

BARBARA KUNICKA-MICHALSKA

**OSZUSTWO KOMPUTEROWE.
REGULACJE PRAWA POLSKIEGO***

I

Oszustwo komputerowe, trafnie nazywane zamiennie wyłudzeniem komputerowym, jest jednym z podstawowych przestępstw komputerowych.

Oszustwa związane z wykorzystaniem komputera, obok takich przestępstw jak fałszerstwa komputerowe, zniszczenie danych lub programów komputerowych, sabotaż komputerowy, nieuprawnione wejście do systemu komputerowego, podsłuch komputerowy, bezprawne kopiowanie, rozpowszechnianie lub publikowanie prawnie chronionych programów komputerowych, znalazły się na liście tzw. minimalnej, zawierającej czyny, które powinny być traktowane jako poważne przestępstwa komputerowe, opracowanej przez Komitet Ekspertów Rady Europy w latach 80., który to Komitet w opublikowanym raporcie postulował penalizację pewnej działalności komputerowej, wśród niej tzw. przestępstw „długiej ręki”. Na drugiej liście, „fakultatywnej” (zawierającej działania mniej szkodliwe), znalazły się: modyfikacja danych lub programów komputerowych, bezprawne kopiowanie topografii półprzewodników¹, szpiegostwo komputerowe, używanie komputera bez zezwolenia oraz używanie bez upoważnienia programu komputerowego prawnie chronionego².

* Skróć tego referatu został wydrukowany w języku angielskim: Barbara Kunicka-Michalska, *Computer Fraud. Provisions of Polish Law* w: Juan Carlos Ferre Olive, Enzo Musco, Barbara Kunicka-Michalska, J.A. Cabral and other Authors, *Penal Legislation in the Fight Against Financial Crimes, Fraud and Corruption, Computer Fraud and Internet Crimes*, Grotius II Penal Programme, Universidad de Salamanca Fundación General, Spain, Italy, Portugal and Poland, 2004, s. 12 i n.

¹ Bliżej o tych przestępstwach zob. A. Adamski, *Przestępstwa komputerowe w projekcie kodeksu karnego na tle europejskich standardów normatywnych*, w: idem (red.), *Przestępczość komputerowa. Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*. Materiały z międzynarodowej Konferencji naukowej, Poznań 20–22 kwietnia 1994 r., s. 143–144.

² Zob. ibidem, s. 153–154 oraz M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, *Czasopismo Prawa Karnego i Nauk Penalnych* 2000, rok IV, z. 1, s. 7–8; J. Hajdukiewicz, *E-przestępczość, zagrożenia dla gospodarki*, *Biuletyn Polskiego Towarzystwa Kryminologicznego im. profesora Stanisława Batawii* 2001, nr 10, s. 7 i n., s. 79 i n.

Oszustwo w dziedzinie informatyki znalazło się też na liście minimalnej w Rezolucji Sekcji II (dotyczącej przestępstw komputerowych) XV Międzynarodowego Kongresu Prawa Karnego AIDP³.

Zgodnie z klasyfikacją Interpolu oszustwa przy użyciu komputera obejmują w szczególności: oszustwa bankomatowe, fałszowanie tzw. urządzeń wejścia lub wyjścia (jak np. kart magnetycznych lub mikroprocesorowych), oszustwa na maszynach do gier, oszustwa poprzez podanie fałszywych danych identyfikacyjnych, oszustwa w systemach telekomunikacyjnych. Zarazem Interpol traktuje przestępstwa internetowe jako formę popełnienia przestępstwa komputerowego⁴.

J.W. Wójcik daje następującą definicję oszustw komputerowych: „Oszustwa komputerowe to manipulacje informacjami zawartymi w komputerach. Polegają najczęściej na wykorzystaniu lub przywłaszczeniu danych o aktywach firmy (środki finansowe, manipulacje dot. depozytów, kredytów, długów, wyników bilansów). Polegać mogą również na kradzieży środków finansowych z rachunków bankowych, a także surowców, towarów oraz korzystaniu z cudzych kart kredytowych itp. Zalicza się tu także manipulacje takimi urządzeniami jak bankomaty i automaty do sprzedaży towarów oraz okradanie ich”⁵.

