CBKE
e-BIULETYN

Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni

Agnieszka Kania

Katedra Prawa Karnego Materialnego

Nowe technologie informacyjne, obok swoich pozytywnych aspektów dla postępu cywilizacyjnego, niosą za sobą także liczne zagrożenia. Oferowane przez nie ułatwienia czy udogodnienia pozostają często w opozycji w stosunku do skutecznych metod umożliwiających panowanie nad niebezpieczeństwami, które często się z nimi wiążą, jako ich nieodłączne elementy. Poza dyskusją pozostaje zatem stwierdzenie, że wielkie osiągnięcia mają swoje dwa oblicza – z jednej strony przyczyniają się do rozwijania celów powszechnie akceptowanych, ocenianych pozytywnie, z drugiej zaś - mogą doprowadzić do niekorzystnych konsekwencji, które okazują się niekiedy nawet sprzeczne z prawem.

Powstanie, rozbudowa a wreszcie globalizacja społeczeństwa informacyjnego[1] sprawiły, że w ostatnich latach trudno byłoby sobie wyobrazić którąkolwiek z dziedzin życia, pozostającą poza siecią komputerową. Jej dynamiczny rozwój sprawił, że zasługuje ona na miano najszybciej rozwijającego się medium.[2] Jednakże - to nowe, silnie zdecentralizowane „medium" nie pozwala się pod względem prawnym do końca skontrolować. Przyczyną takiego stanu rzeczy będzie z pewnością jego ogromny zasięg i często skomplikowane rozwiązania techniczne, mające w nim zastosowanie. W związku z powyższym, właściwe unormowanie tej materii, a przede wszystkim

[1] Pojęcie społeczeństwa informacyjnego jest bardzo szerokie, co powoduje trudności z ustaleniem jego zakresu znaczeniowego. Termin ten, umownie oznaczany skrótem SI, pojawił się w pracach ekonomisty Tadeo Umesao, który na początku lat sześćdziesiątych użył go w stosunku do społeczeństwa japońskiego, „w którym o standardach gospodarki zaczęły decydować informacja i technologia". Por. A. Bógdał – Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 31.

[2] Do kategorii „nowych" mediów, obok Internetu i komputerów, zalicza się również: telewizję kablową, satelitarną, radio analogowe, telefonię komórkową oraz wideo. Wspólną ich cechą jest wykorzystanie komunikacji elektronicznej. Por. A. Bógdał – Brzezińska, M.F. Gawrycki, *op. cit*., s. 36.

zapewnienie jej kompleksowej regulacji normatywnej, stanowi największe wezwanie dla ustawodawców obecnych czasów[3], którzy powinni skutecznie zapobiec kryzysowi prawa i całego wymiaru sprawiedliwości.

Ze względu na specyfikę problematyki prawnoinformatycznej można by zastanawiać się nad sensem ewentualnego, doktrynalnego wyróżnienia gałęzi prawa o ujednoliconej i powszechnie zaaprobowanej nazwie np. prawo komputerowe, prawo informatyczne czy prawo cyberprzestrzeni. Argumentem przemawiającym na rzecz takiego postulatu jest fakt, iż wielkie osiągnięcia technologiczne kreują pewne specyficzne konstrukcje (tylko im właściwe), wykraczające poza ramy tradycyjnych instytucji prawnych. Ich innowacyjny charakter sprawia, że nie spełniają one konstytutywnych przesłanek przewidzianych dla tych ostatnich. Wymagają tym samym stworzenia odpowiednich dla nich, sui generis regulacji prawnych. Z drugiej jednak strony dostrzega się ścisłe powiązania interpretacyjne zachodzące między rozwiązaniami z obszaru nowych technologii a dorobkiem innych dziedzin prawa. Trudno byłoby zatem dokonywać dogmatycznej analizy np. e – oświadczenia woli czy e – podpisu, pomijając przy tym zupełnie przepisy cywilistyczne, regulujące tradycyjne formy tych instytucji. Podobnie nie można oddzielać problematyki przestępczości komputerowej od wykształconych i utrwalonych w prawie karnym zasad odpowiedzialności.[4]

Niezależnie od przedstawionych rozważań o potrzebie wyodrębniania bądź niewyodrębniania nowej gałęzi prawa, postulat ciągłego dostosowywania czy uzupełniania rozwiązań normatywnych do zmieniającej się rzeczywistości należałoby uznać za konieczny. „Rewolucja Informacyjna" powinna zatem automatycznie pociągać za sobą rozwój prawa, zwłaszcza zaś takich regulacji, które chroniłyby całe społeczeństwo przed najpoważniejszymi dla niego niebezpieczeństwami w cyberprzestrzeni.[5]

Bezspornie istotna rola w tym zakresie przypada prawu karnemu, które poprzez odpowiednią reglamentację prawną, będzie wypełniać w ten sposób swoją naczelną funkcję, jaką jest zapewnienie bezpieczeństwa podmiotom uczestniczącym w życiu społecznym.[6] Dostrzegając szkodliwy charakter zjawisk towarzyszących zmianom cywilizacyjnym, polski ustawodawca nie mógł pozostać na nie obojętny. Wprowadzone przez niego nowe rozwiązania legislacyjne miały w założeniu stać się skutecznym narzędziem do walki z patologicznymi atakami nowoczesnych technologii teleinformatycznych. Wymieniana w tym kontekście przestępczość związana z systemami i sieciami komputerowymi, zakreślająca coraz szersze widnokręgi swej obecności,

[3] S. Stanisławska – Kloc, *Ochrona baz danych,* Kraków 2002, s. 22 – 23.
[4] Por. K. Dobrzeniecki, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 61 -62.
[5] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. XV.
[6] Por. M. Bojarski, J. Giezek, Z. Sienkiewicz, *Prawo karne materialne. Część ogólna i szczególna*, Warszawa 2004, s. 25 – 26, L. Gardocki, *Prawo karne*, Warszawa 2008, s. 5 – 6.

wymusiła niejako na twórcach obowiązującego od 01.09.1998 r. kodeksu karnego[7] przyjęcie odpowiednich przepisów materialnych. Z uwagi na tą konieczność ustawodawca wprowadził do polskiego systemu prawnokarnego nieznane dotąd typy czynów zabronionych.

Jednym z nich jest występek oszustwa komputerowego, o którym mowa w rozdziale poświęconym przestępstwom przeciwko mieniu - art. 287 kk. Przepis ten nie miał swojego odpowiednika w poprzednim kodeksie karnym z 1969 r.[8] Stosowna regulacja prawna miała zatem wypełnić lukę kryminalizacyjną[9], która pojawiła się w d. kk w związku z postępującym rozwojem informatyzacji. W uzasadnieniu do rządowego projektu kodeksu karnego wskazano, że wprowadzenie tego typu przestępstwa do rozdziału XXXV n. kk jest zabiegiem koniecznym, czyli dostosowującym prawo do zmieniających się czasów, gdyż, jak trafnie zauważono, tradycyjne pojęcie oszustwa zawiera takie ustawowe znamiona, które przy oszustwie komputerowym nie mogą zostać spełnione, mimo że objęta celem działania sprawcy korzyść majątkowa zostanie osiągnięta.[10]

Oszustwo, na które wskazuje art. 287 kk stanowi jeden z wielu przykładów tzw. przestępstw komputerowych. Zarówno pojęcie „oszustwa" w rozumieniu art. 287 kk, jak również „przestępczości komputerowej" wymaga odrębnej uwagi.

