ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ Nr 280
Zarządzanie i Marketing z. 18 (2/2011) 2011

Bogumiła Zofia LUBERA[1]
Agnieszka SIKORSKA[2]

OSZUSTWO A OSZUSTWO KOMPUTEROWE – WYBRANE ASPEKTY

Dynamiczny rozwój Internetu oraz infrastruktury informatycznej na świecie ma obecnie ogromny wpływ na niemalże każdą dziedzinę naszej aktywności. Sieć internetowa oraz nowoczesna technologia może posłużyć jako środek lub cel w działalności przestępczej. Niniejszy artykuł jest próbą syntezy wybranych aspektów prawnych z zakresu przestępstwa oszustwa i oszustwa komputerowego.

1. WPROWADZENIE

Rewolucja spowodowana umasowieniem technologii informatycznych, wywierających największy wpływ na społeczeństwo XXI wieku i jego rozwój, jak niemal każde zjawisko społeczne ma także negatywne oblicze. Technika cyfrowa oraz przestrzeń wirtualna stały się narzędziem w procederze łamania prawa. Wraz z rozwojem Internetu i masowej komunikacji elektronicznej braki odpowiednich regulacji prawnych zauważyli i wykorzystali zarówno zwykli użytkownicy Internetu, których skusiła łatwość zdobycia cyfrowo przetworzonych dóbr, jak też świat przestępczy[3].

W latach 70 i 80 ubiegłego wieku problem skutków ubocznych komputeryzacji, w tym nadużywania technologii informatycznych dla celów sprzecznych z prawem nie angażował szczególnej uwagi organizacji rządowych czy międzynarodowych. Problemy związane z komputeryzacją były wówczas postrzegane raczej w skali lokalnej niż międzynarodowej. Dopiero lata 90 przyniosły zmianę podejścia do problemu nadużyć komputerowych[4]. Masowy charakter tego zjawiska z biegiem lat stawał się bardziej powszechny i zyskał miano przestępstw komputerowych. Różnorodność zachowań patologicznych, jakie składają się na termin „przestępczości komputerowej", powoduje brak jednolitej definicji tego rodzaju działań przestępczych. W znaczeniu *sensu largo* obejmują one kategorię czynów związanych z funkcjonowaniem elektronicznego gromadzenia, przetwarzania oraz przesyłania informacji, polegających zarówno na naruszeniu uprawnień do programu komputerowego, jak również na bezprawnej ingerencji w gromadzoną, przetwarzaną lub przesyłaną informację, w nośnik tychże

---

[1] Mgr Bogumiła Zofia Lubera – doktorantka na Wydziale Prawa i Administracji, Katedra Prawa Karnego i Kryminologii, Uniwersytet Śląski.

[2] Mgr Agnieszka Sikorska – doktorantka na Wydziale Prawa i Administracji, Katedra Prawa Karnego i Kryminologii, Uniwersytet Śląski

[3] R. Tarnogórski, *Konwencja o cyberprzestępczości – międzynarodowa odpowiedź na przestępczość ery informacyjnej*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, pod red. M. Madeja, M. Terlikowski, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 205.

[4] K.J. Jakubski, *Przestępczość komputerowa- zarys problematyki*, „Prokuratura i Prawo", nr 12, 1996, s. 34.

informacji oraz systemy połączeń komputerowych[5]. Przy tego rodzaju przestępczości niezgodne z prawem nadużywanie technologii informatycznych może zostać popełnione przy użyciu elektronicznych systemów gromadzenia, przetwarzania lub przesyłania danych informatycznych oraz być skierowane przeciwko tym systemom. Komputer i Internet może wobec tego stanowić narzędzie przestępstwa, które zostało użyte do jego popełnienia, jak również być celem popełnienia czynu zabronionego. Obecnie względem przestępstw komputerowych stosowana jest terminologia „cyberprzestępstwa" bądź „przestępstwa internetowe"[6].

2. WPŁYW PRAWA MIĘDZYNARODOWEGO NA USTAWODAWSTWO KRAJOWE WZGLĘDEM OSZUSTWA KOMPUTEROWEGO

Podmiotem, który zajął się analizą zjawiska cyberprzestępczości w latach 1985–1989, był Komitet Ekspertów Rady Europy. W 1995 r. powstał pierwszy dokument[7] uwzględniający zagadnienia procesowe związane z technologią informacyjną, z kolei przedstawiony w 1989 r. raport stał się podstawą Zalecenia Nr R(89)9 Komitetu Ministrów Rady Europy[8]. Wyróżniono w nim zachowania przestępcze związane z wykorzystaniem komputera i systemu komputerowego. Dokument ten wzywał rządy krajów członkowskich do uwzględnienia w trakcie prowadzonych prac legislacyjnych w ustawodawstwie wewnętrznym wskazań sformułowanych przez Komitet Ekspertów oraz do poinformowania w 1993 r. Sekretarza Generalnego Rady Europy o wszelkich zmianach ustawodawczych, praktyce sądowej i doświadczeniach, związanych z prawną współpracą międzynarodową w zakresie przestępczości komputerowej[9]. Jednocześnie statuował on dwie listy, minimalną i fakultatywną, zachowań, podlegających kryminalizacji. Na liście minimalnej znalazły się przestępstwa komputerowe, które wymagały kryminalizacji w systemach prawnych państw członkowskich Rady Europy. Zaliczono do nich poszczególne kategorie czynów: oszustwo związane z wykorzystaniem komputera (tzw. oszustwo komputerowe), fałszerstwo komputerowe, zniszczenie danych lub programów komputerowych, sabotaż komputerowy, włamanie do systemu komputerowego przez osobę nieuprawnioną, podsłuch komputerowy, bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych (tzw. piractwo komputerowe) oraz bezprawne kopiowanie topografii półprzewodników. Lista ta zawierała zalecenie ujednolicenia ustawodawstw poszczególnych krajów, co miało wpłynąć na wzajemną współpracę w zakresie ścigania transgranicznych przestępstw. Natomiast lista fakultatywna wskazywała na zachowania

---

[5] Zob. B. Michalski, *Przestępstwa przeciwko mieniu*, [w:] *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316*, t. II, pod red. A. Wąsek, Wydawnictwo C.H. Beck, Warszawa 2006, s. 1039-1340.

[6] Zob. szerzej A. Adamski, *Prawo karne komputerowe*, Wydawnictwo C.H. Beck, Warszawa 2000, s. 30-34 i cytowana tam literatura.

[7] Zalecenie Nr R(95)13 *Problems of Criminal Procedural Law Connected with Information Technology* przyjęte przez Komitet Ministrów Rady Europy 11 września 1995 r.

[8] Czytaj dalej – Komitet RE, Zalecenie Komitetu Ministrów RE *Computer – Related Crime* i końcowe sprawozdanie Komitetu Problemów Przestępczości Rady Europy, Strasbourg 1989 r.

