lata funkcjonowania przepisu dotyczącego oszustwa komputerowego w kodeksie karnym nie przyniosły znaczącej liczby spraw wszczynanych na podstawie tego przepisu. Powolny wzrost daje się zaobserwować od 2003 r., a w 2011 r. przekroczono liczbę 1000 postępowań wszczętych rocznie.

Wykres 1. Oszustwo komputerowe (art. 287 k.k.) – postępowania wszczęte, przestępstwa stwierdzone, skazania prawomocne w latach 1999–2014



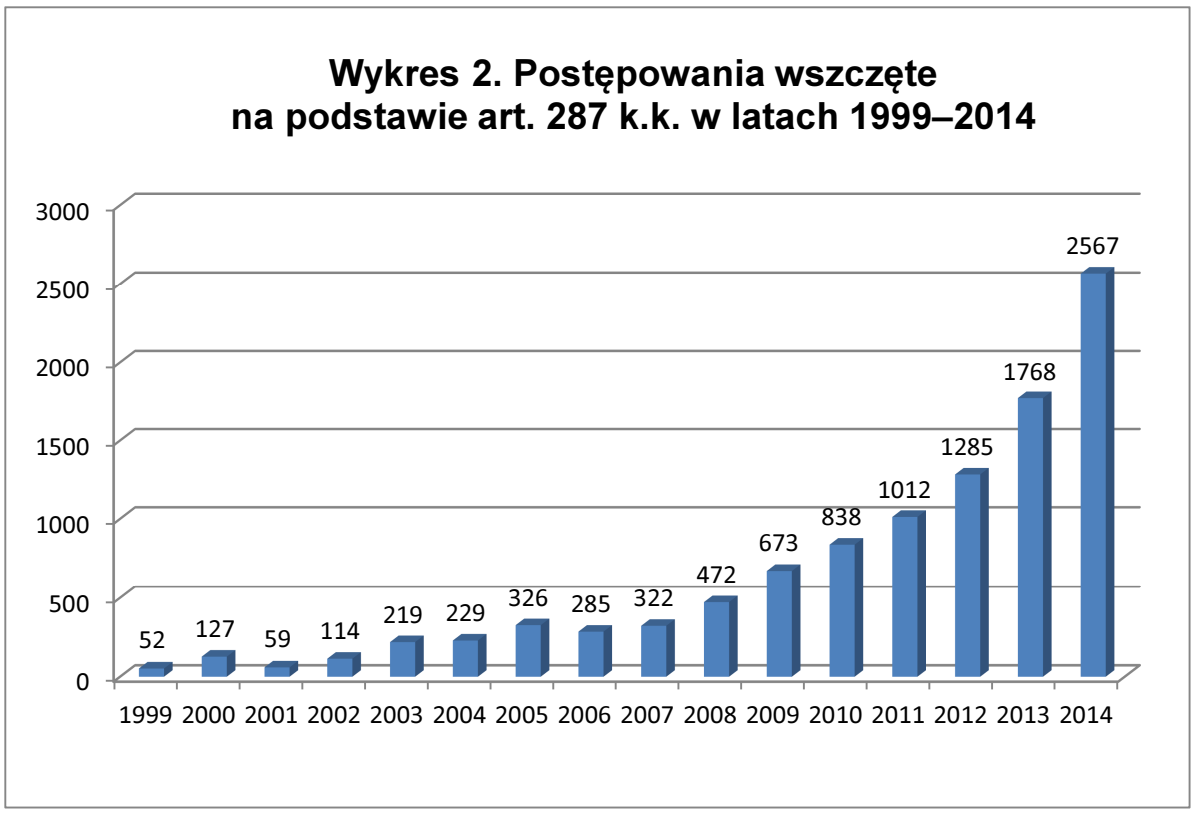
Analizę funkcjonowania w praktyce art. 287 k.k. przeprowadzono na podstawie danych statystycznych pochodzących z następujących statystyk:

1) postępowań przygotowawczych wszczętych w oparciu o wskazany wyżej artykuł w latach 1999–2014,

2) przestępstw stwierdzonych (za lata 1999–2014),

3) sądowej statystyki prawomocnych skazań publikowanej przez Wydział Statystyki Ministerstwa Sprawiedliwości za lata 1999–2014.

Od początku funkcjonowania art. 287 k.k. w ramach przepisów kodeksu karnego obserwujemy stały wzrost liczby postępowań wszczynanych w oparciu o jego postanowienia[53]. O ile w latach 1999–2007 następowały jeszcze drobne wahania dotyczące liczby postępowań, to od 2008 r. ten wzrost jest już stały i wynosi od 120% do 145% – licząc rok do roku. Gdyby porównać liczbę postępowań wszczętych w 2014 r. (2567) do liczby postępowań z 2008 r. (472), to zauważymy wzrost o ponad 543%, a w stosunku do pierwszego roku objętego analizą, tj. 1999 r. – aż o niemal 5000%. Dane szczegółowe (w liczbach bezwzględnych) z podziałem na poszczególne lata prezentuje wykres 2.



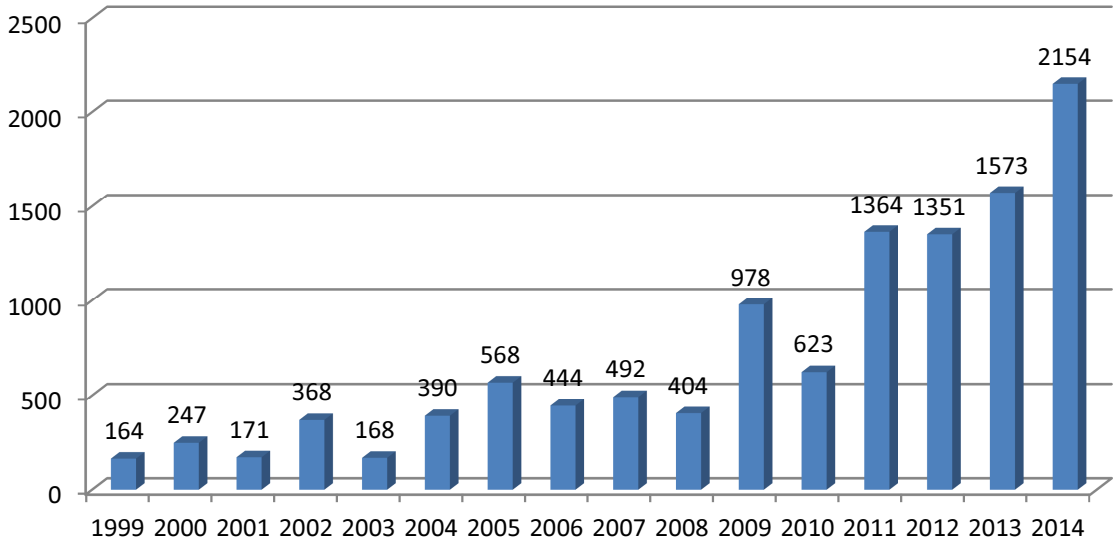
Oczywiście odnosząc te dane do ogólnej liczby postępowań wszczętych w tym samym okresie, tj. 17 379 428 postępowań w sprawach o popełnienie wszystkich przestępstw przewidzianych w polskich aktach prawnych, stwierdzimy, że postępowania z art. 287 k.k. stanowiły 0,045% wszystkich wszczętych[54].

[53] Za: http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63977,Oszustwo-komputerowe-art-287.html (dostęp dnia 17 listopada 2015 r.).

[54] Za: http://statystyka.policja.pl/st/ogolne-statystyki/47682,Postepowania-wszczete-przestepstwa-stwierdzone-i-wykrywalnosc-w-latach-1999-2014.html (dostęp dnia 17 listopada 2015 r.). Należy pamiętać o zmianie przeprowadzonej od 2013 r. w zakresie generowania danych statystycznych przez

Analiza danych za lata 1999–2014 dotycząca liczby przestępstw stwierdzonych[55] z art. 287 k.k. (wykres 3) koreluje z danymi dotyczącymi liczby postępowań wszczętych, wykazując wzrosty, choć nie tak jednoznaczne jak w przypadku wcześniej prezentowanych danych.

Wykres 3. Przestępstwa stwierdzone na podstawie art. 287 k.k. w latach 1999–2014

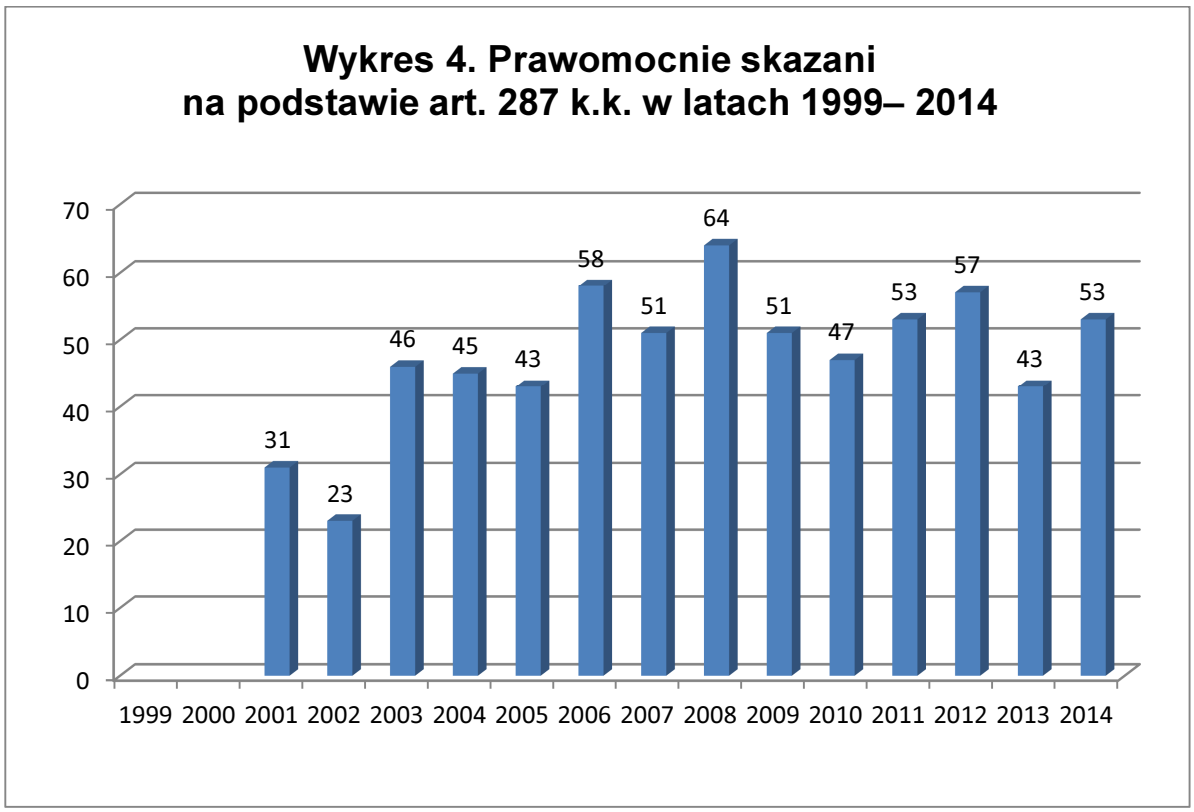


Różnice te są uzasadnione, gdyż prezentują odmienne fazy prowadzonego postępowania. Nie każde bowiem postępowanie karne zakończy się stwierdzeniem popełnienia czynu określonego w art. 287 k.k., jak również może zaistnieć sytuacja odmienna, gdy jedno postępowanie daje podstawy do stwierdzenia popełnienia przez sprawcę kilku przestępstw tego samego typu. Dobrą ilustrację stanowi tu rok 1999, w którym przy 52 postępowaniach wszczętych stwierdzono 164 przestępstwa. Tendencję odmienną pokazuje rok 2003, w którym przy 219 postępowaniach wszczętych stwierdzono jedynie 168 oszustw komputerowych.