Poszukując objaśnienia terminu „oszustwo", można by odwołać się do jednego ze starszych podręczników prawa karnego - podręcznika F. Maciejewskiego „Wykład prawa karnego", w którym autor przybliżył znaczenie tego pojęcia. W świetle przedstawionego tam ujęcia: „Wyraz oszustwo pochodzi od słowa szukać, obszukać, oszukać, czyli naokoło szukać, jak ten co zwierzyny szuka, aby ją złowić, a dostrzegłszy ślady obszukuje wedle niej stosownych środków i naokoło niej chodzi, obchodzi (stąd obejście), aż obszukawszy, czyli oszukawszy ją, łapie ją albo w matnię wpędza i trzyma, że aż się wyślizgnąć nie zdoła".[11] Aktualne znaczenie, a przede wszystkim ujęcie prawne tego terminu jest oczywiście znacznie inne, z pewnością nie tak obrazowe. Tzw. klasyczne oszustwo, o którym mowa w art. 286 kk polega na wprowadzeniu w błąd, wyzyskaniu błędu lub niezdolności pokrzywdzonego do należytego pojmowania przedsiębranego działania. Zgodnie z poglądami orzecznictwa przepis ten pozwala na rozróżnienie dwóch rodzajów oszustw: oszustwa czynnego (wprowadzenie w błąd) oraz oszustwa biernego (wyzyskanie błędu innej osoby).[12]

---

[7] Ustawa kodeks karny z dn. 06.06.1997 r., DzU Nr 88, poz. 553, z póź. zm. Dzień wejścia w życie kk określała odrębna ustawa zawiera przepisy wprowadzające kodeks karny z dn. 06.06.1997 r., DzU Nr 88, poz. 554, z póź. zm.
[8] Ustawa kodeks karny z dn. 16.04.1969 r., DzU Nr 13, poz. 94, z póź. zm.
[9] Por. P. Kardas, J. Satko, *Przestępstwa przeciwko mieniu. Przegląd problematyki. Orzecznictwo (SN 1918 – 2000). Piśmiennictwo,* Kraków 2002, s. 82, A. Chmiel, *Przestępstwa związane z wykorzystaniem komputera – charakterystyka zagadnienia*, Palestra 1991, nr 10, s. 16 -17.
[10] Por. *Uzasadnienie rządowego projektu kodeksu karnego. Nowe kodeksy karne z uzasadnieniami*, Warszawa 1997, s. 206 – 207.
[11] F. Maciejowski, *Wykład prawa karnego w ogólności z zastosowaniem kodeksu kar głównych i poprawczych z dniem 20 grudnia – 1 stycznia 1848 r. w Królestwie Polskiem obowiązującego tudzież ustawy przechodniej i instrukcji dla sądów,* Warszawa 1848, za: Z. Szczurek, *Oszustwo w handlu na szkodę nabywcy w polskim prawie karnym,* Warszawa 1976, s. 5 oraz E. Jakimiuk, J. Zając, *Systematyka oszustw w prawie karnym i taktyka ich zwalczania*, Legionowo 2008, s. 15.
[12] Wyrok SN z 27.10.1986 r. , sygn. II KR 134/86, OSNPG z 1997 r., nr 7, poz. 80.

Z kolei oszustwo komputerowe, mające na względzie zastępowanie relacji interpersonalnych relacjami człowieka z urządzeniami elektronicznymi, zachodzi wówczas, gdy, sprawca oddziałuje na procesy techniczne związane z automatycznym przetwarzaniem danych.[13]

W obu przypadkach oszustwa – art. 286 kk oraz art. 287 kk - ustawodawca podkreśla cel działania sprawcy, jakim jest osiągniecie korzyści majątkowej. Warunek ten oznacza, że jeżeli sprawca działa w innym celu niż osiągnięcie korzyści majątkowej, a w przypadku oszustwa komputerowego, także w innym, niż w sposób alternatywnie podany w tym przepisie tzn. w celu wyrządzenia szkody, nie jest oszustem w rozumieniu prawa karnego.[14] Często powoływanym przykładem oszustwa komputerowego popełnionego w celu osiągnięcia korzyści majątkowej jest spowodowanie przelewu nierzadko wysokiej sumy pieniężnej na rachunek sprawcy poprzez złamanie hasła w sieci komputerowej banku. Z kolei odpowiedzialność za oszustwo komputerowe popełnione w celu wyrządzenia innej osobie szkody, dotyczy zarówno przypadków, gdy szkoda to wynik podjętej przez sprawcę aktywności, którą określają taksatywnie wymienione znamiona strony przedmiotowej przepisu, charakteryzujące jego zachowanie, jak i sytuacji, gdy działanie sprawcy jest tylko sposobem dla wyrządzenia innej szkody.[15] Podmiotem przestępstwa w świetle art. 286 kk, jak również w ujęciu art. 287 kk nie będzie natomiast osoba działająca np. w celu samodowartościowania się i zaspokojenia w ten sposób własnych ambicji.[16]

O wiele więcej kontrowersji wywołuje pojęcie, a właściwie zagadnienie tzw. przestępczości komputerowej, które nie zostało bliżej określone przez polskiego ustawodawcę. Nie precyzuje go ani art. 115 kk, zawierający objaśnienie wyrażeń ustawowych, ani nie odwołuje się do tego terminu (a tym bardziej nie wyjaśnia go) żaden przepis części szczególnej kodeksu karnego. Doktryna prawnicza posługuje się jednak powszechnie tym określeniem, co oznacza, że zostało ono przez nią zaakceptowane, choć nadal istnieje szereg wątpliwości co do jego zakresu znaczeniowego. Stąd też ewentualna definicja przestępczości komputerowej będzie pozbawiona waloru naukowego, a jedynie można jej nadać charakter publicystyczny.[17] W literaturze amerykańskiej pojawiają się jednocześnie coraz to nowe wyrażenia synonimiczne w odniesieniu do przestępstw komputerowych. Często określa się je mianem cyberprzestępstw[18], przestępstw związanych z technologią cyfrową[19] czy przestępstw internetowych.[20] Niezależnie

[13] A. Adamski, *Prawo*…, s. 115.
[14] K. Daszkiewicz, *Kodeks karny z 1997 roku. Uwagi krytyczne*, Gdańsk 2001, s. 353 – 354.
[15] J. Wojciechowski, *Kodeks karny, Wyd. II poprawione i uaktualnione. Komentarz. Orzecznictwo*, Warszawa 2000, s. 537 – 538.
[16] K. Daszkiewicz, *op. cit*., s. 354.
[17] A. Adamski, *Przestępstwa komputerowe w nowym kodeksie karnym. Nowa kodyfikacja karna, kodeks karny – krótkie komentarze, zeszyt 17, Ministerstwo Sprawiedliwości, Departament Kadr i Szkolenia*, Warszawa 1998, s. 15.
[18] L. E. Quarautiello, *Cyber Crime: how to protect yourself from computer criminals?,* Tiare Pubns, 1996, za A. Adamski, *Prawo*…, s. 33.
[19] N. Barrett, *Digital Crime – Policing the Cybernation*, Kogan Page 1997, za A. Adamski, *Prawo*…, s. 33.
[20] R. Clark, *Technological Aspects of Internet Crime Prevention*, 1998, za A. Adamski, *Prawo*…, s. 33.

od przedstawionego powyżej sceptycyzmu, związanego ze sprecyzowaniem tego terminu, A. Adamski eksponuje dwa jego ujęcia, wyróżniając przy tym materialnoprawny oraz procesowy aspekt przestępczości komputerowej.[21] Powyższa koncepcja świadczy o współzależności zachodzącej między przepisami materialnymi i proceduralnymi, gdyż wypełnienie przez sprawcę znamion ustawowych stanów faktycznych, stwarza w świetle prawa procesowego, zwłaszcza dowodowego, realną możliwość zastosowania sankcji karnych.[22]

Przechodząc, w pierwszej kolejności, na płaszczyznę regulacji prawa karnego materialnego[23] należy stwierdzić, że przestępczość komputerową powinno się wiązać z dwojakiego rodzaju czynami zabronionymi. Pierwsza grupa obejmuje przestępstwa stricte komputerowe, nazywane także przestępstwami skierowanymi przeciwko bezpieczeństwu przetwarzanych informacji. W tym kontekście na uwagę zasługuje rozdział XXXIII kodeksu karnego, zatytułowany: „Przestępstwa przeciwko ochronie informacji", gdzie przedmiotem ochrony jest szeroko rozumiana informacja. Przepisy tego rozdziału umożliwiają pociągnięcie do odpowiedzialności karnej sprawców zamachów na bezpieczeństwo elektronicznie przetwarzanych danych. W tym zakresie należy wymienić następujące przestępstwa: hacking (art. 267 § 1 kk), podsłuch (art. 267 § 2 kk), naruszenie integralności komputerowego zapisu informacji (art. 268 § 2 kk), sabotaż komputerowy (art. 269 § 1 i 2 kk). Druga grupa czynów obejmuje typowe nadużycia komputerowe, które prowadzą do naruszenia dóbr prawnych w związku z elektronicznymi systemami przetwarzania danych. Komputer staje się w tym przypadku narzędziem niezbędnym do popełnienia przestępstwa. Wykorzystując elektroniczne przetwarzanie danych można popełnić różne pod względem rodzajowym przestępstwa. Sieci komputerowe oferują najprostsze i jednocześnie najszybsze sposoby porozumiewania się sprawców. Wykorzystanie Internetu sprzyja rozpowszechnianiu treści, które można by określić mianem społecznie szkodliwych np. pornograficzne, rasistowskie, pochwalające popełnianie przestępstw, nawołujące do ich popełniania. Niekiedy szczególnie przydatnym instrumentem, umożliwiającym popełnianie niektórych przestępstw komputerowych okazuje się poczta elektroniczna np. w sytuacji grożenia innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby dla niej najbliższej, jeżeli ta groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona – art. 190 kk. Ponadto do tej kategorii przestępstw zalicza się również określone typy czynów zabronionych, których sposób popełnienia będzie decydował o ich komputerowym charakterze np. przestępstwa określone