[9] A. Adamski, *Przestępstwa komputerowe w projekcie kodeksu karnego na tle europejskich standardów normatywnych*, [w:] *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z międzynarodowej konferencji naukowej – Legal aspects of computer-related abuse. Procedings of the International Conference. (Poznań 20-22 April 1994)*, pod red. A. Adamski, Toruń 1994, s. 142-143.

o mniejszym stopniu szkodliwości, które nie wymagały już ścisłej współpracy międzynarodowej w zakresie ich ścigania i jurysdykcji[10]. Znalazły się na niej: modyfikacja danych lub programów komputerowych, szpiegostwo komputerowe, używanie komputera bez zezwolenia, a także używanie prawnie chronionego programu komputerowego bez upoważnienia[11]. W ustawodawstwie polskim, jeszcze przed wejściem w życie ustawy karnej z 1997 r., zmiany uwzględniające zalecenia Komitetu RE znalazły po części odzwierciedlenie w pracach nad projektem kodeksu karnego. Przestępczość komputerowa, ze względu na przedmiot ochrony, została usankcjonowana w poszczególnych rozdziałach m.in. w rozdziale przestępstw przeciwko bezpieczeństwu powszechnemu, przeciwko ochronie informacji oraz przeciwko mieniu. Komisja ds. reformy prawa karnego zaleciła również stworzenie odrębnej regulacji względem przepisów dotyczących ochrony sfery prywatności, odnoszącej się do zakresu danych, ich gromadzenia oraz korzystania z nich bądź dostępu nieuprawnionego[12]. Ponadto z uwagi na zobowiązania, wynikające z potrzeby harmonizacji prawa polskiego względem europejskiego, wskazane na listach Komitetu RE niektóre zachowania zostały penalizowane m.in. w ustawie z 30.10.1992 r. o ochronie topografii układów scalonych[13] czy ustawie z 04.02.1994 r. o prawie autorskim i prawach pokrewnych[14]. Reakcją finalną procedowania w zakresie przestępczości komputerowej było wprowadzenie do kodeksu karnego z 1997 r. poszczególnych typów przestępstw z listy minimalnej[15].

Z uwagi na przedmiot podejmowanych rozważań regulacje dotyczące przestępczości komputerowej będą obejmowały wyłącznie przestępstwa przeciwko mieniu, oszustwo internetowe z art. 286 § 1 k.k. i oszustwo komputerowe z art. 287 k.k. Kodeks karny z 1997 r. wprowadził w art. 287 nieznany kodeksowi karnemu z 1969 r., w przeciwieństwie do przestępstwa oszustwa klasycznego, szczególny typ przestępstwa nazywany oszustwem komputerowym[16]. Jak uzasadniał rządowy projekt nowego kodeksu karnego: „wprowadzenie oszustwa komputerowego jest niezbędne, gdyż tradycyjne pojęcie

[10] K.J. Jakubski, *op. cit*., s. 35.

[11] Tekst Zalecenia w języku polskim zawiera aneks opracowania B. Fischera, *Przestępstwa komputerowe i ochrona informacji*, Zakamycze 2000, s. 237 i n.; Także M. Dąbrowska- Kardas, P. Kardas, *Przestępstwa przeciwko mieniu*, [w:] *Kodeks karny. Część szczególna. Komentarz do art. 278-363 k.k.*, t. III, Wydawnictwo a Wolters Kluwer business, Warszawa 2008, s. 319.

[12] Projekt wprowadzał oszustwo komputerowe w art. 288 k.k. Zob. szerzej K. Buchała, *Reforma polskiego prawa materialnego. Przestępstwa przeciwko ochronie informacji i oszustwo komputerowe*, [w:] *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z międzynarodowej konferencji naukowej - Legal aspects of computer- related abuse, Procedings of the International Conference. (Poznań 20-22 April 1994)*, pod red. A. Adamski, Toruń 1994, s. 131-132.

[13] Dz.U. Nr 100, poz. 498.

[14] Dz.U. Nr 24, poz. 83.

[15] Penalizacją w kodeksie karnym z 6 czerwca 1997 r. (Dz.U. Nr 88, poz. 553 z późn. zm) objęte zostały oszustwo komputerowe, fałszerstwo komputerowe, uzyskanie nieuprawnionego dostępu do systemu, podsłuch komputerowy, sabotaż komputerowy, naruszenie integralności komputerowego zapisu informacji oraz bezprawne kopiowanie programów komputerowych. Zob. A. Adamski, *Cyberprzestępczość- kontrola zjawiska w Polsce- aspekty prawne i kryminologiczne*, [w:] *Przestępczość teleinformatyczna, Materiały seminaryjne*, pod red. A. Misiuk, J. Kosiński, P. Ciszka, Wyższa Szkoła Policji, Szczytno 2003, s. 10.

[16] P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, „ Przegląd Sądowy", nr 11- 12, 2000, s. 43. Treść art. 287 § 1 k.k. statuowała: „ 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".

oszustwa zawiera znamiona („wprowadza w błąd", „inną osobę", „wyzyskuje błąd" lub „wyzyskuje niezdolność innej osoby do należytego pojmowania przedsiębranego działania", „doprowadza ją do niekorzystnego rozporządzenia mieniem"), które przy oszustwie dokonywanym za pomocą komputera lub innego urządzenia automatycznie gromadzącego, przetwarzającego lub przesyłającego informacje, nie są przez działanie sprawcy spełniane, chociaż nienależna korzyść majątkowa jest osiągana"[17]. Penalizacja w kodeksie karnym niniejszego przestępstwa była związana m.in. ze sposobem jego popełnienia. Czynność sprawcza dotyczyła bowiem wykorzystania automatycznego urządzenia służącego do gromadzenia, przetwarzania bądź przesyłania informacji lub dokonania zmiany, usunięcia lub wprowadzenia nowego zapisu na komputerowym nośniku informacji. Działania przestępne z wykorzystaniem nowoczesnej technologii spowodowały więc powstanie luki w obszarze prawa karnego, a przepis przestępstwa oszustwa z art. 286 k.k.[18] nie był wystarczający do oddania kryminalnej zawartości oraz nie harmonizował z nowoczesną formą ataku na mienie[19].

Potrzeba dostosowania przepisów polskiego prawa karnego względem regulacji międzynarodowych, w obszarze przestępczości internetowej, wymogła na ustawodawcy krajowym kontynuację prac w tym zakresie. Wprowadzona nowelizacja przestępstwa oszustwa komputerowego z 2004r.[20] związana była z podpisaniem przez Rzeczypospolitą Polską 28 listopada 2001r. Konwencji o cyberprzestępczości[21]. Definicja oszustwa komputerowego, ujęta w art. 8 Konwencji, zobowiązywała strony do uznania za przestępstwo w jej prawie krajowym umyślnego spowodowania utraty własności przez inną osobę na skutek: wprowadzenia, zmiany, usunięcia lub zablokowania danych informatycznych, innej ingerencji w funkcjonowanie systemu informatycznego w oszukańczym lub nieuczciwym zamiarze bezprawnego uzyskania korzyści ekonomicznych dla siebie lub innej osoby[22]. Dostosowanie art. 287 k.k. do definicji

[17] *Uzasadnienie rządowego projektu kodeksu karnego. Nowe kodeksy karne z uzasadnieniami*, Warszawa 1997, s. 206-207.