Policję. Do końca 2012 r. prezentowane w statystyce policyjnej dane zawierały zarówno informacje o postępowaniach przygotowawczych prowadzonych przez Policję, jak również o postępowaniach prowadzonych we własnym zakresie przez prokuraturę – bez udziału Policji. Od początku 2013 r. statystyka policyjna obejmuje dane o postępowaniach przygotowawczych prowadzonych wyłącznie przez Policję. Dlatego też dane dotyczące lat 2013–2014 nie są w pełni porównywalne w stosunku do danych z lat wcześniejszych.

[55] Za: http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63977,Oszustwo-komputerowe-art-287.html (dostęp dnia 17 listopada 2015 r.).

Powyższe dane można skonfrontować ze statystyką sądową skazań prawomocnych w oparciu o art. 287 k.k.[56]. Dane obejmują lata 1999–2014 (wykres 4).



W latach 1999–2014 na podstawie wszystkich paragrafów art. 287 k.k. prawomocnie skazano 665 osób, z czego 608 na podstawie art. 287 § 1 k.k., 49 – na podstawie art. 287 § 2 k.k. Statystyka sądowa podaje również, że pozostałe 8 osób skazano na podstawie § 3 tego artykułu. Ta informacja musi budzić zdziwienie, gdyż § 3 nie przewiduje kolejnego typu przestępstwa, a jedynie wskazuje na tryb wnioskowy w przypadku, gdy oszustwo z art. 287 k.k. popełniono na szkodę osoby najbliższej.

Dane dotyczące skazań prawomocnych pokazują, jak niewielka liczba spraw o przestępstwo oszustwa komputerowego kierowana jest do sądu z aktem oskarżenia. Rocznie na podstawie art. 287 k.k. skazywanych jest tylko od 23 do 64 osób.

Tak niewielka liczba orzeczeń prawomocnych może dziwić, gdy zestawimy te liczby z danymi chociażby o przestępstwach stwierdzonych. Oczywiście liczba przestępstw

[56] Źródło: http://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/download,2853,43.html (dostęp dnia 17 listopada 2015 r.).

stwierdzonych nie będzie tożsama z liczbą skazanych, gdyż jedna osoba może być oskarżoną o kilka przestępstw. Jednak tak duża rozbieżność musi powodować powstanie pytania o jej przyczyny.

Odpowiedzi można szukać w liczbie umorzeń spraw wszczętych na podstawie art. 287 k.k. Z danych uzyskanych na potrzeby niniejszego badania ze wszystkich prokuratur w kraju wynika, że przeważająca większość spraw wszczynanych na podstawie analizowanego przepisu jest następnie umarzana. Otrzymane dane obejmują tylko okres dwóch lat: 2012–2013, jednak już tylko one pozwalają na wskazanie przyczyny tak małej liczby spraw kierowanych do sądów.

W 2012 r. umorzonych zostało 1220 postępowań na 1285 wszczętych (według danych Policji), a w 2013 r. umorzono 1435 spraw na 1768 wszczętych. Oznacza to, że aż 95% postępowań z 2012 r. i ponad 81% spraw wszczętych w 2013 r. zostało następnie umorzonych. Nie można oczywiście wykluczyć, że liczba ta jest wyższa, gdyż część postępowań mogła zostać umorzona w roku kolejnym, a zatem nie została objęta danymi przekazanymi przez prokuratury.

Warto ponadto odnotować, że skazania na podstawie art. 287 k.k. w ogólnej liczbie skazań prawomocnych w skali roku nie przedstawiają istotnego znaczenia. Przykładowo w 2014 r. skazano prawomocnie 295 353 osoby, w tym 53 na podstawie art. 287 k.k. Skazania na podstawie analizowanego artykułu stanowiły tym samym w 2014 r. jedynie 0,02% ogółu skazań.

3. Wyniki badań aktowych

3.1. Założenia badania

Badania przeprowadzono w oparciu o akta spraw z art. 287 k.k. zakończonych w 2013 r. odmową lub umorzeniem postępowania oraz postępowań, w których w tym samym roku zapadło prawomocne orzeczenie sądowe.

Zapytanie o dane dotyczące liczby postępowań zakończonych na etapie postępowania przygotowawczego przesłane zostało do wszystkich jednostek prokuratury, za pośrednictwem prokuratur okręgowych.

W odpowiedzi z 304 prokuratur rejonowych uzyskano informację o 1435 postępowaniach, w których wydano postanowienie o odmowie lub umorzeniu postępowania.

Na zapytanie o dane dotyczące liczby spraw, w których w 2013 r. zapadło orzeczenie prawomocne wydane na podstawie art. 287 k.k., w odpowiedzi uzyskano informację o 41 takich sprawach rozpoznanych w 28 sądach rejonowych i 6 sądach okręgowych.

Do analizy została wylosowana 10% reprezentatywna próba losowa akt postępowań zakończonych na etapie postępowania sprawdzającego lub przygotowawczego w 2013 r. (144 sprawy). W odniesieniu do akt spraw ukończonych prawomocnym orzeczeniem sądowym w badanym okresie (41 spraw) podjęto decyzję o analizie wszystkich postępowań.

Po wstępnej ocenie nadesłanych akt, do badania ostatecznie zakwalifikowano 140 postępowań przygotowawczych, w tym sześć zakończonych wydaniem postanowienia o odmowie wszczęcia postępowania i 40 spraw sądowych. W pięciu przypadkach (cztery dotyczyły postępowań przygotowawczych i jedno – postępowania sądowego) przesłane akta nie dotyczyły analizowanego czynu, dlatego nie zostały uwzględnione w przeprowadzonym badaniu.

3.2. Sprawy zakończone na etapie postępowania przygotowawczego

3.2.1. Zawiadomienie o przestępstwie

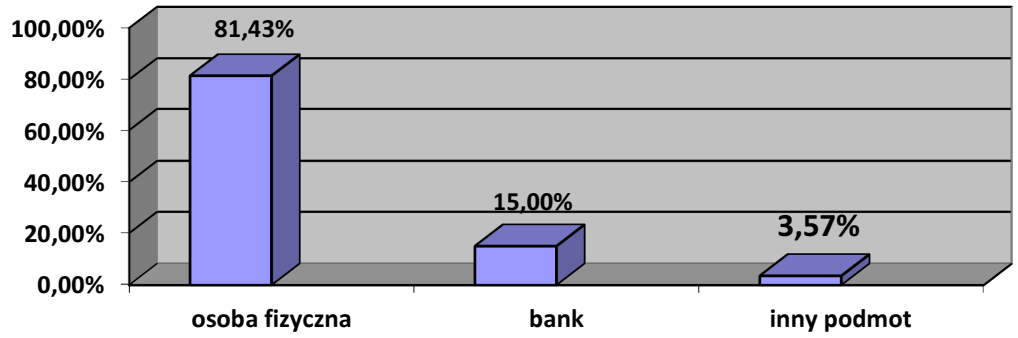
Zachowanie sprawcy przestępstwa z art. 287 § 1 k.k. polega na działaniu ukierunkowanym na osiągnięcie przez niego korzyści majątkowej lub wyrządzenie innej osobie szkody, poprzez zrealizowanie jednego ze znamion strony przedmiotowej tego czynu.

Z punktu widzenia sprawcy, którego zachowanie przestępcze ma polegać na wpłynięciu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianie, usunięciu albo wprowadzeniu nowego zapisu danych informatycznych, bez posiadania przez niego upoważnienia, najłatwiejsze do realizacji tych znamion będą dane informatyczne należące do osób fizycznych. Wynika to z tego, że przy ogromnej liczbie użytkowników sieci internetowej i dostępnych w nich serwisów, a także świadczonych usług lub masowego korzystania z innego rodzaju przedmiotów wykonawczych (urządzeń będących częścią systemu informatycznego funkcjonującego automatycznie lub nośników, na których są zapisane dane informatyczne) to dane osób fizycznych będą dla sprawcy najbardziej „dostępne", bo często są to dane niewłaściwie lub niewystarczająco przez ich dysponentów chronione.

Nie budzi zatem zdziwienia, że ponad 81% składających zawiadomienie o popełnieniu na ich szkodę przestępstwa z art. 287 k.k. to osoby fizyczne, które – w większości przypadków – stwierdziły nieautoryzowany dostęp do ich danych osobowych zamieszczonych w różnego rodzaju serwisach internetowych lub też ujawniły nieautoryzowane przez nie transakcje przeprowadzone za pomocą wykorzystywanych przez nie elektronicznych instrumentów płatniczych, instytucji pieniądza elektronicznego lub karty płatniczej[57].

[57] Definicje tych pojęć zawierała ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (tj. Dz. U. z 2012 r. poz. 1232), która została uchylona z dniem 7 października 2013 r. na mocy ustawy z dnia 12 lipca 2013 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. z 2013 r., poz. 1036) Zgodnie z tą ustawą: elektroniczny instrument płatniczy to każdy instrument płatniczy, w tym z dostępem do środków pieniężnych na odległość, umożliwiający posiadaczowi dokonywanie operacji przy użyciu informatycznych nośników danych lub elektroniczną identyfikację posiadacza niezbędną do dokonania operacji, w szczególności kartę płatniczą lub

Wykres 5. Podmiot zawiadamiający o przestępstwie (w procentach)



Kolejnym źródłem zawiadomienia o podejrzeniu popełnienia przestępstwa oszustwa komputerowego (15% przypadków) były banki, które w ramach prowadzonej przez siebie działalności są wystawcami lub akceptantami dla transakcji dokonywanych za pomocą wystawianych przez te podmioty kart płatniczych, kart kredytowych lub kart debetowych[58]. W tych przypadkach, w których bank uznaje reklamację złożoną przez swojego klienta – posiadacza wydanej przez bank karty, staje się pokrzywdzonym czynem z art. 287 k.k.