[21] R. Kmiecik, *Prawnodowodowe aspekty ochrony programów komputerowych w postępowaniu karnym (problematyka wszczęcia* postępowania*)*, Prokutatura i Prawo 1997, z. 6, s. 7 i podana tam lit.
[22] W obowiązującym od 01.01.1998 r. kodeksie karnym znalazła się liczna grupa przepisów, których zastosowanie, przy spełnieniu ustawowych znamion, ma istotny wpływ dla użytkowników komputerów. Por. przestępstwa stypizowane m. in. w rozdziałach: XXXIII, XXXIV, XXXV kk.
[23] A. Adamski, *Przestępstwa*…, s. 16 – 24.

w rozdziale XXXV kk – nielegalne uzyskanie programu komputerowego (art. 278 § 2 kk), paserstwo programu komputerowego (art. 293 § 1 kk), oszustwo telekomunikacyjne (art. 285 kk), oszustwo komputerowe (art. 287 kk), przestępstwa stypizowane w rozdziale XXXIV kk - fałszerstwo komputerowe (art. 270 § 1 kk), zniszczenie lub pozbawienie mocy dowodowej dokumentu elektronicznego (art. 276 kk), a także inne pozornie nietypowe przestępstwa komputerowe, jak np. uprzywilejowany typ szpiegostwa – art. 130 § 3 kk.

Inaczej natomiast przedstawia się problematyka przestępczości komputerowej w ujęciu karnoprocesowym. Z tego punktu widzenia istotne są te zagadnienia, które wiążą się z koniecznością uzyskania dostępu do systemów informatycznych przez organy ścigania dla wykrycia określonego rodzaju czynów zabronionych przez ustawę pod groźbą kary.

Nietypowość przestępczości komputerowej wymaga odpowiednich regulacji na płaszczyźnie procesowej. Specyfika tego rodzaju przestępstw sprawia, że organy ścigania napotykają na duże trudności natury dowodowej, aby móc ująć sprawcę i wykazać, że dopuścił się zarzucanego mu czynu zabronionego. Ponadto organy te nie zawsze dysponują odpowiednimi urządzeniami, które pozwoliłyby im zastosować nowoczesne metody zwalczania tego rodzaju przestępstw oraz rozpoznać osobę podejrzaną. Nie ułatwia im z pewnością tego zadania, często odmienny od tradycyjnego, sposób działania sprawców, którzy rzadko pozostawiają ślady pozwalające na ich zidentyfikowanie, jak np. odciski palców czy ślady pisma.[24] Poza tym osobami popełniającymi przestępstwa komputerowe są często doskonali fachowcy z zakresu informatyki, którzy dzięki zainstalowaniu w programie np. systemu usuwającego dane po zakończonym działaniu, bez trudu będą zacierać za sobą dowody w sprawie. Charakter przestępczości komputerowej powoduje także szereg wątpliwości przy ustalaniu miejsca popełnienia czynu.[25]

W art. 236a kpk ustawodawca wskazuje, że do danych elektronicznych należy stosować odpowiednio przepisy rozdziału 25 kpk, regulującego czynności dowodowe - zatrzymanie rzeczy oraz przeszukanie.[26] W art. 218a kpk zwraca się zaś uwagę na obowiązek urzędów, instytucji i podmiotów prowadzących działalność telekomunikacyjną zabezpieczenia danych informatycznych, na żądanie sądu lub prokuratora, na czas określony, maksymalnie wynoszący 90 dni. Szczegółowa zaś regulacja związana z wymogami technicznymi stawianymi systemom i sieciom służącym do przekazywania informacji, wymienionych w art. 218b kpk, a także dotycząca sposobów zabezpieczania uzyskanych danych przed ich utratą, zniekształceniem nieuprawnionym

[24] K.J. Jakubski, *Przestępczość komputerowa – zarys problematyki*, Prokuratura i Prawo 1996, nr 12, s. 34 – 36.
[25] J. Dzierżanowska, *Karnoprocesowa problematyka przestępczości komputerowej*, [w:] *Internet 2000 Prawo – Ekonomia – Kultura,* pod red. J. Skupisza, Lublin 2000, s. 286 – 288.
[26] Ustawa kodeks postępowania karnego z dn. 06.06.1997 r., DzU Nr 89, poz. 555 z póź, zm.

ujawnieniem urządzeniom elektronicznym, została zawarta w rozporządzeniach wykonawczych.[27] Nadal jednak wiele wątpliwości wzbudza przepis art. 219 § 1 kpk, określający podstawy prawne przeszukania[28], stanowiący, że można dokonać przeszukania pomieszczeń i innych miejsc, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że osoba podejrzana lub rzeczy mogące stanowić dowód w sprawie lub podlegające zajęciu w postępowaniu karnym tam się znajdują. Jak słusznie zauważa A. Adamski dane, które są dostępne za pośrednictwem terminalu niekoniecznie muszą się znajdować w przeszukiwanym miejscu, lecz np. nawet za granicą. Wówczas zajęcie terminalu w miejscu, na które wskazuje art. 219 § 1 kpk, nie będzie miało większego znaczenia dla toczącego się postępowania.[29] Przy przeprowadzaniu tego rodzaju czynności dowodowej organy ścigania mogą napotkać również na pewne dodatkowe trudności ze strony podejrzanego, który ma prawo odmowy złożenia wyjaśnień. Świadek z kolei może odmówić składania zeznań, gdy np. ujawniona informacja stanowiłaby tajemnicę państwową, służbową czy zawodową lub gdy jest osobą najbliższą dla podejrzanego.

Kodeks postępowania karnego upoważnia także w art. 241 kpk do odpowiedniego stosowania przepisów regulujących kontrolę i utrwalanie rozmów do kontroli i utrwalania rozmów, przekazów informacji przy użyciu środków technicznych, w tym korespondencji przesyłanej pocztą elektroniczną. Zastosowanie podsłuchu komputerowego wymaga spełnienia szeregu przesłanek określonych w rozdziale 26 kpk. Dotyczą one m.in. rodzaju przestępstw, w przypadku których podsłuch może znaleźć zastosowanie, maksymalnego czasu jego trwania, podmiotu uprawnionego do wydania stosownego postanowienia w tym zakresie, etapu postępowania, na którym może być wydane. Zaprezentowane powyżej dwa ujęcia przestępczości komputerowej ani nie wyczerpują, ani też nie zabraniają dokonywania jeszcze innych jej klasyfikacji. Interesujący podział został wypracowany przez Interpol. International Criminal Police Organization przedstawiła w tym zakresie następujące wyodrębnienie: 1) naruszenie praw dostępu do zasobów np. hacking, 2) modyfikację zasobów np. przy pomocy wirusa komputerowego, 3) oszustwo przy wykorzystaniu komputera np. oszustwo bankomatowe, w kasach fiskalnych, 4) powielanie programów np. gry, topografie układów scalonych, 5) sabotaż komputerowy, 6) przechowywanie prawnie zabronionych zbiorów, przestępczość w sieci, przestępstwa dokonywane za pomocą BBS – ów.[30]

Jeszcze inną propozycję podziału przestępstw komputerowych wyróżnił angielski prawnik i znawca w zakresie tematyki nowych technologii P. Sommer: 1) przestępstwa, których dokonanie