Oszustwo komputerowe jest ujęte w Konwencji Rady Europy o cyberprzestępczości, podpisanej przez Polskę w Budapeszcie w dniu 23 listopada 2001 r. Konwencja dotyczy przestępstw popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji i współpracy międzynarodowej w dziedzinie ich ścigania. Poprzedzona była opracowanymi przez Radę Europy zaleceniami dotyczącymi kontroli przestępczości komputerowej, to jest Zaleceniem z 1989 r. dotyczącym zakresu kryminalizacji nadużyć komputerowych i Zaleceniem z 1995 r. odnoszącym się do zagadnień procesowych związanych z technologią informacyjną. W Konwencji tej oszustwo komputerowe ujęte jest w Tytule 2 „Przestępstwa związane z komputerem”, Części I „Prawo karne materialne”, Rozdziału II „Środki podejmowane na szczeblu krajowym”, w art. 8. Art. 8 stanowi: „Każda Strona podejmie środki ustawodawcze i inne, niezbędne do uznania za przestępstwo w jej prawie krajowym umyślnego spowodowania utraty własności przez inną osobę na skutek: a. wprowadzenia, zmiany, usunięcia lub zablokowania danych informatycznych, b. innej ingerencji w funkcjonowanie systemu informatycznego, w oszukańczym lub nieuczciwym zamiarze bezprawnego uzyskania korzyści ekonomicznych dla siebie lub innej osoby”⁶.

³ Bliżej zob. B. Kunicka-Michalska, *Rezolucje XV Międzynarodowego Kongresu Prawa Karnego AIDP (Rio de Janeiro, 4–10 września 1994 r.)*, cz. I, „Przegląd Prawa Karnego” 1995, nr 12, s. 62 i n., zwłaszcza s. 70 i n. Referat polski na ten Kongres dla Sekcji II Kongresu opracował K. Buchała, *Poland, Computer Crimes and Other Crimes against Information Technology in Poland*, w: *Delits Informatiques et autres Infractions a la Technologie de l' Information*, Revue Internationale de Droit Penal, 1 i 2 semestr 1993, s. 507–516.

⁴ M. Kliś, *Przestępczość w Internecie...*, op. cit., s. 8. Zob. też S. Redo, *Zapobieganie i kontrola przestępczości komputerowej z perspektywy ONZ* (w jęz. angielskim), w: A. Adamski (red.), *Przestępczość komputerowa. Prawne aspekty nadużyć...*, op. cit., s. 71 i n.

⁵ J.W. Wójcik, *Przestępstwa komputerowe*, cz. I, *Fenomen cywilizacji*, Warszawa 1999, s. 93–94.

⁶ Korzystam z oficjalnego polskiego tłumaczenia.

Oszustwo komputerowe w Konwencji ujęte jest w sąsiedztwie fałszerstwa komputerowego, o którym mowa w art. 7 Konwencji. Art. 7 Konwencji brzmi: „Każda Strona podejmie środki ustawodawcze i inne, niezbędne do uznania za przestępstwo w jej prawie krajowym umyślnego i dokonanego bez uprawnienia wprowadzenia, zmiany, usunięcia lub zablokowania danych informatycznych, następstwem czego jest powstanie danych nieautentycznych, które mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to czy można je bezpośrednio odczytać i zrozumieć. Strony mogą wprowadzić wymóg, że warunkiem zakwalifikowania czynu jako przestępstwa jest zamiar dokonania oszustwa lub występowanie podobnego nieuczciwego zamiaru”⁷. Jak widać, zwłaszcza z ostatniego zdania art. 7 Konwencji, przepis ten może być związany z oszustwem. W związku z posłużeniem się w cytowanym art. 8 Konwencji pojęciem „danych informatycznych” i „systemu informatycznego”, przypomnieć warto, że w rozumieniu Konwencji „system informatyczny” oznacza „każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych”, a „dane informatyczne” to dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny” (art. 1 Rozdziału I Konwencji)⁸.

Oszustwo komputerowe, jak trafnie podkreśla się w literaturze przedmiotu, jest ubocznym skutkiem informatyzacji systemów bankowych i finansowo-księgowych⁹, a główna trudność w jego ściganiu polega na tym, że poszkodowany (np. bank) nie chce ujawniać słabości własnego systemu, obawiając się utraty klientów¹⁰.

Jeśli ofiarą oszustwa komputerowego będzie bank, mówić będziemy o oszustwie komputerowym jako przestępstwie bankowym (o komputerowym oszustwie bankowym)¹¹.

Jako najczęstsze formy oszustwa komputerowego J. Jakubski wymienia: manipulację danymi, która polega na wprowadzeniu nieprawdziwych danych, by uzyskać nienależne korzyści majątkowe, np. wprowadzenie tzw. „martwych dusz” do systemu informatycznego ZUS-u albo manipulację danymi w kilku bankach; manipulację programem, która polega na takim przygotowaniu programu albo na jego modyfikacji, by program wykonywał określone czynności niezależnie od woli operatora, np. tzw. metoda „salami” (np. program sam zmniejsza rachunki

⁷ Zob. przyp. 6.