Zawiadomienia w sprawach objętych badaniem wpłynęły od czterech banków, w tym ponad 76% zawiadomień pochodziło od banku PKO BP S.A.

instrument pieniądza elektronicznego; instrument pieniądza elektronicznego to urządzenie elektroniczne, na którym jest przechowywany pieniądz elektroniczny, w szczególności kartę elektroniczną zasilaną do określonej wartości; karta płatnicza to karta identyfikująca wydawcę i upoważnionego posiadacza, uprawniająca do wypłaty gotówki lub dokonywania zapłaty, a w przypadku karty wydanej przez bank lub instytucję ustawowo upoważnioną do udzielania kredytu – także do dokonywania wypłaty gotówki lub zapłaty z wykorzystaniem kredytu.

[58] Regulację w zakresie świadczenia usług płatniczych zwiera ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (tekst jedn.: Dz. U. z 2014 r. poz. 873 ze zm.), która definiuje na swoje potrzeby różnego rodzaju karty wydawane przez instytucje płatnicze w następujący sposób: karta płatnicza – karta uprawniająca do wypłaty gotówki lub umożliwiająca złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego, akceptowana przez akceptanta w celu otrzymania przez niego należnych mu środków; karta debetowa – karta płatnicza umożliwiającą wykonywanie transakcji płatniczych, z wyjątkiem transakcji w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego – kredytu, o którym mowa w art. 74 ust. 3 lub art. 132j ust. 3 tej ustawy; karta kredytowa – karta płatnicza umożliwiającą wykonywanie transakcji płatniczych w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego – kredytu, o którym mowa w art. 74 ust. 3 lub art. 132j ust. 3 tej ustawy.

Ostatnią, niewielką (pięć przypadków) grupę zawiadamiających stanowią pozostałe podmioty, niemieszczące się w pozostałych dwóch grupach, które bądź uzyskały wiedzę o możliwości zaistnienia popełnienia przestępstwa oszustwa komputerowego w ramach prowadzonych przez nie czynności (Policja), jak również – w ich ocenie – stały się pokrzywdzonymi działaniem sprawcy (urząd miasta, zarząd transportu miejskiego, stowarzyszenie, osoba fizyczna prowadząca działalność gospodarczą).

3.2.2. Ujawnione mechanizmy przestępcze – przedmiot przestępstwa, strona przedmiotowa

Analiza postępowań karnych w sprawach o oszustwo komputerowe pozwoliła na wyodrębnienie kilku podstawowych mechanizmów przestępczego działania wykorzystywanych przez sprawców w celu popełnienia tego przestępstwa.

Scharakteryzować je można w następujący sposób:

1) przygotowanie przez sprawcę fałszywej strony internetowej banku, która posłużyła mu do osiągnięcia nienależnej korzyści majątkowej na szkodę posiadacza rachunku bankowego.

W tym celu wykorzystano podrobioną stroną internetową banku, a na adres osoby pokrzywdzonej przesłano wiadomość z informacją o konieczności zalogowania się na konto. Po kliknięciu w link załączony do wiadomości otwierała się fałszywa strona internetowa banku, wyglądająca jak prawdziwa. Pokrzywdzona otrzymała następnie informację, aby podała kolejny kod z karty zdrapka, co też uczyniła. To umożliwiło sprawcy wypłatę wszystkich środków z rachunku bankowego.

Wskazać należy, że nastąpiło tutaj dobrowolne przekazanie żądanych informacji przez posiadacza rachunku bankowego, a tym samym utrudniło to wykrycie sprawcy.

Transakcja przy użyciu prawidłowego kodu nie będzie mogła również zostać uznana przez bank w drodze reklamacji, gdyż z punktu widzenia banku została autoryzowana prawidłowo.

Tak więc, wobec niemożności ustalenia sprawcy, wyłącznym pokrzywdzonym jest posiadacz rachunku, którego nie zastanowiło nietypowe żądanie ze strony banku, niestosowane w dotychczasowych z nim kontaktach.

2) pozyskanie przez sprawcę danych o numerze karty, posiadaczu i numerze PIN, niezbędnych do dokonywania transakcji w sklepach internetowych lub wypłaty środków pieniężnych z bankomatu.

Wśród analizowanych postępowań była to najczęstsza metoda popełnienia przestępstwa z art. 287 k.k., występująca w prawie 53% przypadków.

Metoda ta może podlegać różnego rodzaju modyfikacjom, a sprowadza się do wejścia przez sprawcę w posiadanie danych karty płatniczej i wykorzystaniu ich w celu wypłaty gotówki lub dokonania zakupów w sklepach internetowych, zwykle poza granicami kraju, w którym karta została wydana. W ten sposób dochodzi do nieuprawnionego przetworzenia i zmiany danych informatycznych powodujących obciążenie rachunku pokrzywdzonego.

Uzyskanie danych karty może nastąpić w drodze przełamania przez sprawcę zabezpieczeń rachunku karty lub też w drodze tzw. skimmingu danych karty dokonanych w trakcie codziennego jej używania przez jej posiadacza.

Odmianą tej metody jest przełamanie zabezpieczeń rachunku bankowego pokrzywdzonego i wykorzystanie go do opisanych wyżej celów przestępczych.

3) nieuprawnione uzyskanie dostępu do konta użytkownika na portalu aukcyjnym, zmiana danych dotyczących aukcji internetowych i uzyskanie korzyści majątkowej z tytułu przeprowadzenia fikcyjnej aukcji.

Wśród analizowanych postępowań była to druga najczęściej wykorzystywana metoda popełnienia przestępstwa z art. 287 k.k., występująca w ponad 31% przypadków.

Typowy *modus operandi* sprowadzał się do tego, że nieznany sprawca w nieustalony sposób uzyskał dostęp do konta internetowego osoby pokrzywdzonej na portalu aukcyjnym, a następnie w celu osiągnięcia korzyści majątkowej na tym koncie

wprowadził nowy zapis dotyczący aukcji internetowych, wystawiając na niej fikcyjny przedmiot, w wyniku czego uzyskał on nienależną korzyść majątkową.

Sprawcy wykorzystują w tym przypadku zasadę działania portalu aukcyjnego pozwalającą na wysyłkę sprzedanego towaru dopiero po otrzymaniu od zwycięzcy aukcji wylicytowanej kwoty.

Pokrzywdzony najczęściej dowiaduje się o popełnionym na jego szkodę przestępstwie dopiero w chwili, gdy nabywca wystawionego towaru zwraca się do niego o realizację wysyłki lub jest zniecierpliwiony przedłużającym się okresem oczekiwania na towar.

W bardziej skomplikowanych stanach faktycznych w celu popełnienia przestępstwa sprawcy wykorzystują telefony komórkowe pre-paid, logują się do Internetu z komputerów wykorzystujących oprogramowanie maskujące, konta bankowe zakładają za pośrednictwem Internetu i nienależne wypłaty realizowane są przy użyciu kart bankomatowych.

4) wprowadzenie w celu osiągnięcia korzyści majątkowej, bez upoważnienia, nowego zapisu danych informatycznych w postaci złośliwego oprogramowania komputerowego blokującego działanie komputera należącego do pokrzywdzonego.

Metoda ta wykorzystywana jest w przypadku korzystania przez pokrzywdzonego ze stron internetowych. Świadoma (dokonana przez pokrzywdzonego) lub nieświadoma (np. już w wyniku samego wejścia na stronę internetową) instalacja oprogramowania zawierającego program blokujący komputer skutkuje skierowaniem do takiego pokrzywdzonego żądania zapłaty określonej kwoty za możliwość odblokowania komputera. W ostatnich latach metoda ta była wykorzystywana przez przestępców w stosunku do użytkowników internetowych stron pornograficznych, w tym również w ramach analizowanych spraw.

5) posłużenie się w formie elektronicznej za pośrednictwem Internetu danymi osobowymi pokrzywdzonego w firmie oferującej tzw. szybkie pożyczki, gdzie nieznany sprawca, w celu osiągnięcia korzyści majątkowej, w jego imieniu zawarł umowę pożyczki na szkodę pokrzywdzonego.

Metoda ta wykorzystuje fakt, że prawdziwość podawanych danych osobowych nie jest w stopniu wystarczającym przez takie firmy sprawdzana, a tym samym umożliwia „podszycie się” przez sprawcę pod osobę pokrzywdzonego.

Odmianą tej metody jest posłużenie się danymi pokrzywdzonego i zamówienie na jego koszt usług (np. dostępu do Internetu).

6) zmiana lub wprowadzenie nowego zapisu danych informatycznych na koncie użytkownika gry internetowej i sprzedaż lub przejęcie przez sprawcę posiadanych przez pokrzywdzonego postaci lub ich wyposażenia.

Jest to odpowiedź sprawców oszustwa komputerowego na stosunkowo nowe zjawisko, jakim są sieciowe gry internetowe. W przypadku takich gier ich uczestnik współdziała z innymi graczami, tocząc wspólną rozgrywkę. W zależności od rodzaju gry może ona być prowadzona latami. Gracz zdobywa postaci, nabywa doświadczenie, wyposaża je w określone moce, artefakty itp. Czas poświęcony na „wyszkolenie” takich postaci, czy zbudowanie określonego wirtualnego świata w grze jest często na tyle duży, że może on dla graczy być przeliczalny na realne pieniądze. W wyniku tego na portalach aukcyjnych dokonywane są transakcje zdobytymi przez graczy przedmiotami, które jednak nie stanowią oddzielnego programu komputerowego, a są niesamodzielnymi elementami programu gry – są bytem niematerialnym będącym zapisem danych informatycznych, posiadającym wymierną wartość. Nabycie takich przedmiotów umożliwia graczowi przeskoczenie pewnych poziomów gry i stanie się od razu uczestnikiem gry na poziomie zaawansowanym.

Wejście przez sprawcę czynu z art. 287 k.k. w posiadanie takich przedmiotów powoduje realną szkodę po stronie gracza, wymierną w kwocie, jaką mógłby on uzyskać, gdyby samodzielnie dokonał ich sprzedaży.