[27] P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego, T. I, Komentarz do art. 1 – 296*, pod red. P. Hofmańskiego, Warszawa 2007, s. 1001 i n.
[28] Por. Rozporządzenie Ministra Sprawiedliwości z dn. 28.04.2004 r., DzU Nr 100, poz. 1023, Rozporządzenie Ministra Sprawiedliwości z dn. 24.06.2003 r., DzU Nr 110 poz. 1052.
[29] A. Adamski, *Komputery w paragrafach*, [w:] *Rzeczpospolita* z dn. 30.10.1997 r., nr 254 (4811) s. 16.
[30] Por. B. Fischer, *Przestępczość komputerowa i ochrona informacji. Aspekty prawno – kryminalistyczne,* Kraków 2000, s. 27 - 28.

byłoby niemożliwe bez komputerów – np. hacking, 2) przestępstwa, w odniesieniu do których komputery jedynie ułatwiają ich popełnienie np. fałszowanie przy wprowadzaniu danych, 3) przestępstwa popełniane niezależnie od udziału komputerów np. w zakresie prowadzenia podwójnej księgowości, 4) przestępstwa dokonywane przez zawodowych sprawców, dla których komputer jest narzędziem wspomagającym działalność sprzeczną z prawem – dotyczy to przede wszystkim przestępczości zorganizowanej.[31]

Z przedstawionej analizy wynika, że nie ma jednej i w miarę uniwersalnej definicji przestępczości komputerowej. Pojęcie to jest na tyle wieloznaczne i tym samym nieprecyzyjne, że trudno byłoby sformułować i zaproponować takie ujęcie, które mogłoby znaleźć zastosowanie zarówno na płaszczyźnie prawa karnego materialnego, procesowego, a także na gruncie kryminalistyki oraz kryminologii. Niewątpliwe jest jednak to, że określenie przestępczość komputerowa powinno być kojarzone z systemami komputerowymi, zmienionymi z postaci analogowej na cyfrową informacjami oraz elektronicznym przetwarzaniem danych.[32] Ze względu na ogromny zasięg zastosowania informatyzacji za U. Sieber należałoby stwierdzić, że z punktu widzenia fenomenologii nie ma jednej homogenicznej przestępczości komputerowej.[33]

Do grupy omawianych przestępstw komputerowych, któremu należałoby poświęcić więcej należy wspomniany już wcześniej występek oszustwa komputerowego – art. 287 kk. A. Marek podkreśla, że nazwa tego przestępstwa nie jest do końca trafna, gdyż ta odmiana oszustwa nie odwołuje się do typowych, klasycznych znamion tego typu przestępstwa. W tym bowiem przypadku sprawca ani nie wprowadza w błąd, ani nie wykorzystuje cudzego błędu, lecz tylko ingeruje w urządzenie lub system przeznaczony do gromadzenia, przetwarzania lub przesyłania informacji. Jednocześnie autor ten nie przedstawia żadnej, nowej propozycji terminologicznej.[34]

Przepis art. 287 kk został umieszczony w rozdziale XXXV kodeksu karnego, dla którego przedmiotem ochrony/zamachu jest mienie. Kodeks nie objaśnia jednocześnie czym jest „mienie", poprzestając w art. 115 § 5 i § 6 na rozróżnieniu mienia znacznej i wielkiej wartości. „Mienie" jako termin prawniczy występuje przede wszystkim na obszarze prawa cywilnego. J. Balcerzak zastanawiając się nad ewentualnymi różnicami w rozumieniu tego pojęcia na obszarze prawa karnego i cywilnego, doszedł do wniosku, że normy cywilnoprawne będą w tym wypadku wiążące dla norm prawnokarnych, chyba że te wyraźnie ograniczą ich zastosowanie[35]– jak np. art. 278 obowiązującego kodeksu karnego, w rozumieniu którego przedmiotem przestępstwa kradzieży

[31] Por. B. Fischer, *Przestępczość komputerowa i ochrona…,* s. 25 – 26.
[32] Por. B. Fischer, *Przestępczość komputerowa*, Prawo i Życie 1997, nr 22, s. 3.
[33] U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, Przegląd Policyjny 1995, nr 3, s. 6.
[34] A. Marek, *Kodeks karny. Komentarz*, Kraków 2007, s. 527.
[35] J. Bednarzak, *Przestępstwo oszustwa w polskim prawie karnym*, Warszawa 1971, s. 75.

może być tylko rzecz (mienie) ruchoma. Zgodnie z art. 44 kodeksu cywilnego[36] mienie obejmuje swym zakresem własność i inne prawa majątkowe i będzie - w związku z powyższym - pokrywało się w całości z pojęciem mienia na gruncie przestępstwa oszustwa z art. 286 kk (oszustwo „klasyczne"). Podobnie przyjął SN w jednym ze swych niedawnych orzeczeń. W postanowieniu z 15 czerwca 2007 r. Sąd Najwyższy uznał, że mienie, o którym mowa w art. 286 kk obejmuje całokształt sytuacji majątkowej, zarówno prawa rzeczowe, jak i obligacyjne, zaś niekorzystne nimi rozporządzenie może nastąpić nie tylko przez rzeczywisty uszczerbek, ale również przez utratę należnych korzyści.[37] W orzecznictwie wskazano m. in., że przedmiotem ochrony w świetle art. 286 kk jest każde świadczenie majątkowe.[38]

Poczynione uwagi należy odnieść do przestępstwa oszustwa komputerowego. Również w tym przypadku przyjmuje się, że przedmiotem ochrony jest mienie, choćby ze względu na fakt umieszczenia art. 287 kk w rozdziale XXXV kodeksu karnego, który chroni właśnie to dobro prawne. Specyfika ustawowych znamion oszustwa komputerowego sprawia, że mienie nabiera w tym przepisie nietypowego znaczenia. Będzie ono zatem zbiorczą nazwą dla wszelkich praw majątkowych, dla których dowodem istnienia jest stosowny zapis w systemie gromadzącym, przesyłającym lub przetwarzającym informacje lub zapis na komputerowym nośniku informacji albo mienie, z którym związany jest ten zapis. Przedmiot przestępstwa oszustwa komputerowego jest w istocie bardzo złożony - są nim szczególnego rodzaju informacje, związane ściśle z cudzym mieniem, a także samo mienie.[39] Ochronie podlegają zatem poufność, integralność i dostępność informacji, a także prawa majątkowe, wyrażone w postaci zapisu na odpowiednim nośniku informacji.[40] Z zakresu przedmiotu ochrony wyłączona została natomiast osoba pokrzywdzona przestępstwem z art. 287 kk ze względu na miejsce popełnienia tego występku, jakim jest system informatyczny.[41] Nie można jednakże pomijać faktu, że prawa do mienia przysługują zawsze określonemu podmiotowi. Skoro zatem mienie stanowi przedmiot ochrony, to również związane z nim prawa danej osoby będą korzystały z właściwej im ochrony.[42]

Podobnie jak to ma miejsce w przypadku przedmiotu ochrony/zamachu, wspomnianą złożoność można dostrzec również przy znamieniu czasownikowym, charakteryzującym sposób zachowania sprawcy. Ustawowy opis czynu zabronionego w postaci oszustwa komputerowego

[36] Ustawa kodeks cywilny z dn. 23.04 1964 r., DzU Nr 16 poz. 93 z póź. zm.
[37] Postanowienie SN z dn. 15.06.2007 r., IKZP 13/07, OSNKW 2007, nr 7 – 8, poz. 56.
[38] Wyrok SN z dn. 10.03.2004 r., IV KK 381/03, Prokuratura i Prawo 2004, dodatek - Orzecznictwo SN, SA, NSA i TK, nr 7 – 8, poz. 3.
[39] B. Michalski, [w:] O. Górniok, W. Kozielewicz, E. Pływaczewski, B. Kunicka – Michalska, R. Zawłocki, B. Michalski, J. Skorupka, *Kodeks karny. Część szczególna. T. II. Komentarz do art. 222 – 316*, pod red. A. Wąska, Kraków 2006, s. 1041.
[40] R. Góral, *Kodeks karny. Praktyczny komentarz*, Warszawa 2007, s. 497.
[41] B. Michalski, [w:], *op. cit*., s. 1041
[42] M. Dąbrowska – Kardas, P. Kardas, [w:] A. Barczak – Oplustil, G. Bogdan, Z. Ćwiąkalski, M. Dąbrowska – Kardas, P. Kardas, J. Majewski, J. Raglewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel, A. Zoll, *Kodeks karny. Część szczególna. Komentarz do art. 278 – 363 kk*, pod red. A. Zolla, Kraków 2006, s. 336.

uległ w 2004 r. nowelizacji.[43] Dla zachowania postulatu przejrzystości prawnoporównawczej warto w tym momencie przytoczyć pierwotne i obecne brzmienie art. 287 § 1 kk. Przed nowelizacją art. 287 § 1 kk stanowił: „Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, 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." Po zmianie przepis ten otrzymał brzmienie: „Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5." Powyższa zmiana redakcyjna wiązała się z koniecznością dostosowania polskiego prawa karnego do standardów określonych w Konwencji o cyberprzestrzeni z 28.11.2001 r., która została podpisana również przez Polskę.[44] Z przytoczonego powyżej fragmentu art. 287 kk wynika, że przestępstwo w nim określone można popełnić w jednej z dwóch form ujętych alternatywnie.