⁸ Zob. przyp. 6. Zob. też A. Adamski, *Międzynarodowa kontrola cyberprzestępczości*, w: T. Zasępa, R. Chmura (red.), *Internet i nowe technologie – ku społeczeństwu przyszłości*, Częstochowa 2003, s. 519 i n., zwłaszcza s. 528–529, *Przestępstwa związane z użyciem komputera*.

⁹ J. Jakubski, *Przestępczość komputerowa – próba zdefiniowania zjawiska*, w: R. Skubisz (red.), *Internet – problemy prawne*, Lublin 1999, s. 266 oraz bliżej J. Jakubski, *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo” 1996, nr 12, s. 36.

¹⁰ M.in. J. Hajdukiewicz, *E-przestępczość...*, op. cit., s. 8.

¹¹ Zob. bliżej J. Bojarski, *Przestępstwa gospodarcze związane z działalnością banków*, Toruń 2001, s. 41 in.

o minimalne kwoty i przekazuje je na rachunek sprawcy); manipulację wynikiem, zwaną manipulacją urządzeniami wyjścia–wejścia, która polega na wykorzystywaniu ogólnie dostępnych peryferii komputerów i systemów, np. przestępstwa dokonywane za pomocą bankomatów (na szkodę banków i ich klientów) i oszustwa dokonywane przez właścicieli automatów do gier¹².

Zgodnie z ustaleniami M. Klisia, który zwraca uwagę na wprost nieograniczone możliwości dokonywania oszustw stwarzane przez Internet i na fakt, że oszustwo w sieci połączone jest integralnie z hackingiem komputerowym (który stanowi element konieczny do dokonania takiego przestępstwa), podstawowym oszustwem w cyberprzestrzeni jest posługiwanie się skradzionym wcześniej numerem karty kredytowej, a dysponowanie numerem karty pozwala na okradanie banków, kas i ubezpieczycieli, na wypożyczanie samochodów, na dokonywanie zakupów w sklepach internetowych. Kolejnym rodzajem oszustwa jest manipulacja programem (tak by system wykonywał określone czynności bez woli operatora), np. poprzez włamanie się do systemu bankowego podrzucenie programu obcinającego minimalne kwoty z rachunków bankowych, które przesyłane są na jedno konto. Autor ten wymienia też fałszerstwa listy płac jako klasyczne oszustwo omawianego typu (pobory tzw. „martwych dusz” przelewane są na konto przestępcy), a także inne przestępstwa wskazujące na nieograniczoną pomysłowość w ich popełnianiu, jak np. przekierunkowywanie rozmów telefonicznych z lokalnych providerów na numery pobierające dużo wyższe stawki¹³.

Szczególnie rozległa problematyka wiąże się z oszustwami związanymi z posługiwaniami się kartami płatniczymi (kredytowymi), w tym z użyciem posiadanych informacji o numerach kart kredytowych niebędących własnością sprawcy. Jako przykłady wyłudzenia mienia za pośrednictwem Internetu (art. 287 polskiego k.k.) w taki właśnie sposób w literaturze dotyczącej praktyki policyjnej podaje się wyłudzenia karnetów lotniczych, wydawnictw książkowych, wyłudzenia różnych towarów i usług w sklepach sieci komputerowej Internetu¹⁴. Także inne oszustwa związane z użyciem kart płatniczych (kredytowych), jako często występujące w praktyce, cieszą się dużym zainteresowaniem w polskich publikacjach prawniczych¹⁵. Co się tyczy natomiast oszustw na szkodę ZUS-u, wskazuje się

¹² K.J. Jakubski, *Przestępczość komputerowa – próba zdefiniowania zjawiska...*, op. cit., s. 266–268 i podana tam literatura oraz K.J. Jakubski, *Przestępczość komputerowa...*, op. cit., s. 36–38.

¹³ M. Kliš, *Przestępczość w Internecie...*, op. cit., s. 11–12.

¹⁴ J. Kosiński, *Przykład wykorzystania nowoczesnych technologii przetwarzania informacji do dokonania przestępstwa*, w: T. Zasępa (red.), R. Chmura (współpr. red.), *Internet. Fenomen społeczeństwa informacyjnego*, Częstochowa 2001, s. 601 i n., zwłaszcza s. 613–615.