Należy podkreślić, że w tego typu rozgrywkach gracze mogą ze sobą współpracować, wymieniając się posiadanym przez siebie wyposażeniem. W takim przypadku dobrowolne przekazanie np. części uzbrojenia postaci i odmowa zwrotu, a nawet jej sprzedaż, nie będzie stanowiła przestępstwa. Podobnie, jeżeli w wyniku pomyłki gracza przekaże on dobrowolnie część wyposażenia niewłaściwej osobie, która następnie je sprzeda. W wyniku takiego przekazania nastąpi co prawda przysporzenie po stronie osoby otrzymującej wyposażenie (a zatem dojdzie też do

zmiany zapisu danych informatycznych), ale nie dojdzie do realizacji znamienia działania „bez upoważnienia”, gdyż w takim przypadku osoba ta weszła w posiadanie wyposażenia w sposób prawny i jako nowy właściciel może nim swobodnie rozporządzać.

Dlatego też po stronie użytkowników tego typu gier leży zachowanie szczególnej ostrożności przy rozporządzaniu posiadanych przez nich elementów związanych z postacią, którą grają.

7) wpływanie bez uprawnień na automatyczne przetwarzanie danych informatycznych przez nieustalonego sprawcę, który w celu osiągnięcia korzyści majątkowej przełamał elektroniczne zabezpieczenie skrytki pocztowej będącej własnością pokrzywdzonego prowadzącego działalność gospodarczą, po czym rozesłanie do jego kontrahentów fałszywej informacji o zmianie numeru rachunku bankowego do wpłat za zamówione towary.

Tego typu działanie sprawcy może być szczególnie groźne w przypadku realizacji w krótkim terminie wielu przelewów na znaczne kwoty, gdyż – niezależnie od szkody po stronie pokrzywdzonego – może zagrozić płynności finansowej firmy, a nawet spowodować jej niewypłacalność.

Ten sam sposób działania sprawców może dotyczyć rachunków osób fizycznych nieprowadzących działalności gospodarczej.

8) przełamanie zabezpieczeń routera teleinformatycznego obsługującego połączenia VoIP (*voice over IP* – telefonia za pośrednictwem Internetu) i wykonanie za jego pośrednictwem szeregu rozmów telefonicznych do różnych państw, a tym samym spowodowanie szkody po stronie pokrzywdzonego.

Pokrzywdzony przestępstwem, o ile jego sieć komputerowa nie jest nadzorowana przez informatyków, może się dowiedzieć o fakcie włamania na router dopiero w chwili otrzymania rachunku za usługi telefoniczne. Wykonanie przez sprawcę szeregu połączeń, szczególnie na numery krajów „egzotycznych”, leżących na innych kontynentach, może spowodować, że szkoda będzie niezwykle wysoka.

Wydaje się, że pewnym sposobem przeciwdziałania temu może być ustalenie limitu, do którego połączenia będą mogły być wykonywane.

3.2.3. Wysokość szkód popełnionych przestępstwem

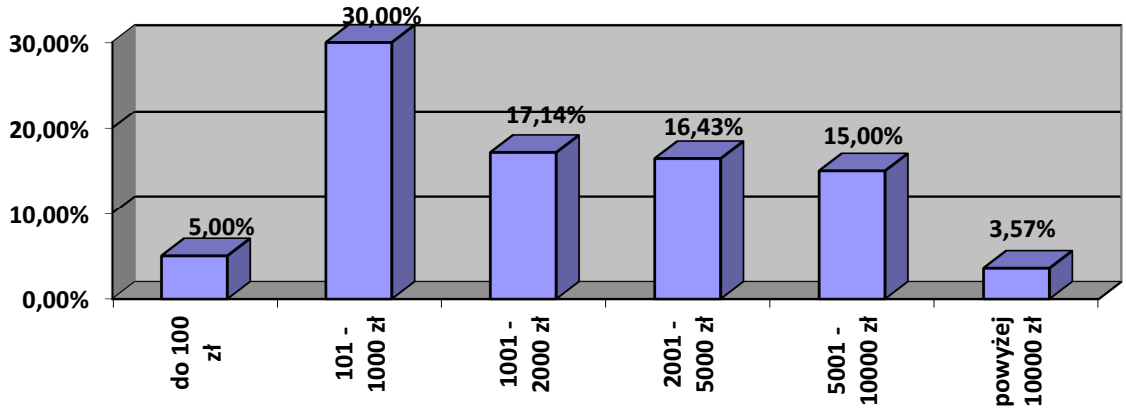
Zachowanie przestępcze sprawcy czynu z art. 287 k.k. polega na działaniu w celu osiągnięcia korzyści majątkowej lub wyrządzenia szkody innej osobie.

Korzyścią majątkową jest korzyść zarówno dla siebie, jak i dla kogo innego (art. 115 § 4 k.k.) i jest nią każde zwiększenie aktywów lub zmniejszenie pasywów. Natomiast szkodą będą wszelkie uszczerbki w dobrach lub interesach prawnie chronionych, których poszkodowany doznał wbrew swojej woli. W odniesieniu do analizowanego przestępstwa należy przyjąć, że będzie chodzić tylko o szkodę majątkową, która może się wyrazić w stracie rzeczywistej (*damnum emergens*) lub utraconych korzyściach (*lucrum cessans*).

Zgodnie z konstrukcją strony podmiotowej, dla zrealizowania znamion czynu zabronionego z art. 287 k.k. ani szkoda, ani korzyść majątkowa, nie muszą w rzeczywistości zaistnieć. Wystarczy, że sprawca dąży do ich zrealizowania.

Dlatego też wskazywane wysokości szkód, które ponieśli lub mogli potencjalnie ponieść poszkodowani przestępstwem, podawane są w oparciu o kwoty wskazywane przez samych pokrzywdzonych w zawiadomieniu o przestępstwie.

Wykres 6. Wysokość szkód (wg zawiadomienia o przestępstwie)



Największa jednostkowo grupa podawanych w zawiadomieniach o możliwości popełnienia przestępstwa szkód dotyczyła kwot pomiędzy 101 a 1000 zł (30% – 42 sprawy), a zatem kwot stosunkowo niewielkich. W 5% zawiadomień szkoda była niższa niż 100 zł (od 20 do 98 zł).

Ponad 48% zawiadomień wskazywało na szkody po stronie pokrzywdzonych w wysokości od 1001 do 10000 zł.

W pięciu przypadkach (3,57%) przewyższała 10 000 zł, przy czym najwyższa wyniosła 35 080 zł.

3.2.4. Kwalifikacja prawna czynu

Kwalifikacja prawna przyjęta za podstawę wszczęcia postępowań w objętych badaniem sprawach odnosiła się tylko do art. 287 § 1 k.k. Kwalifikacja z art. 287 § 2 k.k. nie wystąpiła.

W przypadku postępowań, w których odmówiono wszczęcia postępowania, zastosowano wyłącznie kwalifikację z typu podstawowego art. 287 k.k.

Kwalifikacja prawna zastosowana w analizowanych postępowaniach w 87,31% wskazywała na art. 287 § 1 k.k. (117 spraw) jako czyn wyczerpujący zachowanie sprawcy.

W 4,48% przypadków (sześć spraw) zastosowana została kwalifikacja kumulatywna art. 286 § 1 k.k. w zb. z art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.

Również w 4,48% zachowanie przestępcze zakwalifikowano jako czyny z art. 267 § 1 k.k. i 287 § 1 k.k. w zw. z 11 § 2 k.k. oraz jako czyny z art. 287 § 1 w zw. z art. 278 § 1 k.k. przy zastosowaniu art. 11 § 2 k.k. (po trzy przypadki).

W pozostałych sprawach (3,37%) przyjęto następujące kwalifikacje czynów:

- art. 13 § 1 k.k. w zw. z art. 286 § 1 k.k. w zb. z art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.,
- art. 287 § 1 k.k. i art. 279 § 1 k.k. w zw. z art. 11 § 2 k.k.,

- art. 13 § 1 k.k. w zw. z art. 287 § 1 k.k.,
- art. 286 § 1 k.k.,
- art. 279 § 1 k.k.

W odniesieniu do kwalifikacji z art. 279 § 1 k.k. przyjętej w postępowaniu *modus operandi* polegał na pozyskaniu w bliżej nieustalonym miejscu oraz okolicznościach na terenie Polski przez nieustalonego sprawcę kodu PIN do karty bankomatowej należącej do poszkodowanej, a następnie dokonanie zaboru z jej rachunku bankowego prowadzonego przez bank z siedzibą w Stanach Zjednoczonych pieniędzy w kwocie 2136 dolarów amerykańskich poprzez ich wypłacenie za pośrednictwem bankomatów znajdujących się na terenie Włoch.

W istocie sprawca swoim zachowaniem nie realizował znamion strony przedmiotowej przestępstwa z art. 287 § 1 k.k., chyba że przyjmiemy, iż poprzez posłużenie się skradzionym numerem PIN wpłynął na automatyczne przetwarzanie danych informatycznych i działając bez upoważnienia, osiągnął nienależną mu korzyść majątkową. Jednak wówczas powinna zostać przyjęta kwalifikacja kumulatywna obu przepisów.

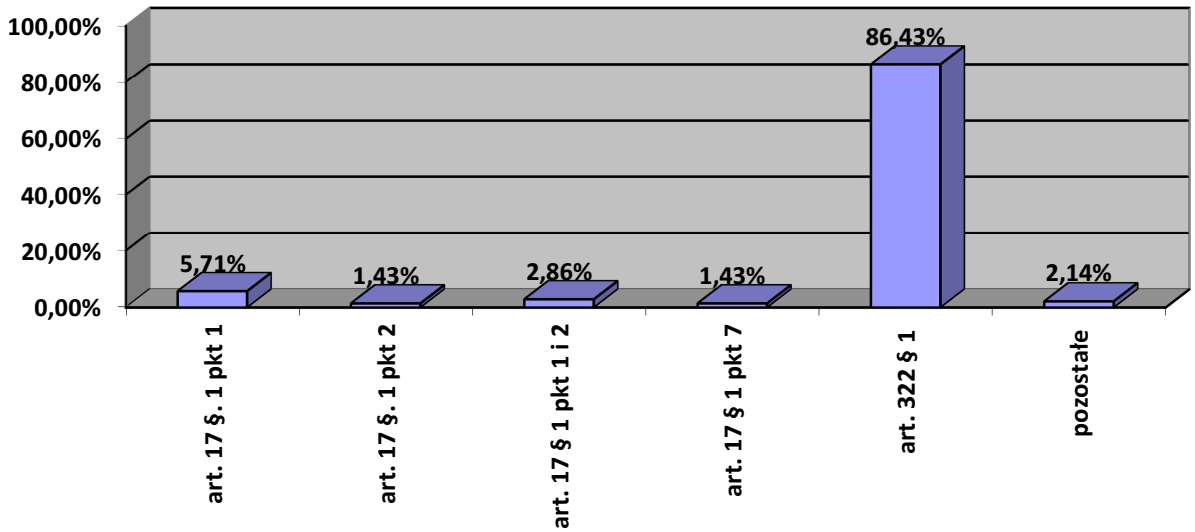
W przypadku kwalifikacji prawnej z art. 286 § 1 k.k. stan faktyczny polegał na doprowadzeniu w celu osiągnięcia korzyści majątkowej do niekorzystnego rozporządzenia mieniem, z tytułu nieautoryzowanych transakcji, wpływając na automatyczne przetwarzanie danych informatycznych i odczytanie zawartości paska magnetycznego poprzez posłużenie się skopiowaną kartą płatniczą przy wypłatach na terenie Dominikany i Tajlandii. Wydaje się jednak, że w tym przypadku właściwa byłaby kwalifikacja z art. 287 § 1 k.k.