[18] Art. 286 § 1 na gruncie kodeksu karnego z 1997r., jak i obecnego statuuje: „Kto w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8". Przepis ten był odpowiednikiem dawnego art. 205 k.k. z 1969 r. (Dz.U. Nr 13, poz. 94 z dnia 14 maja 1969 r.). Ustawodawca w kodeksie karnym z 1997 r. zaostrzył jedynie odpowiedzialność karną podnosząc górną granicę z 5 lat do lat 8.

[19] P. Kardas, *op. cit*., s. 44.

[20] Ustawa z 18 marca 2004 r. o zmianie kodeksu karnego, kodeksu postępowania karnego i kodeksu wykroczeń wprowadzająca nowelizację weszła w życie 1 maja 2004 r. z dniem akcesji Polski do Unii Europejskiej (Dz.U.z 2004 Nr 69, poz. 626). Zob. szerzej R. Koszut, *Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań Konwencji o cyberprzestępczości*, [w:] *Przestępczość teleinformatyczna, Materiały seminaryjne*, pod red. J. Kosiński, Wyższa Szkoła Policji, Szczytno 2004, s. 35-38.

[21] Konwencja z 23 listopada 2001r. zawarta w Budapeszcie wskazywała na postanowienia, z których najważniejsze dotyczyły harmonizacji narodowych systemów prawnych wglądem zdefiniowania przestępstw, wypracowania standardów prowadzenia śledztw i procedur sądowych dostosowanych do zasad działania globalnej sieci oraz stworzenia szybkiego i skutecznego systemu współpracy międzynarodowej. Zob. J.W. Wójcik, *Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne*, [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, pod red. T. Jemioła, J. Kisielecki, K. Rajchel, Warszawa 2009, Za: http://www.dobrauczelnia.pl/279, s. 19-20.

[22] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawiska w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001, s. 48; Także B. Michalska- Kunicka, *Oszustwo komputerowe. Regulacje prawa polskiego*, „Studia Prawnicze", z. 4, 2006, s. 104.

konwencyjnej w konsekwencji oznaczało przyjecie przez ustawodawcę polskiego szerszego zakresu w opisie czynu. Przepis ten ze względu na stronę podmiotową przestępstwa określa dwie odmiany oszustwa komputerowego, bowiem alternatywny cel działania sprawcy obok oszustwa komputerowego charakteryzującego się celem osiągnięcia korzyści majątkowej określa również inny typ tzw. szkodnictwo komputerowe, którego celem jest wyrządzenie innej osobie szkody[23]. Istota tego czynu, jak wskazuje A. Adamski, polega na usiłowaniu uzyskania korzyści majątkowej lub spowodowania szkody przez manipulowanie zapisem na komputerowym nośniku informacji bądź innym oddziaływaniu na automatyczne przetwarzanie informacji[24]. Zatem zmiany względem pierwotnej wersji przepisu 287 k.k. wprowadzone powyższą ustawą dotyczyły po pierwsze określenia przedmiotu bezpośredniego oddziaływania, jakim był „zapis na komputerowym nośniku informacji". Wiązało się to głównie z modyfikacją ustawowej definicji dokumentu z art. 115 § 14 k.k. oraz art. 47 § 8 k.w., do treści których wprowadzono termin „inny zapisany nośnik informacji" za dotychczasowy „komputerowy nośnik informacji"[25]. Po wtóre, w skutek nowelizacji, w opisie czynu w § 1 oszustwa komputerowego dokonano następujących zmian: znamię „przesyłanie" zastąpiono słowem „przekazywanie", pierwotny przedmiot bezpośredniego oddziaływania jako „informacja" zamieniono na zwrot „dane informatyczne", natomiast termin „zapis na komputerowym nośniku informacji" zwrotem „zapis danych informatycznych". Nowe regulacje zawarte w tym przepisie, modyfikując czynności wykonawcze odnoszą się wobec tego do określonych wspólnym terminem „danych informatycznych", który zastąpił wcześniejsze terminy „informacje" oraz „zapis na komputerowym nośniku informacji"[26].

3. OSZUSTWO KOMPUTEROWE A KLASYCZNA FORMA OSZUSTWA INTERNETOWEGO[27]

Szczególne zainteresowanie w polskich publikacjach prawnokarnych wzbudziło poszukiwanie cech zbieżnych oraz różnic występujących pomiędzy oszustwem a oszustwem komputerowym[28]. Kwestia zachodzących relacji pomiędzy poszczególnymi znamionami obu czynów ma istotny wpływ na sposób ich interpretacji, a tym samym pozwala określić, która z norm będzie mogła mieć zastosowanie. W przypadku obu omawianych typów przestępstw głównym przedmiotem ochrony jest mienie w znaczeniu

[23] B. Michalski, *op. cit*., s. 1041.

[24] Z kolei według Konwencji o dokonaniu oszustwa komputerowego decyduje wywołanie skutku w postaci utraty własności przez osobę pokrzywdzoną przestępstwem. Cechuje się zatem węższym zakresem regulacji oszustwa komputerowego. A. Adamski, *op. cit*., s. 48.

[25] M. Dąbrowska- Kardas, P. Kardas, *op. cit*., s. 318. Regulacje ustawowej definicji „dokumentu" w kodeksie karnym miały znaczenie nie tylko dla przestępstwa oszustwa komputerowego, ale także dla innych przepisów związanych z cyberprzestępczością. Nowelizacją objęte zostały również art. 165 i 269 k.k. Ponadto, na skutek tej zmiany stypizowane zostały nowe odmiany przestępstw w art. 268a, 269a i 269b k.k. Zob. także W. Grzeszczyk, *Zmiany prawa karnego wprowadzone ustawą z dnia 18 marca 2004 r.*, „Prokuratura i Prawo, nr 7-8, 2004, s. 77-80.

[26] *Ibidem*, s. 318; B. Michalski, *op. cit*., s. 1039.

[27] Na potrzeby niniejszego artykułu przestępstwo oszustwa z art. 286 k.k. potraktowane będzie tylko w zakresie czynów popełnionych w Internecie.