¹⁵ Zob. m.in. A. Adamski, *Nadużycia związane z kartami płatniczymi i ich karalność*, w: A. Adamski (red.), *Przestępczość gospodarcza z perspektywy Polski i Unii Europejskiej*. Materiały z Konferencji międzynarodowej (Mikołajki 26–28 września 2000 r.), Toruń 2003; J. Kukulski, J. Pluta, *Karty płatnicze. Teoria i praktyka*, Warszawa 1998; R. Łuczak, M. Wojtas, K. Woźniak, *Przestępstwa związane z obrotem kartami płatniczymi*, Warszawa 1996; K.J. Jakubski, *Wyłudzenie towarów i usług na podstawie numerów kart kredytowych przez Internet*, w: R. Skubisz (red.), *Internet 2000. Prawo – ekonomia – kultura*, Lublin 2000, s. 249 i n.; K.J. Jakubski, *Przestępstwa związane z użyciem kart*, „Prawo Bankowe” 1998, nr 2; K.J. Jakubski, *Przestępstwa na szkodę bankowych systemów kart płatniczych, rynek kart płatniczych*. Dodatek do Prawa bankowego z października 2000 r., nr 3; K.J. Jakubski, *Ściganie oszustw w sieci (...)*; K.J. Jakubski, *Wybrane aspekty prawnej ochrony systemu kart płat-*

na takie występujące w praktyce policyjnej zachowania, jak wprowadzanie „martwych dusz” świadczeniobiorców lub fikcyjne zasiłki pogrzebowe¹⁶.

Jak wskazuje J. Kosiński (zwracając zarazem uwagę na dużą tzw. ciemną liczbę cyberprzestępstw), w latach 1999–2001 liczba stwierdzonych przestępstw oszustwa komputerowego kształtowała się na poziomie od 207 w 1999 r., do 323 w 2000 r. i 279 w 2001 r.¹⁷ Według statystyk Ministerstwa Sprawiedliwości prawomocne skazania osób dorosłych za czyn z art. 287 k.k. były nieliczne. I tak np. w 1999 r. skazano 33 osoby, w roku 2003 – 46 osób, a w roku 2005 – 43 osoby.

W środkach masowego przekazu, na podstawie wywiadów z pracownikami Policji, podkreśla się, że największym problemem związanym z łamaniem prawa za pomocą Internetu jest działanie oszustów. Píše się o nielegalnych transakcjach oszustów internetowych oraz o wysokiej wykrywalności tych przestępstw. W 2002 r. stwierdzono 368 oszustw komputerowych¹⁸.

Niedawno środki masowego przekazu informowały zwłaszcza o instalowaniu w sieci specjalnych programów (dialerów, czyli programów modyfikujących numery wybierane przez modem służący użytkownikowi do połączenia z Internetem) instalowanych w sieci komputerowej przez operatorów bez informowania abonentów, że wchodząc na niektóre strony internetowe przełączani są na numery 0–700, co oznaczało dużo droższe opłaty za połączenia. I tak, zgodnie z informacjami prasowymi, Urząd Ochrony Konkurencji i Konsumentów wszczął postępowanie przeciwko Telekomunikacji Polskiej S.A. i poczynił obserwacje operatorów (*sernice providerów*)¹⁹. Po skargach klientów korzystających z sieci Internet za pomocą modemów Urząd Regulacji Telekomunikacji i Poczty w okresie od 14 maja do 13 czerwca 2003 r. kontrolował świadczenie tych usług przez Telekomunikację Polską S.A. Prezes tego Urzędu m.in. wystąpił do ministra infrastruktury z propozycją wprowadzenia aktem prawnym uprawnienia abonenta do żądania nieodpłatnego zablokowania dostępu do numerów 0–700. Uznał za-

nicznych, w: E. Gruza, T.R. Tomaszewski (red.), *Problemy współczesnej kryminalistyki*, t. IV, Warszawa 2001, s. 117 i n.; J. Bojarski, *Przestępstwa gospodarcze...*, op. cit., s. 53 i n.; G. Rejman, *Falszowanie pieniędzy i papierów wartościowych* (art. 310 § 1 k.k.), „Przegląd Prawa Karnego” 2001, nr 21, s. 29 i n.; J. Skorupka, *Przestępstwa przeciwko obrotowi pieniędzmi i papierami wartościowymi. Rozdział XXXVII Kodeksu karnego. Komentarz*, Warszawa 2002 i podana tam literatura; J. Piórkowska-Flieger, *Falsz dokumentu w polskim prawie karnym*, Kraków 2004; M. Samcik, J. Iskra, *Karty płatnicze. Nowe prawo lepiej chroni klientów banków. Chlip, chlip, gdyby to był chip*, „Gazeta Wyborcza” z 27 sierpnia 2003 r., s. 22–23.

¹⁶ Zob. J. Liszewski, *Oszustwa popełniane z wykorzystaniem komputera w Polsce (dwa studia przypadków)*, w: A. Adamski (red.), *Przestępczość komputerowa. Prawne aspekty nadużyć...*, op. cit., s. 53 i n.