Pierwsza z odmian analizowanego występku polega zatem na „wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych". Znamię czynnościowe „wpływa", dla którego wyrażeniem synonimicznym może być oddziałuje, powoduje zmianę w świecie zewnętrznym, dotyczy samoczynnych procesów związanych z informacjami.[45] Próby bliższego wyjaśnienia tego terminu mogą spowodować powstanie wielu wątpliwości interpretacyjnych. Istota owego „wpływania" będzie się sprowadzała do niedozwolonych prawnie ingerencji sprawcy we właściwy przebieg procesów wymienionych a art. 287 kk – tj. automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych, przy czym może ono przybierać bardzo różne formy np. uszkodzenie, niszczenie, czynienie niezdatnym do użytku urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych, wprowadzenie wirusa lub niezgodnych z prawdą danych do systemu informatycznego.[46]

Z kolei kodeksowy zwrot „przetwarzanie danych informatycznych" odnosić należałoby do uzyskania określonych informacji dzięki opracowaniu przy pomocy maszyn cyfrowych znaczącej ilości danych pomiarowych.[47] Legalna definicja przetwarzanie danych została zawarta

[43] Ustawa z dn. 18.03.2004 r. o zmianie ustawy kodeks karny, ustawy kodeks postępowania karnego, ustawy kodeks wykroczeń, DzU Nr 69, poz. 626 (obowiązująca od 01.05.2004 r.).

[44] *Konwencja o cyberprzestrzeni* z dn. 23.11.2001 r. – dostęp na stronie www.interpol.int./Public/TechnologyCrime/Conferences./6.htmlConf/Convention.pdf

[45] *Słownik języka polskiego*, tom III, Warszawa 1984, s. 756, pod red. M. Szymczaka.

[46] M. Dąbrowska – Kardas, P. Kardas, [w:] *op. cit*., s. 341.

[47] B. Michalski, [w:], *op. cit.,* s. 1043.

w ustawie o ochronie danych osobowych.[48] Zgodnie z art. 7 pkt. 2 tej ustawy przetwarzanie danych obejmuje „jakiekolwiek operacje wykonywane na danych osobowych". Jako ich przykłady zostały wymienione następujące procesy: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zwłaszcza zaś te, które wykonuje się w systemach informatycznych. Wskazane w ustawie o ochronie danych osobowych sposoby operacji na tego rodzaju danych można by relacjonować do przetwarzania danych, o których mowa w art. 287 § 1 kk, z tym jednak, że danych, o których mowa w ustawie karnej, nie należy ograniczać do kategorii tylko jednego rodzaju - osobowych. Dane informatyczne, według Konwencji o cyberprzestrzeni – art. 1 lit. b, oznaczają bowiem „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym powodującym wykonanie funkcji przez system informatyczny".[49] Kolejny kodeksowy zwrot - „gromadzenie danych informatycznych" oznacza zebranie, skoncentrowanie danych, przy jednoczesnej dbałości o ich właściwą segregację i uporządkowanie.[50] Ostatnie z określeń w tej części analizowanego przepisu - „przekazywanie danych informatycznych", które zastąpiło, jako bardziej adekwatne, sformułowanie - „przesyłanie informacji" wskazuje na czynność dostarczanie tych danych od nadawcy do odbiorcy, przy zachowaniu wymaganych procedur.[51]

Druga odmiana bezprawnego działania sprawcy oszustwa komputerowego polega, zgodnie z art. 287 § 1 kk in fine, na zmienianiu, usuwaniu albo wprowadzaniu nowego zapisu danych informatycznych. Wspomniana nowelizacja z 18.03.2004 r. rozszerzyła stosowanie tego przepisu. W pierwotnym brzmieniu ograniczał on bowiem czynności wykonawcze tylko do zmiany, usuwania albo wprowadzania nowego zapisu na komputerowym nośniku informacji. Obecne sformułowanie pozwala na objęcie penalizacją działań sprawcy niezależnie od rodzaju nośnika, na którym dane utrwalono. Wymieniony w ustawie sposób przestępnego działania, polegający na zmienianiu danych informatycznych polega na dokonaniu ingerencji w zakresie treści istniejącego już zapisu np. na CD, DVD czy twardym dysku komputera. Zmiana taka oznaczać będzie modyfikację istniejącego zapisu, w postaci np. dodania treści czy częściowego jej usunięcia. Z kolei całkowite usunięcie zapisu prowadzi do jego likwidacji, która może mieć charakter zarówno trwały, jak i odwracalny.[52]

Zarówno pierwsza jak i druga forma oszustwa charakteryzują się tym, że sprawca tego przestępstwa realizuje swe czynności „bez upoważnienia", czyli w sposób bezprawny. Za szeroką

[48] Ustawa o ochronie danych osobowych, z dn. 29.08. 1997 r., DzU Nr 133 poz. 883, z póź. zm.
[49] *Konwencja o cyberprzestrzeni* z dn. 23.11.2001 r. – dostęp na stronie www.interpol.int./Public/TechnologyCrime/Conferences./6.htmlConf/Convention.pdf
[50] B. Michalski, [w:], *op. cit.,* s. 1043.
[51] M. Dąbrowska – Kardas, P. Kardas, [w:] *op. cit*., s. 343.
[52] *Ibidem,* s. 344.

interpretacją tego znamienia opowiada się P. Kardas. O prawidłowym jego znaczeniu muszą decydować zarówno elementy obiektywne, jak i subiektywne. Ujęcie obiektywne sugerowałoby jedynie na działanie sprawcy bez należytego umocowania. Natomiast podejście subiektywne wymagałoby spełnienia dwóch przesłanek: brak umocowania oraz celu w podejmowanych czynnościach, jakim jest wprowadzenie w błąd urządzenia cyfrowego.[53]

W odniesieniu do wspomnianych powyżej rodzajów oszustwa komputerowego istnieją poważne rozbieżności w doktrynie w zakresie ustalenia skutkowości lub bezskutkowości tego występku. A. Adamski opowiada się za formalnym charakterem tego przestępstwa. Oznacza to, że penalizowane jest już samo zachowanie sprawcy, czyli wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych, jak również zmienianie, usuwanie albo wprowadzanie nowego zapisu danych informatycznych, niezależnie od wystąpienia skutku w postaci uzyskania korzyści majątkowej lub wyrządzenia szkody innej osobie.[54] Taki pogląd prezentują także R. Góral,[55] R. Korczyński oraz R. Koszut.[56] Zupełnie przeciwnego zdania są P. Kardas i M. Dąbrowska – Kardas, którzy twierdzą, że występek z art. 287 kk w obydwu odmianach jest przestępstwem materialnym. Do jego znamion należy skutek w postaci wpływu na procesy wymienione w art. 287 kk. Znamię skutku nie musi ograniczać się bowiem tylko do określonej zmiany w świecie zewnętrznym np. spowodowania szkody majątkowej, lecz obejmuje każdą zmianę, jaka może wiązać się z zachowaniem sprawcy, gdy urzeczywistnia on jedną z alternatywnie wymienionych czynności wykonawczych.[57] Jeszcze inną propozycję rozstrzygnięcia charakteru prawnego oszustwa komputerowego proponuje B. Michalski. Wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych zostało uznane za odmianę przestępstwa formalnego, do którego dokonania nie jest wymagane zakłócenie przebiegu tych procesów. Natomiast oszustwo z art. 287 kk, penalizowane jako wprowadzanie nowego zapisu danych informatycznych, jest traktowane jako występek materialny, którego skutkiem jest faktyczne dokonanie „nowego zapisu danych informatycznych".[58] Istniejące wątpliwości co do charakteru prawnego omawianego przestępstwa powinny doczekać się szybkiego i jednoznacznego rozstrzygnięcia w orzecznictwie Sądu Najwyższego.