[28] B. Kunicka- Michalska, *op. cit*., s. 113.

szerokim[29]. Jednakże, ze względu na kształt znamion przestępstwa oszustwa komputerowego, jak też ustawowy kontekst, pojęcie mienia należy rozumieć szerzej jako zbiorczą nazwę dla wszelkich praw majątkowych, których potwierdzeniem (dowodem istnienia) jest odpowiedni zapis w systemie gromadzącym, przetwarzającym lub przesyłającym automatycznie dane informatyczne albo mienie, z którym związany jest taki zapis. Przestępstwo to chroni więc przed wszelkimi działaniami oszukańczymi własność lub inne prawa rzeczowe albo obligacyjne do mienia, wyrażone w postaci zapisu na odpowiednim nośniku informacji[30]. Oszustwo komputerowe swoją konstrukcją różni się zatem od oszustwa klasycznego, gdyż oprócz mienia chroni integralność i nienaruszalność samych informacji (zapisy informacji), a także zasady automatycznego ich przetwarzania, gromadzenia lub przesyłania[31]. Z kolei w przestępstwie oszustwa klasycznego, poza mieniem, przedmiotem ochrony jest osoba pokrzywdzonego, z którą w przypadku oszustwa komputerowego nie mamy do czynienia, ponieważ przepis art. 287 k.k. wyłącza ją jako przedmiot ochrony tego przestępstwa[32]. Taka konstrukcja czynu zabronionego związana jest bezpośrednio z brakiem wykorzystania przez sprawcę środków oddziaływania na osobę dokonującą rozporządzenia mieniem[33]. W przypadku oszustwa z art. 286 k.k. mamy do czynienia z Internetem jako narzędziem, za pomocą którego sprawca doprowadza drugiego uczestnika do niekorzystnego rozporządzenia mieniem, porozumiewa się z nim, wpływając jednocześnie na jego procesy decyzyjne. Natomiast w przypadku przestępstwa oszustwa komputerowego specyficzna relacja nie ma miejsca, bowiem dla dokonania tego czynu pokrzywdzony nie musi być wprowadzony w błąd lub nie musi nastąpić wyzyskanie błędu bądź nienależytego pojmowania przedsiębranego działania. Sprawca oddziałuje bezpośrednio na urządzenia lub procesy techniczne związane z automatycznym gromadzeniem, przetwarzaniem i przesyłaniem danych, nie zaś na inną osobę.

Istotne różnice dotyczą również strony przedmiotowej rozważanych przestępstw. Znamiona określające czynność sprawczą z art. 287 k.k. wskazują na dwie grupy działań. Pierwsze obejmują wpływanie na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji, na co składają się manipulacje komputerowe dokonane na wejściu i wyjściu. Drugie natomiast polegają na zmianie, usuwaniu lub wprowadzeniu nowego zapisu danych informatycznych i do tych czynności odnosi się ściślej rozumiana nazwa

[29] W kontekście tych czynów określenie „mienie" spełnia funkcję nazwy zbiorczej, oznaczające wszelkie kategorie podmiotowych praw majątkowych, zarówno rzeczowych, jak i obligacyjnych, niezależnie od treści lub przedmiotów tych praw ani od charakteru podmiotów, którym te prawa przysługują. Zob. szerzej postanowienie SN z dnia 15 czerwca 2007 r., I KZP 13/07, OSNKW 2007, nr 7-8, poz. 56.

[30] M. Dąbrowska- Kardas, P. Kardas, *op. cit*., s. 320.

[31] Zob. szerzej K. Kardas, *op. cit*., s. 56-57; Podobnie R. Korczyński, K. Koszut, *Oszustwo komputerowe wobec klasycznej formuły oszustwa*, „Prokuratura i Prawo", nr 2, 2002, s. 24-25. Podkreślenia wymaga fakt, że same zapisy informacji zamieszczone na nośniku nie będące dowodem istnienia lub nie związane z określonymi prawami majątkowymi będą podlegać ochronie z art. 268 § 1 k.k., nie zaś z art. 287 k.k., gdyż nie dotyczą szczególnego rodzaju informacji związanych ściśle z mieniem.

[32] Nie oznacza to jednak, że przepis z art. 287 nie chroni pokrzywdzonego. Mienie jako główny przedmiot ochrony związane jest z prawami, które przysługują określonemu podmiotowi (pokrzywdzonemu).

[33] L.K. Paprzycki, *Oszustwo informatyczne właściwe i niewłaściwe a nielegalne wykorzystywanie dialerów*, „Studia Prawnicze", z. 4, 2007, s. 123-124. Autor określa takie oszukańcze zachowanie niewłaściwym oszustwem informatycznym.

oszustwa komputerowego[34]. Według większości autorów[35] *modus operandi* przy oszustwie komputerowym wiąże się z wpływaniem, które obejmuje: a) manipulację danymi, polegającą na wprowadzeniu nieprawdziwych danych w celu uzyskania nieuprawnionych korzyści majątkowych, b) manipulację programem, polegającą na wprowadzeniu do programu czy systemu informacji, której skutkiem jest samoczynne (niezależnie od woli operatora) przysporzenie korzyści majątkowej poprzez modyfikację procesu przetwarzania, gromadzenia lub przekazywania danych informatycznych, c) manipulację wynikiem, która polega na wykorzystaniu ogólnie dostępnych peryferii komputerów i systemów komputerowych w celu zmiany wyniku procesu automatycznego przetwarzania, gromadzenia lub przekazywania danych. Niezależnie od dokonywanych podziałów każde z wymienionych zachowań musi być podejmowane bez upoważnienia. Oznacza to, iż znamię „bez upoważnienia" zostanie wypełnione tylko wówczas, gdy osoba dopuszczająca się takiego czynu nie będzie miała do tego upoważnienia, które może polegać na dowolnym umocowaniu przez osobę mającą do tego prawo[36]. Elementem charakteryzującym stronę przedmiotową oszustwa z art. 286 k.k. jest doprowadzenie innej osoby do niekorzystnego rozporządzenia mieniem za pomocą wprowadzenia jej w błąd, wyzyskania błędu bądź niezdolności do należytego pojmowania przedsiębranego działania, co stanowi różnicę względem zawartych w art. 287 k.k. czynności sprawczych. Oszustwo komputerowe charakteryzuje się tym, że sprawca w ogóle nie oddziałuje na inną osobę, a w konsekwencji nie doprowadza jej do podjęcia czynności, zmierzających do rozporządzenia mieniem. Doprowadzenie innej osoby do niekorzystnego rozporządzenia mieniem, w znamionach przestępstwa z art. 287 k.k., zastępuje czynność sprawcza polegająca na: wpływaniu bez upoważnienia na automatyczne przetwarzanie, gromadzenie lub przesyłanie danych informatycznych bądź na zmianie, usunięciu lub wprowadzeniu nowego zapisu danych informatycznych[37]. Odmienne zachowania sprawcze, w obu tych typach czynu, wywołują także różne skutki. W przestępstwie oszustwa klasycznego skutkiem oddziaływania sprawcy jest niekorzystne rozporządzenie mieniem, którego z kolei brak w oszustwie komputerowym. Skutek taki następuje już w momencie wpływania, dokonywania zmiany, usunięcia zapisu lub jego wprowadzenia, zatem gdy nie nastąpiło jeszcze przesunięcie w sferze majątkowej lub rzeczywiste powstanie zamierzonej szkody. Jeżeli sprawca nie osiągnął korzyści majątkowej lub nie wyrządził szkody, ponieważ podjął jedynie działania zmierzające do uzyskania określonego wpływu, dokonania zmiany, usunięcia czy wprowadzenia zapisu, możemy przyjąć ewentualne usiłowanie tego czynu[38].

---

[34] O. Górniok, *Przestępstwa przeciwko mieniu***,** [w:] *Kodeks karny. Komentarz*, pod red O. Górniok, Gdańsk 2002/2003, s. 1185.