¹⁷ J. Kosiński, *Przestępczość komputerowa w statystyce policyjnej*, w: T. Zasępa, R. Chmura (red.), *Internet i nowe technologie – ku społeczeństwu przyszłości*, Częstochowa 2003, s. 539 i n. Co się tyczy problemów praktyki patrz też szczególnie K.J. Jakubski, *Ściganie oszustw w sieci* (wybrane zagadnienia), w: T. Zasępa, R. Chmura (red.), op. cit., s. 549 i n. oraz J.W. Wójcik, *Przestępstwa komputerowe...*, op. cit. Część I i Część II. *Techniki zapobiegania*, Warszawa 1999, i podana tam literatura.

¹⁸ P. Ożadowicz, *Śmieci sieci. Przestępczość. Internetowe paragrafy*, „Trybuna” z 18 sierpnia 2003 r., s. 4 (na podstawie wywiadu z M. Szyndlerem z Biura Prasowego Komendy Głównej Policji). Zob. też E. Grochala-Włodek, *Złodziej czyha w sieci*, „Gazeta Prawna” 2005, nr 54.

¹⁹ Zob. H.F., *Za rozrywkę w Internecie płaci się. Seksstrony kosztują drożej, lecz internauta musi o tym wiedzieć*, „Rzeczpospolita” z 29 lipca 2003 r., s. C2.

razem za niewystarczające takie działania Telekomunikacji Polskiej S.A., mające na celu poprawę ochrony interesów abonentów, jak ogłoszenie konkursu na program antydialerowy i zmiany umów z dostawcami usług 0–700 oraz autoryzacja dialerów²⁰.

Zbliżoną działalność prowadziły też wyspecjalizowane grupy tzw. telefonicznych włamywaczy, to jest hackerów podłączających się do cudzych telefonów²¹ lub organizatorzy nielegalnych central telefonicznych²².

W środkach masowego przekazu opisywane były też występujące w praktyce takie sposoby działania sprawców, jak oszukańcze wypożyczanie łodzi przez ogłaszające się w Internecie firmy, zajmujące się czarterowaniem łodzi. Opisywane były również przypadki oszustów sprzedających przez Internet fałszywe dokumenty (jak dyplomy wyższych uczelni), a także przede wszystkim dokonujących kradzieży pieniędzy z kont bankowych, z wykorzystaniem do tego bankomatów.

II

Przestępstwo oszustwa komputerowego zostało wprowadzone do polskiego ustawodawstwa karnego Kodeksem karnym z 1997 r. i ujęte w art. 287 tego kodeksu. W uzasadnieniu do rządowego projektu tego kodeksu podkreślono, że wprowadzenie przepisu o oszustwie komputerowym było niezbędne, ponieważ tradycyjne pojęcie oszustwa zawiera znamiona, które przy komputerowym oszustwie nie są spełniane, choć nienależna korzyść może być osiągnięta. (Chodzi o znamiona wprowadzenia w błąd innej osoby, wyzyskania jej błędu lub niezdolności do należytego pojmowania przedsiębranego działania, doprowadzenia jej do niekorzystnego rozporządzenia mieniem)²³.

W literaturze przedmiotu wskazuje się na dwie przyczyny (dwa powody) wprowadzenia tego nowego typu przestępstwa do polskiego k.k. Po pierwsze, chodziło o zobowiązania międzynarodowe dotyczące kryminalizacji nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji, a po drugie, o konieczność uwzględnienia zagrożeń polegających na tym, że stało się technicznie możliwe dokonanie bezprawnych przesunień majątkowych poprzez wprowadzenie odpowiednich dyspozycji do oprogramowania obsługi operacji finansowych, czy też obsługi zgromadzonego kapitału bankowego²⁴,

²⁰ T.ŚW. *Blokada powinna być za darmo. Telekomunikacja. Dialerowa kontrola URTiP*, „Rzeczpospolita” z 19–20 lipca 2003 r., s. B3.

²¹ Bliżej zob. R. Krupa-Dąbrowska, *Telefoniczni włamywacze nie mają wakacji. Właściwe zabezpieczenie aparatu może ustrzec przed niespodziewanie wysokim rachunkiem*, „Rzeczpospolita” z 13–14 lipca 2002 r. (żółte strony). Zob. też M. Białkowski, *Oszustwo komputerowe*, GS 2002, nr 6.

²² Zob. J.W. Wójcik, *Przestępstwa w biznesie, zapobieganie*, tom I, *Afery gospodarcze, łańcuszki, piramidy, parabanki. Oszustwa ubezpieczeniowe, manipulacje giełdowe*, bez daty, s. 38.

²³ Por. *Kodeks Karny, Kodeks Postępowania Karnego, Kodeks Karny Wykonawczy. Nowe kodeksy karne – z 1997 r. z uzasadnieniem*, Warszawa 1997, s. 206–207.