W ramach przestępstwa oszustwa komputerowego dotychczasowa praktyka wyróżnia trzy rodzaje manipulacji: 1) manipulację danymi, 2) manipulację programem oraz 3) manipulację wynikiem. Pierwsze ze wspomnianych zachowań polega na wprowadzeniu do bazy danych

[53] P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, Przegląd Sądowy 2000, nr 11 – 12, s. 60.
[54] A. Adamski, *Prawo*…, s. 116.
[55] R. Góral, *op. cit*., s. 497.
[56] R. Korczyński, R. Koszut, *„Oszustwo" komputerowe,* Prokuratura i Prawo 2002, nr 2, s. 35.
[57] J. Giezek, N. Kłączyńska, G. Łabuda, *Kodeks karny. Część ogólna,* pod red. J. Giezka, Warszawa 2007, s. 43.
[58] B. Michalski, [w:], *op. cit.,* s. 1048 – 1049.

nieprawdziwych informacji, dla uzyskania nienależnych korzyści. Przykładem takich operacji mogą być: doprowadzenie do upadku firmy, podawanie nieprawdziwych informacji o świadczeniobiorcach. Manipulacja programem obejmuje działania polegające na wprowadzaniu nowych bądź przekształcaniu istniejących poleceń programowych, które spowodują samoczynne wykonywanie zadań, na które nie będzie miał wpływu operator np. prowadzenie tzw. podwójnej księgowości. Ostania z przedstawionych manipulacji oznacza manipulację urządzeniami peryferyjno – systemowymi oraz urządzeniami wejścia – wyjścia np. wyłudzenie wypłaty gotówki z bankomatu przy pomocy skradzionej karty magnetycznej.[59]

Występek oszustwa komputerowego może być popełniony przez każdy podmiot zdolny do ponoszenia odpowiedzialności karnej. W świetle przepisów kodeksu karnego wymaga się w tym zakresie, co do zasady, ukończenia 17 lat oraz poczytalności, czyli takiego stanu psychicznego sprawcy, który pozwala mu rozpoznać znaczenie czynu oraz znaczenie normy prawnej, którą tym czynem narusza. Przestępstwo z art. 287 kk należy do grupy przestępstw ogólnosprawczych, czyli powszechnych, określanych łacińskim terminem delicta communia.[60] Płynie stąd wniosek, że znamię normatywne, wskazujące na osobę sprawcy działającego „bez upoważnienia", nie świadczy zatem o tym, że występku z art. 287 kk może dopuścić się tylko podmiot o określonych właściwościach (intraneus – w tym przypadku działający bez umocowania). Określenie to bowiem nie ma na celu wyszczególniania cech, jakimi powinien charakteryzować się sprawca, lecz jest elementem należącym do znamion strony przedmiotowej oszustwa komputerowego.[61]

Przestępczość komputerowa będzie wymagała jednak od osób aktywnie w niej uczestniczących i pragnących tym samym uzyskać określonego rodzaju nienależną korzyść jeszcze jednej, dodatkowej zdolności. Nie ulega bowiem wątpliwości, że sprawcy tego rodzaju przestępstw muszą wykazywać się doskonałą znajomości technik informacyjnych oraz nieprzeciętną sprawnością intelektualną. O powodzeniu i zamierzonej efektywności działań oszukańczych będzie decydował przede wszystkim wysoki poziom wiedzy teoretycznej, a także znajomość praktyczna funkcjonowania systemów informatycznych. Oszustem komputerowym nie może być zatem osoba przypadkowa, lecz tylko taka, która posiada specjalistyczne kwalifikacje w zakresie informatyki. Sprawcy występku z art. 287 kk, w przeciwieństwie do podmiotu przestępstwa z art. 286 kk, czyli klasycznego oszustwa, nie będzie potrzebna jakakolwiek wiedza psychologiczna, pozwalająca mu poznać słabości ludzkiego charakteru. Oszust komputerowy nie wprowadza bowiem w błąd innej osoby, nie wyzyskuje jej błędu ani niezdolności do należytego pojmowania przedsiębranego działania, jak to ma miejsce w przypadku występku z art. 286 kk. Jego zadanie może okazać się

[59] A. Adamski, *Prawo*…, s. 119 - 120.
[60] A. Marek, *Prawo karne*, Warszawa 2007, s. 102.
[61] M. Dąbrowska – Kardas, P. Kardas, [w:], *op. cit*., s. 337.

w danym przypadku trudniejsze. Musi on bowiem zmierzyć się ze skomplikowanymi urządzeniami i procesami technologicznymi, a nie z psychiką ludzką, którą być może łatwiej byłoby mu podstępnie podejść i oszukać.[62]

Występek oszustwa komputerowego znalazł się także na liście przestępstw, których popełnienie przez osobę fizyczną uzasadnia odpowiedzialność podmiotów zbiorowych w rozumieniu ustawy z dn. 28.10.2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary - art. 16 ust. 1 pkt 6 cytowanej ustawy.[63]

Warunkiem sine qua non odpowiedzialności karnej sprawcy na podstawie art. 287 kk jest także ustalenie celu jego działania. Ustawodawca wskazał na dwa alternatywnie występujące motywy działania: osiągnięcie korzyści majątkowej lub wyrządzenie innej osobie szkody. W literaturze pojawił się pogląd, że takie ujęcie może wskazywać na dwie odmiany tego występku. Przyjmując to założenie, należałoby stwierdzić, że z typowym oszustwem komputerowym mamy do czynienia wtedy, gdy sprawca działa w celu osiągnięcia korzyści majątkowej. Natomiast, gdy sprawca zmierzałby do wyrządzenia innej osobie szkody, jego czyn zakwalifikowano by wówczas jako szkodnictwo komputerowe.[64]

Oszustwo komputerowe, jako typ występku umyślnego, stanowi przykład tzw. przestępstwa kierunkowego. Sprawca bowiem działa w ściśle określonym celu (dolus directus coloratus). Jednym z nich jest w świetle art. 287 kk osiągnięcie wspomnianej korzyści majątkowej. Zamiar uzyskania tego rodzaju korzyści – animus lucri faciendi, należy odróżnić od zamiaru posiadania rzeczy dla siebie – animus rem sibi habendi. Ich rozróżnienie pozwala na wskazanie odmienności, jakie charakteryzują przestępstwo oszustwa, także komputerowego, od innych przestępstw przeciwko mieniu. Animus rem sibi habendi dotyczyć może tylko substancji mienia oraz prawa własności i realizuje się poprzez objęcie fizycznego władztwa nad rzeczą albo przez jego wykonanie w stosunku do rzeczy ruchomej, którą sprawca włada. Zamiar przywłaszczenia jest zamiarem, który obejmuje przywłaszczenie wyłącznie dla siebie, niezależnie od tego czy sprawca chce ukraść cudzą rzecz np. dla kogoś innego. Z powyższego wynika, że zamiar sprawcy powinien objąć także pośrednictwo w zakresie przejścia władania rzeczą na kolejną osobę. Inaczej przedstawia się sytuacja przy zamiarze przysporzenia korzyści. Zamiar ten może dotyczyć także innych niż własność praw majątkowych. Jeżeli spodziewana korzyść majątkowa ma przypaść innej osobie niż sprawca, wówczas nie występuje on w tym przypadku w roli pośrednika, gdyż w dokonanie czynu zostaje włączona osoba, która według sprawcy ma wydać dyspozycję majątkową. Taka sytuacja nie

[62] E. Jakimiuk, J. Zając, *op. cit*., s. 49 – 50.
[63] DzU z 2002 r. Nr 197, poz. 1661 z póź. zm.
[64] S. Łagodziński, *Przestępstwa przeciwko mieniu w kodeksie karnym (wybrane zagadnienia),* Prokuratura i Prawo 1999, nr 2, s. 16 -17.