[35] B. Fischer, *op. cit.*, s. 33 i n.; K.J. Jakubski, *op. cit.*, s. 37- 38; A. Adamski, *op. cit*., s. 144 – 146; M. Dąbrowska- Kardas, P. Kardas, *op. cit*., s. 327; B. Kunicka- Michalska, *op. cit*., s. 111; A. Adamski, *op. cit.*, s. 118 i n.

[36] M. Kulik, *Przestępstwa przeciwko mieniu*,[w:] *Kodeks karny. Praktyczny komentarz*, pod red. M. Mozgawa, Oficyna a Wolters Kluwer business, Warszawa 2010, s. 594.

[37] P. Kardas, *op. cit*., s. 58.

[38] W doktrynie wyrażane są jednak odmienne poglądy względem skutkowości przy oszustwie komputerowym. Zadaniem niektórych komentatorów jest to przestępstwo formalne, zatem skutek w postaci wyrządzenia innej osobie szkody, czy osiągnięcia korzyści majątkowej nie należy do znamion tego czynu. Jest bowiem wystarczające, aby sprawca działał w celu osiągnięcia tej korzyści lub wyrządzenia szkody. Pomimo, że sprawca może osiągnąć taką korzyść lub wyrządzić szkodę to skutek taki nie jest warunkiem zaistnienia tego

Znamiona, określające motywację sprawcy, wskazują na dwojaki cel popełnienia oszustwa z art. 287 k.k. Działanie w celu osiągnięcia korzyści majątkowej, według doktryny, należy traktować jako oszustwo komputerowe, zaś działanie w celu wyrządzenia szkody – jako szkodnictwo komputerowe. Różnica występująca względem oszustwa klasycznego, od strony podmiotowej, dotyczy zachowania ukierunkowanego na cel wyrządzenia innej osobie szkody, gdyż dyspozycja z art. 286 k.k. określa jedynie znamię charakteryzujące się celem osiągnięcia korzyści majątkowej[39].

4. WYMIAR KARY

Wymiar odpowiedzialności karnej, jaki przewiduje ustawodawca w kodeksie karnym względem sprawcy występku z art. 287 k.k., w zależności od typu czynu zabronionego, obejmuje karę pozbawienia wolności od 3 miesięcy do lat 5 w typie podstawowym, zaś w typie uprzywilejowanym w § 2 grzywnę, karę ograniczenia wolności albo pozbawienia wolności do roku[40]. Postać kwalifikowana (art. 294 k.k.) zagrożona jest najsurowszą karą pozbawienia wolności od roku do lat 10 i ma zastosowanie wówczas, gdy sprawca dopuści się przestępstwa z § 1 art. 287 k.k. w stosunku do mienia znacznej wartości[41] lub dobra o szczególnym znaczeniu dla kultury. Przy spełnieniu przesłanek z art. 58 § 3 k.k., w stosunku do sprawcy możliwe jest zamiast kary pozbawienia wolności orzeczenie grzywny lub kary ograniczenia wolności zwłaszcza, gdy jednocześnie orzekany jest środek karny, jak również z uwagi na cel działania sprawcy, skazując go na karę pozbawienia wolności, orzeczenie kumulatywnej grzywny obok wymierzonej kary. Zgodnie więc z art. 33 § 2 k.k. taki sposób wymierzenia grzywny może mieć zastosowanie, gdy sprawca dopuścił się czynu w celu osiągnięcia korzyści majątkowej lub gdy korzyść tę osiągnął niezależnie, czy dla siebie czy dla kogoś innego. Przepis ten nie ma jednakże zastosowania wobec sprawcy, którego celem działania było wyrządzenie innej osobie szkody[42]. Osiągnięcie korzyści majątkowej bądź spowodowanie szkody w mieniu pokrzywdzonego, z punktu widzenia wymiaru kary może mieć decydujące

czynu, czego z kolei nie kwestionuje nikt z przedstawicieli doktryny. A. Adamski, *op. cit*., s. 135; R. Korczyński, R. Koszut, *op. cit.*, s. 32 i n.; Przeciwnie, za materialnym charakterem tego przestępstwa opowiada się m.in. M. Dąbrowska- Kardas, P. Kardas, *op. cit.*, s. 330-331; B. Kunicka- Michalska, *op. cit*., s. 110.

[39] Zarówno oszustwo z art. 286 k.k., jak i z art. 287 k.k. jest przestępstwem umyślnym, kierunkowym. Mogą być one popełnione z zamiarem bezpośrednim, który obejmuje cel działania sprawcy oraz sposób jego działania. Por. wyrok SN z dnia 20 lipca 2007r., III KK 29/07, Lex, nr 307787, wyrok SN z dnia 14 stycznia 2004r., IV KK 192/03, Lex, nr 84458, wyrok SN z dnia 3 kwietnia 2007r., III KK 362/06, Lex, nr 296749, wyrok SN z dnia 19 lipca 2007r., V KK 384/06, Biul. PK 2007, nr 14, poz. 33. Sprawca musi chcieć użyć określonego sposobu działania w celu uzyskania korzyści majątkowej, nie musi jednak dążyć do przywłaszczenia mienia, a nawet może zakładać jego zwrot, lecz z zamiarem osiągnięcia korzyści płynącej z rozporządzenia mieniem, przejawiającej się w innej postaci. Por. wyrok SN z dnia 30 sierpnia 2000 r., V KKN 267/00, OSP 2001, z. 3, poz. 51, wyrok SN z dnia 10 marca 2004 r., II KK 381/03, „Prokuratura i Prawo", 2004, nr 7-8, poz. 3, wyrok SA w Warszawie z dnia 21 kwietnia 2005 r., II Aka 74/04, Apel. W-wa 2005, nr 3, poz. 11.

[40] Kwalifikacja z art. 287 § 2 k.k. jest możliwa, gdy wypadek mniejszej wagi będzie oznaczał niewielki rozmiar osiągniętej lub zamierzonej korzyści oraz brak bądź nikłość szkody po stronie pokrzywdzonego. A. Marek, *Kodeks karny. Komentarz*, Dom wydawniczy ABC, Warszawa 2005, s. 592. Skutkiem przyjęcia wypadku mniejszej wagi może być odstąpienie od orzekania kary i zastosowanie środka karnego przy spełnieniu przesłanek z art. 59 k.k.

[41] Zgodnie z dyspozycją art. 115 § 5 k.k. mieniem znacznej wartości jest to, którego wartość w czasie popełnienia czynu zabronionego przekracza 200 000 złotych.