²⁴ M.in. S. Łagodziński, *Przestępstwa przeciwko mieniu w kodeksie karnym (wybrane zagadnienia)*, „Prokuratura i Prawo” 1999, nr 2, s. 16; zob. P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, „Przegląd Sądowy” 2000, nr 11–12, s. 43 i n.

czyli mówiąc w skrócie o przystosowanie naszego prawa karnego do nowoczesnych form ataku, powstałych w wyniku rozwoju technologii cyfrowych²⁵.

Art. 287 § 1 k.k. był zmieniany ustawą z 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz.U. Nr 69, poz. 626), która to ustawa weszła w życie w dniu 1 maja 2004 r., czyli w dniu wejścia Polski do Unii Europejskiej (zob. art. 1 pkt 11 tej ustawy). Po tej zmianie art. 287 § 1 k.k. ma treść następującą: „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”. Przed wspomnianą zmianą przepis ten stanowił: „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”. Z kolei § 2 (który nie był zmieniany wspomnianą ustawą) stanowi: „W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku”. Zgodnie z § 3 (który także nie był zmieniany): „Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego”. Wspomniana zmiana w § 1 cytowanego przepisu związana była z Konwencją dotyczącą cyberprzestępczości.

Jak widać, w kodeksie jest mowa o celu osiągnięcia korzyści majątkowej. W związku z tym wskazać warto, że od 1 lipca 2003 r. (czyli od dnia wejścia w życie ustawy z 13 czerwca 2003 r. zmieniającej m.in. kodeks karny) przez pojęcie korzyści majątkowej (lub osobistej) rozumiemy, zgodnie z nowym ujęciem treści art. 115 § 4 k.k., korzyść zarówno dla siebie, jak i dla kogo innego²⁶.

W art. 294 k.k. przewidziano postać kwalifikowaną omawianego przestępstwa. Jest ona zagrożona surową karą pozbawienia wolności od roku do lat 10 i ma miejsce wtedy, gdy sprawca dopuszcza się oszustwa komputerowego (określonego w art. 287 § 1 k.k.) w stosunku do mienia znacznej wartości. Wyjaśnić trzeba, że mieniem znacznej wartości jest, zgodnie z polskim k.k., mienie, którego wartość w chwili popełnienia czynu zabronionego przekracza dwustukrotną wysokość najniższego miesięcznego wynagrodzenia (art. 115 § 5 k.k.). Taka sama surowa kara grozi sprawcy, który dopuszcza się omawianego przestępstwa w stosunku do dobra o szczególnym znaczeniu dla kultury. Tego rodzaju postać kwalifikowana dotyczy nie tylko oszustwa komputerowego, ale także innych, wymienionych w art. 294 k.k., przestępstw przeciwko mieniu.

Kodeks przewiduje szczególne możliwości zastosowania nadzwyczajnego złagodzenia kary, a nawet odstąpienia od wymierzenia kary, jeżeli sprawca oszustwa

²⁵ R. Korczyński, R. Koszut, „Oszustwo” komputerowe, „Prokuratura i Prawo” 2002, nr 2, s. 17.

²⁶ Ustawodawca uprościł pojęcie korzyści. Poprzednio bowiem przepis ten stanowił, że korzyścią majątkową jest korzyść dla siebie, dla innej osoby fizycznej lub prawnej, dla jednostki organizacyjnej niemającej osobowości prawnej, dla grupy osób prowadzącej zorganizowaną działalność przestępczą.

komputerowego (lub innych wymienionych w przepisie przestępstw) dobrowolnie naprawił szkodę w całości (albo zwrócił pojazd lub rzecz mającą szczególne znaczenie dla kultury w stanie nieuszkodzonym). Jeżeli dobrowolnie naprawił on szkodę w znacznej części, sąd może zastosować nadzwyczajne złagodzenie kary (art. 295 k.k.). Możliwość skorzystania z tych dobrodziejstw przez sprawcę oszustwa komputerowego, który dobrowolnie naprawił szkodę, została poddana krytyce w doktrynie, poprzez uznanie, że premiuje to czyny, których skutkiem jest szkoda (czyli czyny poważniejsze), w sytuacji gdy czyn z art. 287 k.k. jest przestępstwem formalnym²⁷.

Autorzy, którzy twierdzą, że omawiane przestępstwo jest przestępstwem tzw. formalnym (czyli bezskutkowym), rozumieją to w tym sensie, że skutek w postaci wyrządzenia innej osobie szkody lub osiągnięcia korzyści majątkowej nie należy do znamion przestępstwa. Wystarczy bowiem, że sprawca działa w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody. Choć sprawca może osiągnąć korzyść majątkową lub wyrządzić szkodę, skutek taki nie jest konieczny do zaistnienia omawianego przestępstwa, czego nikt z komentatorów k.k. nie kwestionuje. Dokonanie tego przestępstwa zachodzi więc już w momencie wpłynięcia na automatyczne przetwarzanie danych, wprowadzenie nowego zapisu danych informatycznych itp., czyli zanim nastąpiło przesunięcie w sferze majątkowej (powstanie zamierzonej szkody)²⁸.