może mieć oczywiście miejsca np. przy kradzieży. Przy animus rem sibi habendi zamiar sprawcy dotyczy różnicy między szkodą a uzyskanym bądź spodziewanym przysporzeniem. Natomiast animus lucri faciendi może obejmować korzyść mniejszej wartości od spodziewanej straty.[65] Również SN w wyroku z dn. 21.08. 2002 r. uznał, że korzyść majątkowa w ujęciu art. 286 kk jest „(…) pojęciem szerszym niż przywłaszczenie, zagarnięcie mienia, stanowiącego cel działania sprawcy - animus rem sibi habendi".[66]

Wyjaśnieniu ustawowego zwrotu „korzyść majątkowa" obowiązujący kodeks karny nie poświęca zbyt wiele uwagi. Kodeksowe objaśnienie wyrażeń ustawowych wskazuje w art. 115 § 4, że korzyścią majątkową jest korzyść dla siebie, jak i dla kogo innego. Takie mało precyzyjne określenie funkcjonowało także pod rządami poprzednio obowiązującego kodeksu karnego z 1969 r. Ustawodawca nie definiuje zatem w dalszym ciągu tego pojęcia, dokonując jedynie podziału korzyści majątkowej - korzyść dla siebie lub dla kogoś innego. Korzyść majątkową, jak wynika z samej nazwy, charakteryzuje określona wartość ekonomiczną bądź cel, którym będzie zaspokajanie określonej potrzeby materialnej.[67] Niekiedy te kryteria mogą okazać się niewystarczające dla odróżnienia korzyści majątkowej od korzyści niematerialnej. A. Spotowski zaproponował jeszcze dodatkowe kryterium, zakładające, że o rodzaju korzyści decydować może w trudnych przypadkach stopień zaspokojenia potrzeb przez każdą z nich. Przy tak postawionej tezie, należałoby przyjąć, że w sytuacji, gdy korzyść zaspokaja w większym stopniu potrzebę materialną, a w mniejszym potrzebę niematerialną, to w rozumieniu przepisów prawnokarnych stanowi ona korzyść majątkową.[68]

Zgodzić się można natomiast ze stwierdzeniem, że przybierająca różne postacie korzyść majątkowa wyraża się albo w zwiększeniu aktywów, albo w zmniejszeniu pasywów. W zakresie sposobów jej uzyskania wymienia się przy tym np. przeniesienie prawa majątkowego, wejście w posiadanie rzeczy czy uzyskanie dowodu uiszczenia długu.[69]

Działanie sprawcy w celu osiągnięcia korzyści majątkowej nie jest tożsame z podejmowaniem czynności mających spowodować wyrządzenie szkody innej osobie. Nie można wykluczyć jednak przypadku, że osiągnięciu korzyści majątkowej przez sprawcę będzie towarzyszyło wyrządzenie szkody innemu podmiotowi i odwrotnie.[70] Niemniej jednak ustawowe znamię, mówiące o wyrządzeniu innej osobie szkody, informuje o kierunkowym sposobie działania

[65] J. Bednarzak, *op. cit*., s. 97 – 100.
[66] Wyrok SN z dn. 21.08.2002 r. sygn. III K.K. 230/02, Prokuratura i Prawo. Dodatek orzecznictwo Sądu Najwyższego, Sądów Apelacyjnych, Naczelnego Sądu Administracyjnego i Trybunału Konstytucyjnego 2003, nr 3, poz. 12
[67] J. Giezek, N. Kłączyńska, G. Łabuda, *op. cit*., s. 714.
[68] A. Spotowski, *Przestępstwa służbowe*, Warszawa 1972, s. 131.
[69] T. Oczkowski, *Oszustwo jako przestępstwo majątkowe i gospodarcze*, Kraków 2004, s. 30.
[70] Por. P. Kardas, *op. cit.,* s. 74, S. Łagodziński, *op. cit.,* s. 16.

sprawcy. Podobnie jak to ma miejsce w przypadku korzyści majątkowej, również ten termin nie został bliżej określony przez ustawodawcę. Kodeks karny poprzestaje tylko na wyróżnieniu dwóch rodzajów szkód – „znacznej szkody" oraz „szkody w wielkich rozmiarach", odsyłając jednocześnie w art. 115 § 7 do odpowiedniego stosowania w tym zakresie przepisów określających pojęcia: „mienie znacznej wartości" oraz „mienie wielkiej wartości". Zagadnieniem szkody szeroko zajmują się nauki cywilnoprawne, wyróżniając w tym zakresie szkodę na osobie oraz szkodę w mieniu, dzieląc jednocześnie tę ostatnią na szkodę majątkową i niemajątkową. Pod pojęciem szkody w świetle art. 287 kk należy oczywiście rozumieć szkodę majątkową. A. Adamski opowiada się za jej szerokim ujęciem. Według poglądu tego autora szkoda, którą ustawodawca eksponuje w kontekście przestępstwa oszustwa komputerowego, obejmuje zarówno rzeczywisty uszczerbek – damnum emergens np. koszty odtworzenia utraconych danych, jak i realne, oczekiwane, a utracone korzyści – lucrum cesans np. utracona premia za nieterminowo wykonaną transakcję.[71]

Przedstawiony powyżej typ przestępstwa oszustwa komputerowego może występować nie tylko w postaci podstawowej – art. 287 § 1. Ustawodawca wyróżnił jego typ uprzywilejowany – art. 287 § 2, jak również kwalifikowany – art. 294§ 1 w zw. z art. 287 § 1.

Okolicznością powodującą uprzywilejowanie sprawcy jest wskazany w art. 287 § 2 „wypadek mniejszej wagi". Dla sytuacji określonej w tym paragrafie inaczej kształtuje się ustawowe zagrożenie sankcją karną dla sprawcy. Nie będzie to już kara pozbawienia wolności w wymiarze od 3 miesięcy do lat 5, jak to przewidziano w art. 287 § 1, ale grzywna, kara ograniczenia wolności albo pozbawienia wolności do roku. Sędzia korzysta zatem z większej swobody w zakresie doboru kary, która jest dodatkowo łagodniejsza dla sprawcy.

Zakwalifikowanie oszustwa komputerowego jako „wypadku mniejszej wagi" nie wyłącza zatem odpowiedzialności karnej sprawcy, lecz jedynie wpływa na wymiar kary. Istnieją jednakże poważne trudności, które pozwalałyby ustalić kiedy następuje spełnienie omawianej przesłanki. Ustawodawca zaniechał wskazania okoliczności, które przemawiałyby za przyjęciem tej konstrukcji. Stosownej regulacji, o treści podobnej np. do art. 115 § 2, wskazującego kwantyfikatory stopnia społecznej szkodliwości czynu, nie można odnaleźć zarówno w części ogólnej, jak i szczególnej kodeksu karnego. W tym kontekście warto zwrócić uwagę na wyrok Sądu Najwyższego z 06.02.1973 r., jaki zapadł pod rządami kodeksu karnego z 1969 r., który także nie objaśniał „wypadku mniejszej wagi". Organ ten przyznał, że : „Kodeks karny nie zawiera definicji „wypadku mniejszej wagi", pozostawiając określenie tego pojęcia doktrynie i orzecznictwu." W tym samym orzeczeniu SN wskazał, że „Według ustalonych w dotychczasowym orzecznictwie poglądów o uznaniu konkretnego czynu za „wypadku mniejszej wagi" decydują zarówno elementy

[71] A. Adamski, *Prawo…,* s. 117 – 118.

przedmiotowe, jak i podmiotowe, a więc także dotyczące osoby sprawcy, przedsiębranego przez niego sposobu działania, rodzaju winy i stopnia napięcia złej woli”.[72]

Jednakże biorąc pod uwagę dorobek doktryny prawa karnego oraz orzecznictwa, nie można poprzestać na tym orzeczeniu SN. Na uwagę zasługują co najmniej cztery stanowiska, które przyjmowały różne kryteria kwalifikujące „wypadek mniejszej wagi”.[73]

Najstarsza koncepcja wskazywała, że o wypadku mniejszej wagi decydują kryteria stosowane przy wymiarze kary. Sędzia zatem według swoje uznania przyjmował kwalifikację prawną czynu jako „wypadek mniejszej wagi”. Okolicznościami pozwalającymi przyjąć tę konstrukcję prawną były zarówno elementy podmiotowe, jak i przedmiotowe czynu, które łącznie i z osobna uzasadniały, że sprawca zasługuje na łagodniejsze potraktowanie. Wskazywano także, że na przyjęciu „wypadku mniejszej wagi” maja wpływ okoliczności dotyczące sprawcy, m.in. właściwości i warunki osobiste, dotychczasowy sposób życia, zachowanie się po popełnieniu przestępstwa.[74]