3.2.5. Podstawy odmów/umorzeń postępowania

Jak wynika z wykresu 7 przeważająca większość postępowań została umorzona na podstawie art. 322 § 1 k.p.k., czyli w oparciu o przesłankę niewykrycia sprawcy przestępstwa (ponad 86% badanych spraw).

Taka podstawa przyjęta za podstawę zakończenia postępowania nie budzi wątpliwości ze względu na charakter czynów z art. 287 k.k. Zachowanie sprawcy polegające na „wpływie" lub „zmianie" danych informatycznych obejmuje szerokie spektrum czynów realizujących powyższe znamiona strony przedmiotowej. Sprawcy wchodzą w posiadanie danych wrażliwych dla pokrzywdzonych, wykorzystując w tym celu środki techniczne pozwalające im na pozyskanie lub zmianę treści takich danych, w szczególności takie, które pozwalają im na przełamanie zabezpieczeń. Wykrycie sprawców tych zachowań wymaga znacznych środków i współdziałania z dostawcami usług, z których pokrzywdzony korzystał (konta e-mail, bankowość elektroniczna, wystawcy kart płatniczych), a które w znacznej liczbie przypadków kończą się niepowodzeniem. Sam fakt ustalenia numeru IP komputera, z którego korzystał sprawca, nie musi prowadzić do ustalenia jego tożsamości. Uzyskany nr IP mógł bowiem zostać zmieniony za pomocą specjalnego oprogramowania, pozwalającego na ukrycie w ten sposób rzeczywistego miejsca, w którym znajdował się sprawca albo też mógł on korzystać przy popełnieniu przestępstwa z kart pre-paid, które nie pozwalają na ustalenie tożsamości, gdyż w ich przypadku nie ma prawnego obowiązku rejestracji danych ich posiadacza.

Wykres 7. Podstawy prawne zakończenia postępowań (w procentach)



W ośmiu przypadkach postępowanie umorzono na podstawie art. 17 § 1 pkt 1 k.p.k., tj. czynu nie popełniono albo brak danych dostatecznie uzasadniających podejrzenie jego popełnienia.

W pozostałych analizowanych przypadkach spraw jako podstawę umorzeń wskazano art. 17 § 1 pkt 2 k.p.k., art. 17 § 1 pkt 1 i 2 k.p.k., art. 17 § 1 pkt 7 k.p.k., art. 17 § 1 pkt 10 k.p.k., a w odniesieniu do odmowy wszczęcia – art. 305 § 1 k.k.

3.2.6. Czas trwania postępowania

Zbieranie materiału dowodowego w sprawach o przestępstwo oszustwa komputerowego polega w znacznej mierze na konieczności pozyskania danych identyfikujących adres IP komputera, z którego sprawca dokonał czynu zabronionego. Pozyskanie samego adresu IP może, choć w wielu przypadkach nie musi, prowadzić do ustalenia danych osobowych sprawcy.

Adres IP nie jest „numerem rejestracyjnym" komputera – nie identyfikuje jednoznacznie fizycznego urządzenia, może się dowolnie często zmieniać (np. przy każdym wejściu do sieci Internet), jak również kilka urządzeń może dzielić jeden publiczny adres IP. Ustalenie prawdziwego adresu IP użytkownika, do którego następowała transmisja w danym czasie, jest możliwe dla systemu/sieci odpornej na przypadki tzw. IP spoofingu – na podstawie historycznych zapisów systemowych[59].

Jeszcze trudniejsze jest ustalenie sprawcy w przypadku skimmingu danych zawartych na pasku magnetycznym karty płatniczej i osoby, która następnie takimi, skradzionymi danymi się posłużyła.

W przypadku przestępstw transgranicznych (np. dane karty pozyskane w jednym kraju są wykorzystywane w innym lub są wykorzystywane przy zakupach w sklepach internetowych za granicą) dochodzić do tego może jeszcze konieczność oczekiwania na realizację pomocy prawnej.

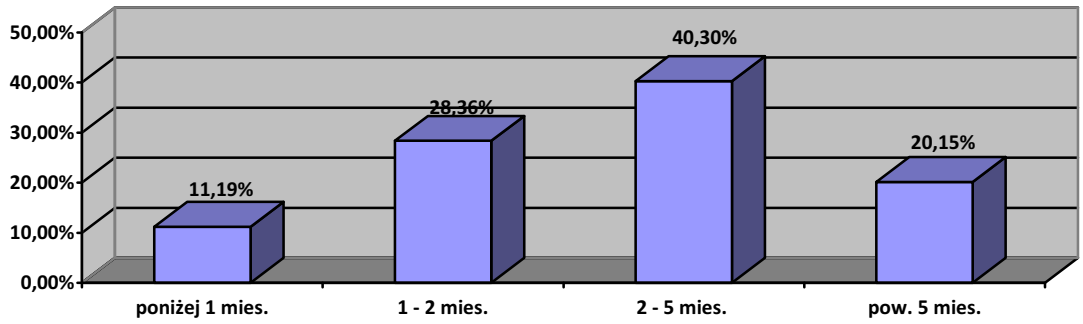
Dlatego też nie budzi wątpliwości, że postępowania w sprawach z art. 287 k.k. prowadzone są przez okres kilku miesięcy.

[59] Za: https://pl.wikipedia.org/wiki/Adres_IP (dostęp dnia 17 listopada 2015 r.).

Ponad 60% analizowanych postępowań prowadzonych było dłużej niż 2 miesiące, w tym ponad 40% – przez okres 2–5 miesięcy.

Poniżej miesiąca prowadzono niewiele ponad 11% spraw (15 przypadków).

Wykres 8. Czas trwania postępowania (od wszczęcia do umorzenia)



Powyżej 5 miesięcy prowadzonych było niewiele ponad 20% postępowań (27 spraw), w tym tylko trzy (ponad 2,2% wszystkich), w których czas postępowania przekraczał 12 miesięcy. W postępowaniu trwającym 14 miesięcy niezbędne było uzyskanie danych teleinformatycznych od operatora z terenu Stanów Zjednoczonych, co wymagało skorzystania z zagranicznej pomocy prawnej.

Na marginesie warto dodać, że w przypadku ponad 62% zawiadomień o popełnieniu przestępstwa czas pomiędzy złożeniem przez pokrzywdzonego zawiadomienia a wydaniem decyzji merytorycznej nie przekraczał miesiąca, w kolejnych ponad 30% przypadków wynosił 1–2 miesiące, w niewiele ponad 2% spraw (trzy przypadki) trwał 2–5 miesięcy, i w jednym przypadku (0,7%) wyniósł 6 miesięcy.

3.3. Sprawy zakończone prawomocnym orzeczeniem sądowym

3.3.1. Analiza postępowań sądowych

Stany faktyczne spraw zakończonych prawomocnym orzeczeniem sądowym różniły się istotnie od stanów faktycznych analizowanych w ramach postępowań

przygotowawczych. Są one zdecydowanie bardziej skomplikowane i nie jest możliwe dokonanie ich pogrupowania w prosty sposób, tak jak to uczyniono wyżej.

Oczywiście wśród analizowanych postępowań sądowych występują stany faktyczne obejmujące nieuprawnione uzyskanie dostępu do konta użytkownika na portalu aukcyjnym, zmianę danych dotyczących aukcji internetowych i uzyskanie korzyści majątkowej z tytułu przeprowadzenia fikcyjnej aukcji (około 17% przypadków). Zaobserwowano też takie, które wskazują na pozyskanie przez sprawcę danych o numerze karty, posiadaczu i numerze PIN, niezbędnych do dokonywania transakcji w sklepach internetowych lub wypłaty środków pieniężnych z bankomatu. Jednak w przypadku tej grupy spraw również one obejmują dodatkowe elementy, np. nieuprawniony dostęp do konta na portalu aukcyjnym, ale w celu dokonania zakupów towarów na szkodę posiadacza konta, czy też nieuprawnione wejście w posiadanie danych o karcie płatniczej wykorzystywanych następnie w celu pobrania gotówki z bankomatów lub płacenia za towary połączone jest z wcześniejszą kradzieżą samej karty.

Należy jednak wskazać, że przypadki postępowań, w których zachowanie sprawcy polegało na nieuprawnionym wykorzystywaniu środków znajdujących się na karcie płatniczej lub pobierania (przelewania) środków z rachunków bankowych, stanowiły aż 30% postępowań zakończonych wydaniem prawomocnego orzeczenia sądowego w 2013 r.

Ponadto sprawcy – w odniesieniu do nieuprawnionego dostępu do portalu aukcyjnego – wystawiali do fikcyjnej sprzedaży nie jeden przedmiot, lecz kilka lub więcej, stanowiących odrębne czyny (w skrajnym przypadku było ich 78).

W jednej ze spraw, w celu nieuprawnionego wejścia w posiadanie haseł dostępu do kont na portalu aukcyjnym, sprawcy wykorzystali pendrive z zainstalowanym na nim oprogramowaniem typu *keylogger*, które to oprogramowanie służące do śledzenia wpisywanych na klawiaturze komputera liter, instalowali na komputerach w kawiarenkach internetowych. W ten sposób uzyskali hasła do prawie 60 kont aukcyjnych, które potem posłużyły im do popełnienia przestępstwa oszustwa komputerowego.

Dającą się zauważyć w badanych postępowaniach sądowych odrębną grupą spraw są czyny zabronione wyczerpujące znamiona art. 287 k.k., a dokonywane przez pracowników firm na szkodę pracodawcy (30% przypadków).