[42] B. Michalski, *op. cit*., s. 1050.

znaczenie także wtedy, gdy sprawca dobrowolnie naprawi szkodę w całości lub w znacznej części, bowiem sąd na podstawie art. 52 i 53 k.k. zgodnie z dyspozycją z art. 295 § 1 lub 2 k.k. może fakultatywnie odstąpić od wymierzenia kary lub zastosować nadzwyczajne złagodzenie kary. Możliwość zastosowania tych środków nie spotkała się jednak w doktrynie z aprobatą. Jeżeli przyjmie się bezskutkowy charakter przestępstwa z art. 287 k.k., to możliwość korzystania z tego rodzaju instytucji z polityczno-kryminalnego punktu widzenia jest wadliwa, gdyż premiuje czyny o większym stopniu społecznej szkodliwości, których skutkiem jest szkoda. Nie mają one natomiast zastosowania do tych zachowań, które dopiero zmierzają do wyrządzenia szkody, a więc cechują się mniejszą społeczną szkodliwością czynu[43]. W sytuacji skazania za przestępstwo z art. 287 k.k. pokrzywdzony może również wnioskować o orzeczenie obowiązku naprawienia szkody w całości lub w części na podstawie art. 46 § 1 k.k.

Inaczej kwestia odpowiedzialności karnej przedstawia się w przypadku przestępstwa oszustwa. Występek z § 1 zagrożony jest karą pozbawienia wolności od 6 miesięcy do lat 8. Typ uprzywilejowany penalizowany w § 3 określa wypadek mniejszej wagi i wprowadza karę grzywny, ograniczenia wolności lub pozbawienia wolności do lat 2. Ponadto, podobnie jak przy przestępstwie oszustwa komputerowego, do oszustwa klasycznego zastosowanie ma art. 294 k.k. jako postać kwalifikowana oraz przepisy z art. 33 § 2, 46 § 1, 295 § 1 i 2 k.k.

5. WNIOSKI KOŃCOWE

Internet w zakresie przestępczości jest narzędziem i celem popełnienia przestępstw[44]. Nadużycia rozwijają się wraz z ewolucją informatyki i telekomunikacji[45]. Czynnikiem decydującym o bycie przestępstw: oszustwa i oszustwa komputerowego w Internecie jest łatwa i pozornie bezpieczna okazja popełnienia czynu zabronionego, a także spodziewany duży zysk[46]. Dokonując analizy danych KGP, dotyczących przestępstw z art. 286 k.k.[47] i 287 k.k.[48], można obserwować coroczny wzrost przestępczości oraz nadużyć związanych z wykorzystaniem technologii informacyjnej. Stawienie czoła temu wyzwaniu będzie wymagać podjęcia szeregu działań idących w trzech zasadniczych kierunkach. Pierwszy z nich dotyczyć będzie tworzenia odpowiednich instrumentów prawnych służących ściganiu, także w przypadku transgranicznego charakteru popełnianych przestępstw.

[43] Oznacza to, że art. 295 k.k. będzie miał zastosowania dopiero wówczas, gdy powstanie szkoda, np. gdy sprawca oszustwa komputerowego, będący pracownikiem banku, dokona manipulacji w postaci przesunięcia majątkowego, zaś w razie ujawnienia takiego zachowania dobrowolnie naprawi szkodę. Gdy do ujawnienia tego przestępstwa doszłoby w początkowej fazie jego realizacji, np. w momencie otwarcia rachunku na nazwisko osoby fikcyjnej, nie będzie możliwości stosowania powyższego przepisu. Zob. szerzej A. Adamski, *op. cit.*, s. 121-122.

[44] R.A. Stefański, *Przestępstwa internetowe w Polsce. Analiza praktyki*, „Studia Prawnicze", nr 4, 2005, s. 127.

[45] A. Adamski, *op. cit*., s. 7.

[46] J.W. Wójcik, *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008, s. 24.

[47] Wg statystyk KGP brak jest danych na temat udziału ilościowego przestępstwa oszustwa internetowego w klasycznym oszustwie z art. 286 k.k. W literaturze przedmiotu spotyka się niepełne dane, na podstawie których hipotetycznie wnioskować można o zwiększającej się corocznie liczbie. Zob. szerzej R. A. Stefański, *Przestępstwa internetowe w Polsce. Analiza praktyki*, „Studia Prawnicze", z. 4, 2006, s. 121-127 .

[48] Wg danych KGP (statystyka dotycząca liczby postępowań wszczętych za poszczególne lata); 1999- 52, 2000- 127, 2001- 59, 2002 – 114, 2003- 219, 2004 – 229, 2005 – 326, 2006 – 285, 2007 – 322, 2008- 472, 2009 – 673.

Drugim kierunkiem działania będzie prowadzenie pełnej analizy dostępnych danych na temat popełnionych przestępstw, a w szczególności aspektów technicznych *modus operandi*. Ostatnim działaniem winno być realizowanie prewencji ogólnej: przeprowadzenie szkoleń pracowników organów ścigania i wymiaru sprawiedliwości w celu podnoszenia poziomu wiedzy na temat technik wykrywania przestępstw komputerowych, metod gromadzenia dowodów elektronicznych oraz ich procesowego wykorzystywania[49].

Dotychczasowa praktyka śledcza oraz orzecznictwo sądowe wskazują na ograniczone możliwości ścigania sprawców omawianych przestępstw. Przyczyny takiego stanu rzeczy są bardzo zróżnicowanie, a wynikają przede wszystkim ze specyfiki tych czynów. Złożoność problemu stwarza poważne trudności wykrywcze[50] i dowodowe[51]. Specyfika przestępstw komputerowych związana jest m.in. z ich transgranicznym charakterem, możliwością zdalnego działania sprawców, krótkim czasem popełnienia przestępstwa, możliwością łatwego kamuflowania czynu, brakiem specjalistycznej techniki w czynnościach wykrywczych i dowodowych, charakterystycznym *modus – operandi*. W przypadku obu omawianych przestępstw trudno mówić o jakichkolwiek ograniczeniach terytorialnych czy czasowych. Internet pozwala na dużą swobodę działań przestępnych. Sprawca ma niejako poczucie anonimowości i dostęp do wszystkich użytkowników, którzy są w sieci internetowej. Powoduje to wiele przeszkód formalnych, utrudniających ściganie. Ponadto sprawca przestępstwa, nie będąc na miejscu popełnienia czynu, nie zostawia śladów, zaś czas pojawienia się skutków czynu może się bardzo różnić od momentu ich zainicjowania, w szczególności w przypadku przestępstwa z art. 287 k.k. Użytkownicy nie mają świadomości o popełnionym przestępstwie, a skutki przestępne przypisywane są błędnemu działaniu oprogramowania czy awarii systemu. Sprawcy często korzystają z nielegalnego oprogramowania z zaprogramowaną funkcją samolikwidacji. Możliwość wykrycia złośliwego programu jest prawdopodobna tylko w przypadku jego działania lub gdy całkowicie nie uległ wymazaniu z nośnika danych. Czynności podejmowane przez organy ścigania po dokonaniu tego rodzaju przestępstw muszą być stosunkowo szybkie, gdyż związane jest to ze swoistym materiałem dowodowym. Przestępstwa popełniane w Internecie mają niespotykane cechy, które w znacznym stopniu utrudniają ujawnianie, ściganie sprawców, a także dowodzenie ich winy[52].