Drugie stanowisko łączyło „wypadek mniejszej wagi” ze szczegółową analizą przedmiotu ochrony oraz strony przedmiotowej. Za taką koncepcją opowiedział się SN w wyroku z 29.08.1978 r. „(…) przy ocenie znamienia „wypadek mniejszej wagi” decydują przede wszystkim okoliczności związane z przedmiotem ochrony i stroną przedmiotową czynu, a więc głównie wysokość wyrządzonej w mieniu społecznym szkody, a także okoliczności popełnienia czynu”.[75]

Trzecia koncepcja kładła akcent zarówno na stronę przedmiotową, podmiotową, jak również na czynniki związane z osobowością sprawcy.[76]

Z kolei czwarta koncepcja, która jest uważana za najbardziej trafną, opiera się na kryterium przedmiotowo – podmiotowym. Elementami podmiotowymi są przede wszystkim motywacja, cel działania sprawcy, zamiar lub jego brak. Natomiast elementy przedmiotowe nawiązują do np. zagrożonego dobra, wyrządzonej lub zagrażającej szkody, sposobu działania sprawcy. Wskazane kwantyfikatory, związane ściśle z popełnionym czynem zabronionym, pozwalają najlepiej uznać i ocenić go w kategorii „wypadku mniejszej wagi”. Tak też uznał SN w wyroku z dn. 15.07.1972 r. „Wypadek mniejszej wagi określają przesłanki dotyczące zarówno przedmiotowej, jak i podmiotowej strony czynu.”[77] Tą ostatnią koncepcję należałoby zastosować do art. 287 § 2 kk. W odniesieniu do tego przestępstwa szczególnie istotne znaczenie, pozwalające na zakwalifikowanie go jako „wypadku mniejszej wagi” będzie miała ocena celu działania sprawcy.

[72] Wyrok SN z dn. 06.02.1973 r., OSKW 1973, nr 9, poz. 112.
[73] R.A. Stefański, *Okoliczności uzasadniające przyjęcie „wypadku mniejszej wagi*”, Prokuratura i Prawo 1996, nr 12, s. 125.
[74] W. Świda, *Prawo karne*, Warszawa 1989, s. 436, F. Majewski, *Przestępstwa przeciwko mieniu w nowym kodeksie karnym*, Państwo i Prawo 1969, nr 8 – 9, s. 348.
[75] Wyrok SN z dn. 29.08.1978 r., OSKW 1978, nr 12, poz. 142.
[76] A. Zelga, *Wypadek mniejszej wagi w kodeksie karnym*, Palestra 1972, nr 1, s. 58 – 67.
[77] Wyrok SN z dn. 15.07. 1972 r., OSNKW 1971, nr 11, poz. 163.

Jeżeli motywem działania sprawcy była chęć uzyskania bezprawnej korzyści, wówczas podstawowe znaczenie będzie miało określenie jej wysokości. Natomiast, gdy sprawca zmierzał swoim sprzecznym z prawem działaniem do wyrządzenia innej osobie szkody, wtedy pod uwagę należy brać w pierwszej kolejności jej wysokość, rozmiar oraz rodzaj.[78]

Ustawodawca obok uprzywilejowanego typu występku oszustwa komputerowego wskazał także na jego kwalifikowaną postać. Art. 294 § 1 i § 2 kk zbiorczo reguluje kwalifikowane odmiany niektórych przestępstw przeciwko mieniu, przyjmując za podstawę wyróżnienia: albo sytuację, gdy przedmiotem przestępstwa jest mienie znacznej wartości, albo przypadek, kiedy czynu dopuszczono się w stosunku do dobra o szczególnym znaczeniu dla kultury.

Pojęcie „mienia znacznej wartości" dzięki ustawowej definicji nie budzi wątpliwości. Z art. 115 § 5 wynika, że jest to mienie, którego wartość w chwili popełnienia czynu zabronionego przekracza dwustukrotność najniższego miesięcznego wynagrodzenia. Wysokość minimalnego wynagrodzenia za pracę określa ustawa z 10.10.2002 r. o minimalnym wynagrodzeniu za pracę. W 2009 r. wynosi ono 1 279 zł.[79]

Druga okoliczność powodującą zaostrzenie wymiaru kary dla sprawcy w kontekście art. 294 § 2 wymaga odwołania się do przepisów ustawy z 15.02.1962 r. o ochronie dóbr kultury i o muzeach.[80] Art. 2 tej ustawy stanowi, że dobrem kultury jest każdy przedmiot ruchomy lub nieruchomy, dawny lub współczesny, mający znaczenie dla dziedzictwa i rozwoju kulturalnego ze względu na wartość historyczną, naukową lub artystyczną. Za dobro kultury uznawane są także zabytki. Ustawa nie definiuje natomiast pojęcia „dobra o szczególnym znaczeniu dla kultury". Powyższe wyrażenie może sugerować, że ustawodawca wyeksponował w ten sposób przedmioty szczególnie cenne, o wyjątkowym charakterze.

Konkludując należałoby stwierdzić, że powszechny dostęp do Internetu, obok swych licznych walorów, umożliwił doskonałe warunki rozwoju przestępczości komputerowej. Ten uboczny skutek informatyzacji powoduje, że wzrastająca liczba uczestników sieci komputerowej przekłada się na coraz większą liczbę popełnianych przestępstw i osób nimi pokrzywdzonych. Internetowa anonimowość sprawiła, że potencjalni sprawcy czują się niemal bezkarni, zaś ich ofiary często bezradne.[81]

Przestępczość komputerowa w dobie gwałtownego rozwoju technik informatycznych stanowi w dalszym ciągu jedno z najgroźniejszych zjawisk. Ważnym wydaje się obok zwalczania

[78] B. Michalski, [w:], *op. cit*., s. 1048.
[79] Ustawa o minimalnym wynagrodzeniu za pracę, z dn. 10.10.2002 r., DzU Nr 16, poz. 79 z póź. zm. Wysokość precyzuje wydane na podstawie ustawy obwieszczenie Prezesa Rady Ministrów w sprawie wysokości minimalnego wynagrodzenia za pracę – MP nr 55, poz. 499.
[80] Ustawa o ochronie dóbr kultury i o muzeach z dn. 15.02.1962 r., DzU z 1999 r., Nr 98, poz. 1150 z póź. zm.
[81] M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, Czasopismo Prawa Karnego i Nauk Penalnych 2000, z. 1, s. 24.

tego procederu, także właściwa profilaktyka, obejmująca politykę zabezpieczeń systemów komputerowych przed możliwymi zagrożeniami. Niemniej istotna jest również świadomość obecności tych niebezpieczeństw przez osoby korzystające z osiągnięć współczesnej informatyki, jak również znajomość czynników im sprzyjających, która nabiera szczególnego znaczenia w przypadku oszustwa komputerowego. Cyberprzestrzeń stworzyła bowiem nieograniczoną możliwość dokonywania oszustw, które integralnie są połączone z hackingiem.[82] Wychodząc zatem naprzeciw obawom przed rozprzestrzenianiem się nieuczciwych działań oszustów komputerowych, ustawodawca słusznie objął kryminalizacją tego rodzaju praktyki. Z danych statystycznych, udostępnionych na stronie internetowej Komendy Głównej Policji wynika, że art. 287 kk, nie pozostaje tzw. martwą literą prawa.[83]

[82] Por. B. Kunicka – Michalska, *Oszustwo komputerowe. Regulacje prawa polskiego*, Studia Prawnicze 2006, z. 4, s. 106, M. Kliś, *op. cit.* s. 10 – 11.
[83] Informacje dostępne na oficjalnej stronie internetowej Komendy Głównej Policji – *www. policja. pl.* Przedstawiona tam statystyka ilustruje liczbę popełnionych występków oszustwa komputerowego: 1999 r. – 217, 2000 r. – 323, 2001 r. – 279, 2002 r. – 368, 2003 r. – 168, 2004 r. – 390, 2005 r. – 568, 2006 r. – 444, 2007 r. – 492.