Niemniej niektórzy autorzy uznają omawiane przestępstwo za przestępstwo materialne, to jest znamienne skutkiem, upatrując tego skutku nie w osiągnięciu korzyści majątkowej lub w wyrządzeniu szkody, lecz w tym, że sprawca dokonuje wpływu (wpływa) na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub dokonuje zmiany, usunięcia albo wprowadzenia nowego zapisu danych informatycznych²⁹. Osobiście także uważam, że oszustwo komputerowe jest przestępstwem materialnym, przy takim właśnie rozumieniu skutku.

Ustawodawca, w art. 287 k.k., wymienił kilka sposobów działania sprawcy. Przestępstwem jest bowiem po pierwsze – wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, po drugie – zmienianie takich danych, po trzecie – usuwanie takich danych i po czwarte – wprowadzanie nowego zapisu danych informatycznych. A zatem w omawianym przepisie wyróżniono kilka sposobów czynności sprawczej. Niemniej w doktrynie owe sposoby czynności sprawczej ujmuje się w dwóch grupach³⁰, co wynika z tego, że – jak na to zwraca uwagę O. Gómiok – pierwsza z owych grup obejmu-

²⁷ A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 121–122.

²⁸ K. Buchała, *Reforma polskiego prawa karnego materialnego. Przestępstwa przeciwko ochronie informacji i oszustwo komputerowe*, w: A. Adamski (red.), *Przestępczość komputerowa. Prawne aspekty nadużyć...*, op. cit., s. 137.

²⁹ M. Dąbrowska-Kardas, P. Kardas, w: A. Zoll (red.), G. Bogdan, K. Buchała, Z. Cwiakalski, M. Dąbrowska-Kardas, P. Kardas, J. Majewski, M. Rodzyńkiewicz, M. Szewczyk, W. Wróbel, A. Zoll; zob. też wyd. II, Kraków 2006 (przy zmianie niektórych autorów), s. 346; *Kodeks karny. Część szczególna. Komentarz do art. 278–363 Kodeksu karnego*, Kraków 1999, s. 181.

³⁰ P. Kardas wyróżnia dwie formy oszustwa komputerowego. Por. P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, op. cit., s. 58–59.

je tzw. wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, a składają się nań tzw. manipulacje komputerowe, dokonane zarówno na wejściu (*input manipulation*), jak i na wyjściu (*output manipulation*). Przykładem manipulacji dokonywanych na wejściu jest wpisanie przez zatrudnionego w firmie operatora skomputeryzowanej listy płac do tej listy fikcyjnych nadgodzin, a na wyjściu – wystawienie za pomocą komputera tzw. podwójnych rachunków. Czynności drugiej grupy natomiast zmieniają lub zastępują dotychczasowy obraz (zapis) danych informatycznych. Druga grupa obejmuje zmienianie, usuwanie, wprowadzanie nowego zapisu danych informatycznych i do tych czynności odnosi się ściślej rozumiana nazwa „oszustwo komputerowe”³¹. Natomiast zdaniem B. Michalskiego wyróżniono trzy zasadnicze odmiany zachowań wyczerpujących znamiona przestępstwa z art. 287 k.k.: 1) manipulacji danymi polegającej na wprowadzeniu nieprawdziwych danych w celu zyskania nienależnych korzyści majątkowych (np. informacji o wyższym od rzeczywistego stanie konta sprawcy), 2) manipulacji programem polegającej na wprowadzeniu do programu takich informacji, które powodują samoczynne (niezależne od woli operatora) przysporzenie korzyści majątkowej, np. wprowadzenie „poleceń”, by od każdej operacji bankowej potrącać niewielką kwotę i przekazywać na wskazane konto, 3) manipulacji wynikiem polegającej na wykorzystaniu ogólnie dostępnych peryferii komputerów i systemów komputerowych, np. wystawianie podwójnych rachunków przy korzystaniu z karty płatniczej³². Niemniej po zmianach przepisu w 2004 r. B. Michalski także wyróżnił tylko dwie odmiany tego przestępstwa, to jest: 1) wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych (informacji) i 2) zmianę, usunięcie albo wprowadzenie nowego zapisu danych informatycznych³³.