Poszczególne zachowania sprawcze sprowadzały się przykładowo do:

1) bezprawnego usunięcia plików z serwera firmy, po uprzednim pozyskaniu hasła komputerowego umożliwiającego dostęp do informacji firmowych przechowywanych na serwerze, czym zablokowano działanie firmy w sieci, w tym dostęp do jej strony internetowej;

2) nieuprawnionego dokonania zmian w zapisie w komputerowym systemie sprzedaży firmy, w celu wyłudzenia towaru, na szkodę tego przedsiębiorstwa;

3) nieuprawnionego dokonania zmian w systemie informatycznym spółki służącym do wystawiania faktur VAT i paragonów oraz księgowania w odniesieniu do faktur sprzedaży i dokumentów wpłat w celu przywłaszczenia powierzonych pieniędzy spółki i jej kontrahentów;

4) manipulacji w systemie lojalnościowym firmy telekomunikacyjnej w ten sposób, że przekraczając udzielone sprawcy upoważnienie do wprowadzania nowych zapisów, działając w porozumieniu z innymi osobami, w sposób nieuprawniony podwyższono liczbę punktów w programie lojalnościowym, które następnie przekazywano klientom firmy w formie punktów lub w postaci kwotowej, czym spowodowano straty znacznej wartości;

5) dokonywania, bez upoważnienia, zmian w systemie bankowym, poprzez rejestrację nowych rachunków bankowych i przelewanie na ich stan bez uprawnienia środków pieniężnych.

W odniesieniu do czynów polegających na nieupoważnionym wpływie na przetwarzanie danych informatycznych w zakresie kart płatniczych zaobserwowano w aktach takich sprawców, którzy znali procedury i zasady przetwarzania takich danych, przez co byli w stanie wyrządzić znaczne szkody instytucji wydającej kartę. W szczególności polegały one na znajomości przez sprawcę mechanizmów działania kart zbliżeniowych, co umożliwiło mu, poprzez wielokrotne dokonywanie naprzemiennie transakcji on-line i off-line, znaczne zwiększenie debetu na

posiadanych przez niego kartach, przez co doprowadził on bank do niekorzystnego rozporządzenia mieniem.

Popularność serwisów społecznościowych (Facebook, Twitter itp.) powoduje, że one również stają się celem działania sprawców oszustwa komputerowego. Niejednokrotnie może to być działanie o charakterze złośliwym w stosunku do użytkowników takiego serwisu, jednak wyczerpujące znamiona typu określonego w art. 287 k.k. w sytuacji, gdy sprawca wchodzi w sposób nieuprawniony w posiadanie haseł dostępu do konta, blokuje je dla innych użytkowników lub dokonuje na nim zmian, ewentualnie udostępnia treści o charakterze prywatnym, które nie były przez posiadacza konta planowane do upublicznienia, bądź zamieszcza treści niepożądane przez osobę będącą użytkownikiem takiego konta (np. o charakterze pornograficznym).

Wśród badanych spraw odnotowano również pojedyncze przypadki dotyczące zmian w koncie uczestnika gry internetowej, nieuprawnionego dostępu do konta poczty e-mail, zawarcia przez Internet umowy pożyczki bez upoważnienia przy wykorzystaniu danych osobowych pokrzywdzonego.

W konsekwencji dla prawidłowego opisu czynu zabronionego sprawcy konieczne było stosowanie różnorodnych kwalifikacji, wśród których kwalifikacja wyłącznie na podstawie art. 287 § 1 k.k. wystąpiła w 37,5% postępowań (15 spraw). Dodatkową komplikację stanowi wielość czynów zarzucanych jednemu sprawcy (nawet aż 78).

Przykładowo można wymienić następujące kwalifikacje czynów (na podstawie aktu oskarżenia):

- art. 279 § 1 i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k.,
- art. 286 § 1 i art. 287 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 91 § 1 k.k.,
- art. 287 § 1 w zb. z art. 294 § 1 w zw. z art. 12 k.k.,
- art. 267 § 3 i art. 310 § 1 w zb. z art. 287 § 1 w zw. z art. 11 § 2 i art. 12 k.k. i art. 310 § 4 w zw. z art. 310 § 1 k.k.;

– art. 287 § 1 w zw. 294 § 1 i art. 279 § 1 k.k. przy zastosowaniu art. 11 § 2 k.k. w zw. z art. 12 k.k.

W jednej ze spraw sprawca oszustwa komputerowego działał w warunkach recydywy z art. 64 § 1 k.k.

Warto również zaznaczyć, że w jednym przypadku wystąpiła kwalifikacja z typu uprzywilejowanego oszustwa komputerowego określonego w art. 287 § 2 k.k.

Podkreślenia wymaga szerokie (w ponad 40% spraw) wykorzystanie w analizowanych postępowaniach opinii biegłych. W wielu przypadkach potwierdzenie popełnienia przestępstwa oszustwa komputerowego wymaga posiadania wiadomości specjalnych, w tym szczególnie z dziedziny informatyki. Dlatego też prokuratury powoływały w celu analizy zapisów danych informatycznych na dyskach komputerowych lub kartach płatniczych biegłych z zakresu informatyki. Ponadto w kilku przypadkach powoływano biegłych psychiatrów – dla oceny stanu zdrowia psychicznego podejrzanych i ewentualnego potwierdzenia ich poczytalności.

Zawiadomienia o popełnieniu przestępstwa w sprawach zakończonych na etapie postępowania sądowego wpłynęły w 57,5% przypadków od osób fizycznych, będących pokrzywdzonymi działaniami sprawców.

Zawiadomienia pochodzące od banków, które w ramach czynności związanych z nadzorowaniem prawidłowości realizacji transakcji bankowych stwierdzały popełnienie oszustwa komputerowego, wystąpiły w 12,5% postępowań (pięć przypadków).

W 20% spraw zawiadomienia wpłynęły od innych podmiotów: spółek prawa handlowego, osób prowadzących działalność gospodarczą, towarzystwa ubezpieczeniowego czy wspólnoty mieszkaniowej.

Pozostałe 10% przypadków to sprawy wyłączone z innych postępowań oraz subsydiarny akt oskarżenia – wycofany następnie przez oskarżyciela.

Celem działania sprawcy przestępstwa oszustwa komputerowego jest osiągnięcie korzyści majątkowej lub wyrządzenie szkody innej osobie. W odróżnieniu od postępowań zakończonych umorzeniem, szkody ustalone w toku postępowania

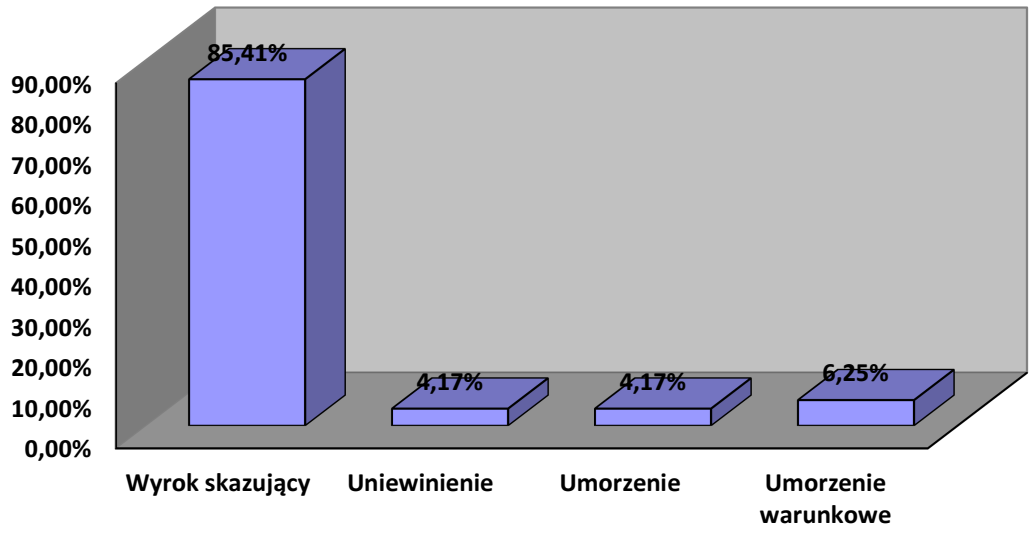
zakończonego skierowaniem do sądu aktu oskarżenia należy uznać za wysokie. Szkody wynoszące powyżej 10 000 zł wystąpiły w ponad 41% przypadków. W ponad 32% ustalona wysokość szkody nie przekraczała 1000 zł. Najniższa z ustalonych szkód wynosiła 4 zł, najwyższa – 924 000 zł.

3.3.2. Rodzaje orzeczeń

W badanych postępowaniach zarzut popełnienia przestępstwa z art. 287 k.k. postawiono 48 osobom. Szczegółowa charakterystyka sprawców została przedstawiona w dalszej części opracowania.

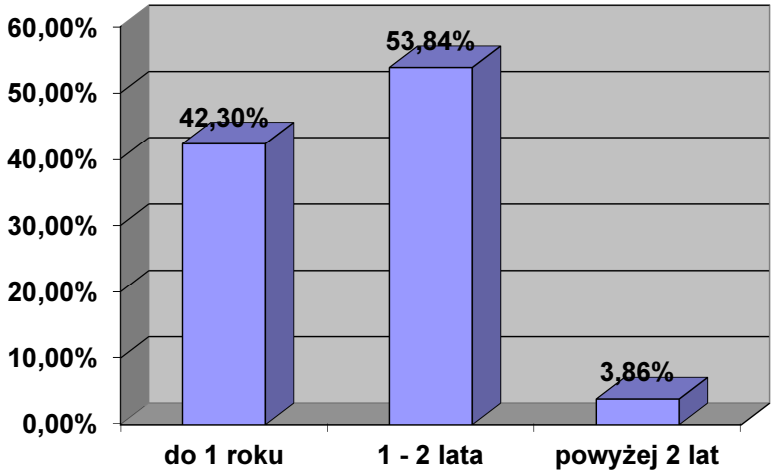
W stosunku do 85,41% oskarżonych wydano wyrok skazujący (41 osób), w pozostałych 12,5% postępowanie zostało umorzone (dwie osoby) lub umorzone warunkowo na okres 2 lat (dwie osoby) lub roku (jedna osoba). W pozostałych dwóch przypadkach wydano wyrok uniewinniający.