Istotną kwestią jest również krzyżowanie się różnorodnych regulacji prawnych. Nie wpływa to korzystnie na ściganie przestępstw popełnianych w Internecie, co więcej, w niektórych sytuacjach nie pozwala na ujęcie sprawcy przestępstwa. Pojawia się przy tym praktyczne zagadnienie, w jaki sposób stosować względem takich czynów przepisy regulujące miejsce popełnienia przestępstwa. Zgodnie z zasadą wyrażoną w art. 6 § 2 k.k. czyn zabroniony uważa się za popełniony w miejscu, w którym sprawca działał lub

[49] A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne,* „Studia Prawnicze", z. 4, 2005, s. 74.

[50] Zob. A. Baworowski, *Metodyka prowadzenia czynności wykrywczych w sprawie o oszustwo w internetowym portalu aukcyjnym w zakresie gromadzenia, danych informatycznych,* „Diariusz Prawniczy", nr 4 (5), 2007, s. 62 -80; Także J. Kosiński, *Przykład wykorzystywania nowoczesnych technologii przetwarzania informacji do dokonania przestępstwa,* [w:] *Internet fenomen społeczeństwa informacyjnego*, pod red. T. Zasępa, Edycja Świętego Pawła 2001, s. 601-615; A. Godlewski, *Trendy w przestępczości elektronicznej*, „Przegląd Policyjny", nr 3, 2006, s. 93-120; B. Fischer, *op. cit*., s. 185-186.

[51] J.W. Wójcik, *op. cit.*, s. 380

[52] *Ibidem,* s. 380.

zaniechał działania, do którego był zobowiązany, albo gdzie skutek, stanowiący znamię czynu zabronionego, nastąpił lub według sprawcy miał nastąpić. W przypadku przestępstw popełnionych przy użyciu komputera miejscem popełniania czynu zabronionego jest miejsce, gdzie sprawca łączy się z Internetem. Zagadnienie to nie rodzi wątpliwości w przypadku, gdy sprawca popełnia przestępstwo na terytorium RP. Sytuacja kształtuje się zgoła inaczej, gdy działa on na szkodę osoby bądź oddziałuje na program komputerowy, znajdujący się na terytorium RP, a sam pozostaje poza granicami kraju[53]. Nierzadkim zachowaniem sprawców popełniających przestępstwa w sieci są działania, mające na celu ukrycie prawdziwego miejsca działania. Wykorzystywane są w tym celu programy komputerowe, które umożliwiają łączenie przez ustalone serwery, co wpływa na zmniejszenie wykrywalności. Sprawca swoim działaniem ukrywa IP komputera, wskazując na inne, przypadkowe lokalizacje, niezwiązane zupełnie z miejscem popełnienia przestępstwa. W metodach przestępczych wykorzystywane są również VPN (wirtualne prywatne sieci), za pomocą których sprawca, używając odpowiedniego programu komputerowego łączy się z wybranym komputerem, dokonując działań przestępnych. W przypadku wykorzystania wirtualnej sieci sprawca otrzymuje IP, którego nie można powiązać z żadnym serwerem w tradycyjny sposób. Korzystają oni również z możliwości zdalnego wykorzystania komputerów osób niepowiązanych, przez włamanie się do ich komputerów za pośrednictwem wirusa komputerowego (koń trojański). Ponadto instalują wirusy na wybranych komputerach, które umożliwiają im całkowite przejęcie systemu i swobodę działań. Równie często użytkownicy padają ofiarami podsłuchu komputerowego, instalując oprogramowanie z nieznanych źródeł, zawierające dodatkowo programy szpiegujące, które umożliwiają poznanie wszystkich działań wykonywanych na komputerze.

Elementem decydującym o powodzeniu i zamierzonej efektywności działań oszukańczych jest zaawansowana wiedza sprawcy z zakresu sieci komputerowych oraz zabezpieczeń systemów teleinformatycznych. Sprawca, który wypełnia znamiona występku penalizowanego w art. 287k.k., nie jest osobą przypadkową – jest to osoba, która posiada specjalistyczną wiedzę informatyczną. Natomiast sprawca oszustwa z art. 286 k.k. mierzy się tylko z ludzką psychiką, a komputer jest jedynie narzędziem, które pozwala mu wykonać swoje oszukańcze zamiary. Osoba taka z założenia posiada odpowiedni zakres wiedzy i bystrości umysłu oraz umiejętność „sugestywnego" oddziaływania, pozyskiwania ludzi i ich zaufania[54].

Zasadniczym problemem jest również brak jednolitego nazewnictwa z pogranicza informatyki i prawa. W doktrynie pojawiały się idee stworzenia odrębnej gałęzi prawa, której zakres merytoryczny obejmowałby działania przestępne popełnione w Internecie. Pomysł ten spotkał się jednak z negatywną reakcją środowiska. Zasadną motywację w przedmiocie wyodrębnienia osobnej gałęzi prawa podniosła A. Kania[55], która uważa, że: „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

[53] K. Gienas, *Cyberprzestępczość*, „Jurysta", nr 12, 2003, s. 9.

[54] J.W. Wójcik, *op.cit*., s. 49.

[55] A. Kania, *Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni*, CBKE e-Biuletyn, za: http://cbke.prawo.uni.wroc.pl/files/ebiuletyn/oszustwo_komputerowe.pdf

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 […] Podobnie nie można oddzielać problematyki przestępczości komputerowej od wykształconych i utrwalonych w prawie karnym zasad odpowiedzialności". Brak jednak ujednoliconego nazewnictwa oraz wiedzy z zakresu informatyki, w kontekście potężnego zasięgu Internetu i skomplikowanych rozwiązań technicznych, mających w nim zastosowanie sprawia, że wirtualna przestrzeń staje się miejscem idealnym do dokonania przestępstwa. Stworzenie odrębnej gałęzi prawa nie będzie miało znaczenia, jeżeli prawo nie będzie dostosowane, czy uzupełniane do wymogów kształtujących nasz byt w wirtualnej rzeczywistości. Rewolucja jaka dokonała się w zakresie informatyzacji powinna nieść za sobą również integralny rozwój prawa.

Kończąc rozważania, należałoby stwierdzić, że powszechny dostęp do Internetu, obok swych licznych walorów, stworzył doskonałe warunki rozwoju przestępczości komputerowej[56]. Internetowa anonimowość sprawiła, że potencjalni sprawcy czują się niemal bezkarni, zaś ich ofiary często pozostają bezradne[57]. Przestępczość komputerowa stawia przed ustawodawcą zupełnie nowe wyzwania. Poznanie specyfiki Internetu jako nowej płaszczyzny dla nadużyć pozwoli na lepsze zrozumienie fenomenu i zagrożeń, związanych z przestępstwami popełnianymi za pomocą komputerowej klawiatury[58].