Wykres 9. Sposób zakończenia postępowania sądowego



Przestępstwo z art. 287 § 1 k.k. nie jest zagrożone wysokimi sankcjami, bo jedynie od 3 miesięcy do 5 lat pozbawienia wolności. Badanie pokazuje, że wobec ponad 42% skazanych orzeczono karę pozbawienia wolności do roku, w stosunku do prawie 54% karę w wymiarze od roku do lat 2. Tylko w niespełna 4% przypadków kara przekroczyła 2 lata (maksimum 4 lata i 4 miesiące).

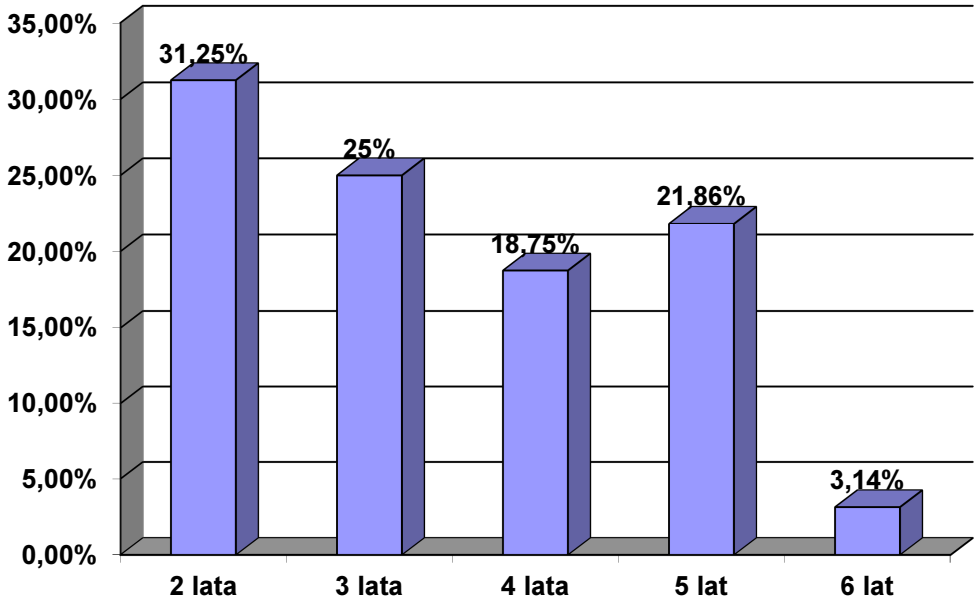
Wykres 10. Wysokość orzeczonej kary pozbawienia wolności (bez kary łącznej)



Trochę inaczej wysokość orzeczonej kary pozbawienia wolności kształtowała się w ramach wymiaru kary łącznej. Tutaj karę do roku pozbawienia wolności orzeczono wobec 21,42% skazanych, do 2 lat pozbawienia wolności – w stosunku do 42,86%, a karę powyżej 2 lat (maksymalnie 5 lat i 6 miesięcy) wobec pozostałych 35,72%.

W stosunku do ośmiu skazanych orzeczono karę bezwzględnego pozbawienia wolności. W pozostałych przypadkach (26 osób – 76,47%) kara ta została warunkowo zawieszona na okres próby. Wykres 11 prezentuje szczegółowe dane dotyczące orzeczonej długości okresu warunkowego zawieszenia wykonania kary pozbawienia wolności.

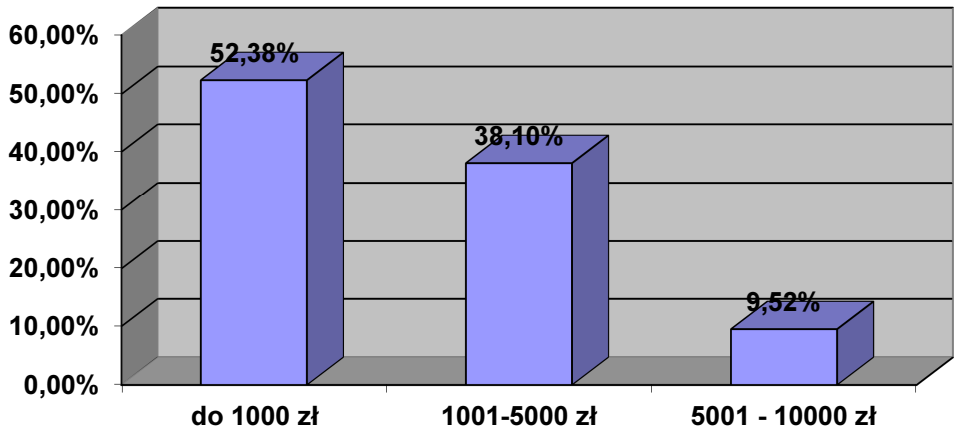
Wykres 11. Długość okresu warunkowego zawieszenia wykonania kary pozbawienia wolności



W stosunku do 21 skazanych (52,5%) orzeczono karę grzywny obok kary pozbawienia wolności.

W ponad 53% przypadków wysokość orzeczonej grzywny nie przekroczyła 1000 zł. W żadnym przypadku nie przekroczyła kwoty 10 000 zł (najwyższa 9000 zł).

Wykres 12. Wysokość kary grzywny orzeczonej obok kary pozbawienia wolności



Wobec dwóch osób orzeczono karę ograniczenia wolności w wymiarze 6 miesięcy nieodpłatnej, kontrolowanej pracy na cele społeczne w wymiarze 20 i 30 godzin miesięcznie, przy czym w stosunku do jednego ze skazanych karę taką wymierzono w związku z kwalifikacją czynu na podstawie art. 287 § 2 k.k.

W stosunku do 22 skazanych orzeczono obowiązek naprawienia szkody, w tym wobec czterech z nich – częściowego naprawienia szkody.

W stosunku do 10 skazanych orzeczono dozór kuratora.

Ponadto wobec pojedynczych skazanych orzeczono: przepadek przedmiotów na podstawie art. 44 § 2 k.k., zobowiązanie do przeproszenia pokrzywdzonego, zakaz zajmowania stanowiska, zakaz wykonywania zawodu.

Jedynie w pięciu przypadkach wniesiono od orzeczenia skazującego środek odwoławczy (apelację). Podstawą dla wniesienia środka zaskarżenia była obraza przepisów prawa materialnego albo rażąca niewspółmierność kary lub niesłuszne zastosowanie lub niezastosowanie środka zabezpieczającego.

W stosunku do trzech apelacji, sąd drugiej instancji orzekł ich całkowitą bezzasadność i utrzymał wydane orzeczenia w mocy. W pozostałych dwóch

przypadkach dokonał częściowej modyfikacji wydanego wyroku w zakresie orzeczenia o karze.

3.3.3. Sprawca oszustwa komputerowego

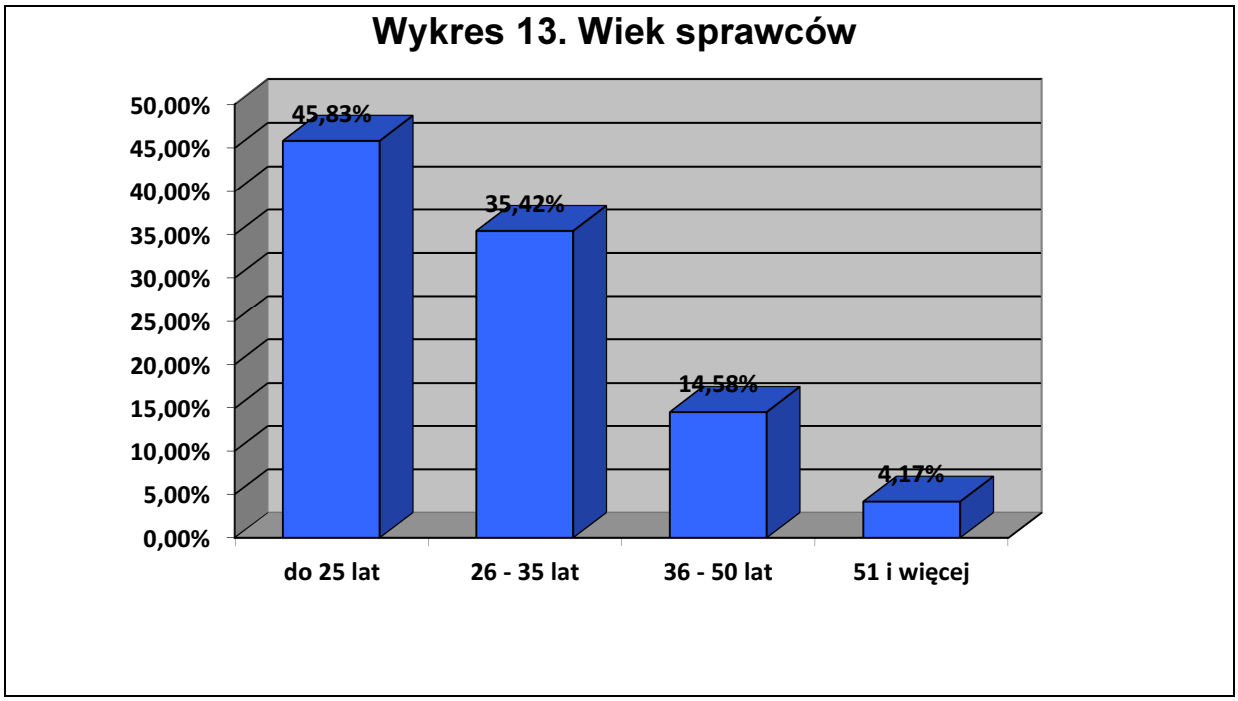
W objętych badaniem postępowaniach zakończonych wydaniem prawomocnego wyroku skazującego w 2013 r. akt oskarżenia o popełnienie przestępstwa z art. 287 k.k. skierowano przeciwko 48 osobom. Wskazać należy, że wszystkim oskarżonym postawiono zarzut z art. 287 § 1 k.k., jako samodzielną podstawę oskarżenia albo w ramach kwalifikacji kumulatywnej. W żadnym z badanych przypadków nie wystąpiła w akcie oskarżenia kwalifikacja z art. 287 § 2 k.k., choć taką kwalifikację w jednym przypadku przyjął w wyroku sąd.

Badanie pokazało, że sprawcami przestępstw oszustwa kredytowego są, co raczej nie zaskakuje, przede wszystkim mężczyźni, którzy stanowią 87,5% ogółu sprawców, kobiety zaś pozostałe 12,5%.

Rozpatrując osobę sprawcy oszustwa komputerowego pod kątem wieku, należy stwierdzić, że oskarżeni w wieku do 25 lat stanowili w badanych sprawach najliczniejszą grupę (niemal 46% wszystkich sprawców).

Równie dużą grupę stanowili sprawcy w wieku 26–35 lat (ponad 35%).

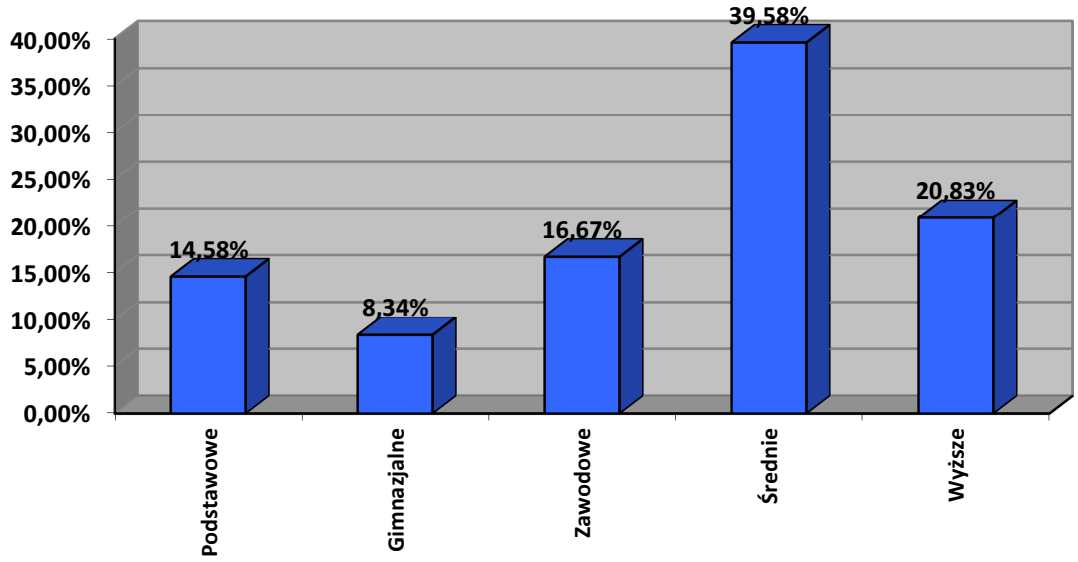
Osoby w wieku powyżej 36 roku życia stanowiły jedynie pozostałe 18,75% sprawców, w tym powyżej 50 roku życia – tylko niewiele ponad 4%.



Sprawca oszustwa komputerowego jest przeciętnie wykształcony. W ponad 64% ma on wykształcenie gimnazjalne, zawodowe lub średnie, podstawowe zaś w ponad 14,5% (co stanowi łącznie ponad 78% wszystkich sprawców). Wykształcenie wyższe ma 20% ogółu sprawców.

Warto w tym kontekście zwrócić uwagę na istotną, bo prawie 40% grupę osób z wykształceniem średnim. Często takie osoby mają przygotowanie techniczne, w tym techniczno-informatyczne lub ekonomiczne, co może być istotne przy popełnieniu przestępstw o charakterze komputerowym.

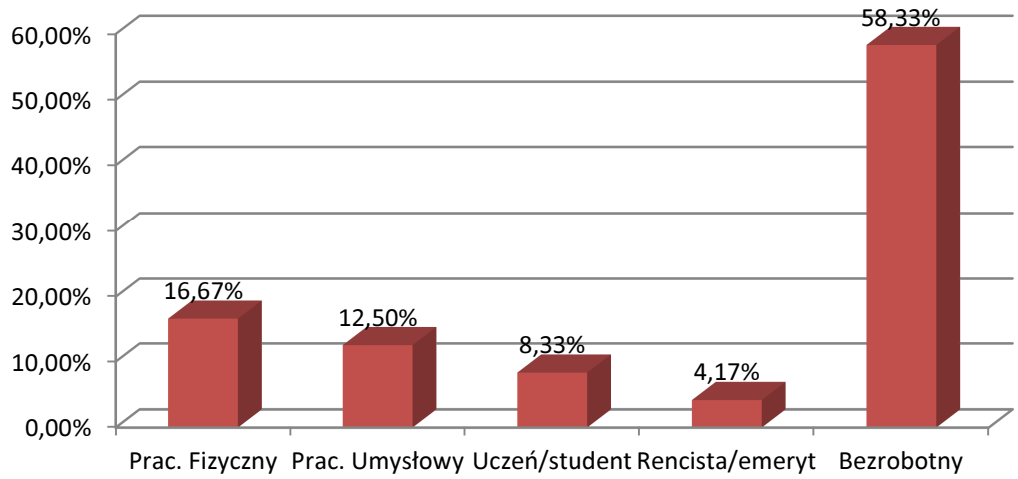
Wykres 14. Wykształcenie sprawców



Pomimo że ponad 60% sprawców przestępstwa z art. 287 k.k. stanowią osoby co najmniej z wykształceniem średnim, co wskazywałoby na możliwość łatwiejszego znalezienia przez nie pracy, to jednak pod względem ich sytuacji zawodowej są to osoby przede wszystkim bezrobotne – prawie 60% przypadków.

Jednak szukając przyczyn takiego stanu, należy tę zmienną odnieść od wieku sprawców. Z porównania tych dwóch danych wynika, że sytuacja taka może wynikać z młodego wieku sprawców. Będą to bowiem osoby, które co prawda ukończyły już szkoły średnie, lecz jeszcze nie pojawiły się na rynku pracy (zatem są formalnie bezrobotne) i pozostają w dalszym ciągu na utrzymaniu rodziców, ewentualnie podejmują jedynie prace dorywcze.

Wykres 15. Sytuacja zawodowa sprawców



Sprawcy oszustwa komputerowego nie byli w większości (ponad 56%) wcześniej karani. Jeżeli już byli wcześniej sprawcami przestępstw, to wchodzili w konflikt z prawem wielokrotnie i skazywani byli za różnego rodzaju przestępstwa, jednak z pewną przewagą czynów z grupy przestępstw przeciwko mieniu, w tym art. 286 § 1 k.k. oraz art. 279 § 1 k.k.

W toku postępowania wobec ośmiu podejrzanych zastosowano środek zabezpieczający w postaci tymczasowego aresztowania. Wobec kolejnych pięciu podejrzanych zastosowano poręczenie majątkowe. Pod dozór Policji oddano sześć osób. W stosunku do dwóch orzeczono zakaz opuszczania kraju. W kolejnych dwóch przypadkach zastosowano zabezpieczenie majątkowe. Jeden ze sprawców odbywał karę pozbawienia wolności w innej sprawie.

Warto również dodać, że jeden ze sprawców został zatrzymany na podstawie Europejskiego Nakazu Aresztowania.

4. Podsumowanie

Przestępczość komputerowa, która pojawiła się wraz z rozwojem systemów teleinformatycznych i dokonywaniem coraz większej liczby operacji za pośrednictwem sieci Internet, to ta grupa przestępstw, której liczba stale będzie rosła. Jest to przestępczość trudna do wykrycia, pomimo istnienia śladów jej popełnienia na nośnikach danych, wymagająca zaawansowanych metod analitycznych i znacznych środków na jej zwalczanie.

W tym też można się doszukiwać przyczyn niewielkiej liczby spraw kierowanych do sądów z oskarżeniem o popełnienie przestępstw z art. 287 k.k. Pomimo wzrastającej, niemal od początku funkcjonowania tego przestępstwa w polskim systemie prawnym, liczby spraw wszczynanych w oparciu o analizowany przepis, to efektywność takich postępowań, rozumiana jako liczba spraw zakończonych aktem oskarżenia i w konsekwencji wydaniem wyroku skazującego, jest niewielka. Dane o liczbie postępowań umarzanych na etapie postępowania przygotowawczego lub kończonych wydaniem postanowienia o odmowie wszczęcia postępowania sięga nawet 95% rocznie.

Wśród postępowań zakończonych umorzeniem lub odmową wszczęcia dominują przypadki wpływania na automatyczne przetwarzanie danych informatycznych i dokonywanie zmian w ich zapisach w celu przejęcia kont użytkowników na portalach aukcyjnych, aby wystawić na nich do sprzedaży fikcyjne towary i w ten sposób uzyskać nienależną korzyść majątkową. Drugą grupą przypadków jest zmiana danych informatycznych zawartych na różnego typu kartach płatniczych lub danych dostępowych do internetowych rachunków bankowych, w celu wyrządzenia szkody majątkowej ich posiadaczom.

W grupie postępowań zakończonych wydaniem prawomocnego orzeczenia sądowego daje się wyodrębnić, poza wskazanymi wyżej dwoma typowymi metodami popełnienia oszustwa komputerowego (jednak zdecydowanie mniej dominującymi), również grupę przypadków, w których sprawcami są pracownicy różnych przedsiębiorstw, a podejmowane przez nich działania wpływające na przetwarzanie danych informatycznych skierowane są przeciwko i na szkodę ich pracodawcy.

W grupie ustalonych sprawców przeważają osoby młode i bardzo młode (do 25 roku życia), o wykształceniu średnim, głównie bezrobotne.

Badanie pokazało, że w procesie dowodzenia zaistnienia czynu zabronionego z art. 287 k.k. istotne jest uzyskanie opinii specjalistycznej, głównie z zakresu informatyki. Dlatego warty odnotowania jest fakt, że w ponad 40% analizowanych spraw skierowanych do sądu występowano o uzyskanie opinii biegłego.

Sam przepis kreujący przestępstwo oszustwa komputerowego, choć w piśmiennictwie jest przedmiotem szerokich analiz dogmatycznych, to wydaje się, że w chwili obecnej nie wymaga żadnej korekty legislacyjnej. Wyposażenie przez ustawodawcę znamion tego typu przestępstwa w przesłanki o charakterze dosyć ogólnym pozwala na ich stosowanie do bardzo szybko rozwijających się oraz zmieniających metod i technik wykorzystywanych przez sprawców oszustwa komputerowego.

Na zakończenie wydaje się być uzasadniona uwaga natury bardziej ogólnej.

W dobie społeczeństwa informacyjnego, uzależnionego od „świata wirtualnego" będziemy coraz bardziej narażeni na stanie się ofiarą któregoś z przestępstw grupy „komputerowych". Jedyne co możemy – jako użytkownicy Internetu – próbować zrobić, to podejmować środki zabezpieczające przed nieuprawnionym wejściem w posiadanie naszych danych osobowych czy danych o numerach rachunków bankowych, z tą jednak świadomością, że choćbyśmy przedsiębrali jak najlepsze środki zaradcze, to i tak nie jesteśmy w stanie wyeliminować ataku na nas, dokonywanego za pośrednictwem systemów teleinformatycznych.