LITERATURA

[1] Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, Studia Prawnicze, 2005, nr 4

[2] Adamski A., *Cyberprzestępczość – kontrola zjawiska w Polsce – aspekty prawne i kryminologiczne*, [w:] *Przestępczość teleinformatyczna, Materiały seminaryjne*, red. A. Misiuk, J. Kosiński, P. Ciszka, Szczytno 2003

[3] Adamski A., *Prawo karne komputerowe*, Warszawa 2000

[4] Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001

[5] Adamski A., *Przestępstwa komputerowe w projekcie kodeksu karnego na tle europejskich standardów normatywnych*, [w:] *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z międzynarodowej konferencji naukowej - Legal aspects of computer- related abuse. Procedings of the International Conference. (Poznań 20-22 April 1994)*, red. A. Adamski, Toruń 1994

[6] Baworowski A., *Metodyka prowadzenia czynności wykrywczych w sprawie o oszustwo w internetowym portalu aukcyjnym w zakresie gromadzenia danych informatycznych*, Diariusz Prawniczy, 2007, nr 4(5)

[7] Buchała K., *Reforma polskiego prawa materialnego. Przestępstwa przeciwko ochronie informacji i oszustwo komputerowe*, [w:] *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z międzynarodowej konferencji naukowej – Legal aspects of computer – related abuse, Procedings of the International Conference. (Poznań 20-22 April 1994)*, red. A. Adamski, Toruń 1994

[8] Dąbrowska- Kardas M., Kardas P., *Przestępstwa przeciwko mieniu*, [w:] *Kodeks karny. Część szczególna. Komentarz do art. 278-363 k.k.*, t. III, Warszawa 2008

[56] *Ibidem,*

[57] M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe.* „Czasopismo Prawa Karnego i Nauk Penalnych", nr 1, 2000, s. 24.

[58] K. Gienas, *op. cit.*, s. 9-10.

[9] Fischer B., *Przestępstwa komputerowe i ochrona informacji,* Zakamycze 2000
[10] Gienas K., *Cyberprzestępczość,* Jurysta, 2003, nr 12
[11] Godlewski A., *Trendy w przestępczości elektronicznej*, Przegląd Policyjny, 2006, nr 3
[12] Górniok O., *Przestępstwa przeciwko mieniu,* [w:] *Kodeks karny. Komentarz,* red O. Górniok, Gdańsk 2002/2003
[13] Grzeszczyk W., *Zmiany prawa karnego wprowadzone ustawą z dnia 18 marca 2004 r.*, Prokuratura i Prawo, 2004, nr 7-8
[14] Jakubski J.K., *Przestępczość komputerowa – zarys problematyki*, Prokuratura i Prawo, 1996, nr 12
[15] A. Kania, *Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni*, CBKE e - Biuletyn, za: http://cbke.prawo.uni.wroc.pl/files/ebiuletyn/oszustwo_komputerowe.pdf
[16] Kardas P., *Oszustwo komputerowe w kodeksie karnym*, Przegląd Sądowy, 2000, nr 11- 12
[17] Kliś M., *Przestępczość w Internecie. Zagadnienia podstawowe.* Czasopismo Prawa Karnego i Nauk Penalnych, 2000, nr 1
[18] Korczyński R., Koszut K., *Oszustwo komputerowe wobec klasycznej formuły oszustwa,* Prokuratura i Prawo, 2002, nr 2
[19] Kosiński J., *Przykład wykorzystywania nowoczesnych technologii przetwarzania informacji do dokonania przestępstwa,* [w:] *Internet fenomen społeczeństwa informacyjnego,* red. T. Zasęp, Edycja Świętego Pawła 2001
[20] Koszut R., *Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań Konwencji o cyberprzestępczości,* [w:] *Przestępczość teleinformatyczna, Materiały seminaryjne,* red. J. Kosiński, Szczytno 2004
[21] Kulik M., *Przestępstwa przeciwko mieniu,*[w:] *Kodeks karny. Praktyczny komentarz,* red. M. Mozgawa, Warszawa 2010
[22] Marek A., *Kodeks karny. Komentarz,* Warszawa 2005
[23] Michalska-Kunicka B., *Oszustwo komputerowe. Regulacje prawa polskiego,* Studia Prawnicze, 2006, z. 4
[24] Michalski B., *Przestępstwa przeciwko mieniu,* [w:] *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316,* t. II, pod red. A. Wąsek, Warszawa 2006
[25] Paprzycki L.K., *Oszustwo informatyczne właściwe i niewłaściwe a nielegalne wykorzystywanie dialerów,* Studia Prawnicze 2007, z. 4
[26] Stefański R.A., *Przestępstwa internetowe w Polsce. Analiza praktyki,* Studia Prawnicze, 2005, nr 4
[27] Tarnogórski R., *Konwencja o cyberprzestępczości – międzynarodowa odpowiedź na przestępczość ery informacyjnej,* [w:] *Bezpieczeństwo teleinformatyczne państwa,* red. M. Madej, M. Terlikowski, Warszawa 2009
[28] Wójcik J.W., *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008
[29] Wójcik J.W., *Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne,* [w:] *Cyberterroryzm – nowe wyzwania XXI wieku,* red. T. Jemioła, J. Kisielecki, K. Rajchel, Warszawa 2009, Za: http://www.dobrauczelnia.pl/279

Akty prawne:
[30] *Uzasadnienie rządowego projektu kodeksu karnego. Nowe kodeksy karne z uzasadnieniami*, Warszawa 1997
[31] Ustawa Kodeks karny z dnia 6 czerwca 1997 r. (Dz.U. Nr 88, poz. 553 z późn. zm)
[32] Ustawa Kodeks karny z dnia 14 maja 1969 r. (Dz.U. Nr 13, poz. 94)
[33] Ustawa z dnia 18 marca 2004 r. o zmianie kodeksu karnego, kodeksu postępowania karnego i kodeksu wykroczeń (Dz.U. Nr 69, poz. 626)
[34] Postanowienie SN z dnia 15 czerwca 2007r., I KZP 13/07, OSNKW 2007, nr 7-8, poz. 56
[35] Wyrok SN z dnia 20 lipca 2007 r., III KK 29/07, Lex, nr 307787
[36] Wyrok SN z dnia 14 stycznia 2004 r., IV KK 192/03, Lex, nr 84458

[37] Wyrok SN z dnia 3 kwietnia 2007 r., III KK 362/06, Lex, nr 296749
[38] Wyrok SN z 19 lipca 2007 r., V KK 384/06, Biul. PK 2007, nr 14, poz. 33
[39] Wyrok SN z dnia 30 sierpnia 2000 r., V KKN 267/00, OSP 2001, z. 3, poz. 51
[40] Wyrok SN z dnia 10 marca 2004 r., II KK 381/03, Prokuratura i Prawo 2004, nr 7-8, poz. 3
[41] Wyrok SA w Warszawie z dnia 21 kwietnia 2005 r., II Aka 74/04, Apel. W-wa 2005, nr 3, poz. 11

THE FRAUD AND COMPUTER FRAUD – SELECTED LEGAL ASPECTS

The dynamic development of the Internet and information infrastructure in the world now has a huge impact on almost every aspect of our activity. Internet network and modern technology can be used as a measure or purpose of criminal activity. This article is an attempt of synthesis of selected legal aspects of criminal fraud and computer fraud.