W każdym z wymienionych przypadków ustawa wymaga działania bez upoważnienia, co zgodnie podkreślają komentatorzy k.k. Chodzi tu o upoważnienie prawne dysponenta danego systemu komputerowego lub komputera³⁴.

Najprostszym, jak się wydaje, przykładem omawianego czynu jest przykład podany przez J. Wojciechowskiego: włamanie się do sieci komputerowej banku i spowodowanie przelewu określonej kwoty na rachunek sprawcy³⁵.

Oszustwo komputerowe, zgodnie z systematyką kodeksu, jest przestępstwem przeciwko mieniu i jest ujęte w tym samym rozdziale przestępstw, w którym ujęte

³¹ O. Gómiok, w: O. Gómiok, S. Hoc, M. Kolutowski, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny. Komentarz*, Gdańsk 2002/2003, s. 1185 i powołany tam A. Adamski, *Przestępstwa komputerowe...*, op. cit., s. 145–146.

³² B. Michalski, *Przestępstwa przeciwko mieniu. Rozdział XXXV Kodeksu karnego. Komentarz*, Warszawa 1999, s. 223–224. Zob. też B. Michalski, w: A. Wąsek (red.), *Kodeks karny. Część szczególna. Tom II. Komentarz do artykułów 222–316*, wyd. 2, Warszawa 2005, s. 984. Por. też J.W. Wójcik, *Przestępstwa komputerowe. Część I...*, op. cit., s. 94 i n.

³³ B. Michalski, w: A. Wąsek (red.), *Kodeks karny...*, op. cit., s. 983. Zob. też wyd. 3, Warszawa 2006, s. 1043.

³⁴ O. Gómiok, w: O. Gómiok, S. Hoc, M. Kolutowski, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny*, s. 1185.

³⁵ J. Wojciechowski, *Kodeks karny*, wyd. II, poszerzone i uaktualnione. Komentarz, orzecznictwo, Warszawa 2000, s. 537.

są m.in. kradzież (w różnych jej postaciach), przywłaszczenie, „kradzież” impulsów telefonicznych, oszustwo, uszkodzenie mienia, paserstwo, paserstwo programu komputerowego. S. Łagodziński obejmuje te czyny mianem przestępstw „przeciw-majątkowych”³⁶. Niewątpliwie więc trafne jest twierdzenie wyrażane w literaturze przedmiotu, że art. 287 k.k. chroni mienie. Mienie zatem postrzegane jest jako zasadniczy przedmiot ochrony przy przestępstwie oszustwa komputerowego³⁷.

Jednocześnie jednak trafne jest twierdzenie, że przedmiotem ochrony z art. 287 k.k. są obok mienia także dane informatyczne o szczególnym charakterze, to znaczy ściśle związane z mieniem³⁸. P. Kardas³⁹ trafnie wymienia tu integralność, poufność oraz dostępność informacji (obecnie danych informatycznych) odnoszących się do mienia, podlegających automatycznemu gromadzeniu, przetwarzaniu lub przekazywaniu, a także integralność, poufność i dostępność zapisów dotyczących mienia, zawartych na komputerowych nośnikach informacji (obecnie danych informatycznych). Zgodzić się więc trzeba z twierdzeniem A. Adamskiego, że nienaruszalność danych jest ubocznym przedmiotem ochrony czynu zabronionego z art. 287 k.k.⁴⁰

Ustawa wymaga działania w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody. Oszustwo komputerowe jest zatem przestępstwem tzw. kierunkowym (celowym). Może przeto być popełnione wyłącznie z zamiarem bezpośrednim⁴¹ o szczególnym zabarwieniu (*dolus coloratus*). Motywacja wyrządzenia szkody innemu podmiotowi może wynikać np. z chęci zniszczenia konkurenta, doprowadzenia go do upadłości, bez odpowiadającej temu korzyści po stronie sprawcy⁴². Zdaniem J. Wojciechowskiego, zamierzona szkoda polegać może na samym tylko zniszczeniu lub zniekształceniu zapisu na komputerowym nośniku informacji (obecnie danych informatycznych), a także na sytuacji, gdy zniszczenie, uszkodzenie itd. zapisu informacji (obecnie danych informatycznych) jest tylko sposobem spowodowania innej szkody⁴³.

Pogląd natomiast, że przestępstwo to popełnione być może z tzw. zamiarem gwosf-ewentualnym, wyrażony przez R. Korczyńskiego i R. Koszuta⁴⁴, wymagałby bardziej dokładnego i bardziej przekonującego uzasadnienia, niż to uczynili Autorzy.

³⁶ S. Łagodziński, *Przestępstwa przeciwko mieniu w kodeksie karnym...*, op. cit., s. 7 i n.

³⁷ P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, op. cit., s. 55 oraz powołany tam S. Łagodziński, *Przestępstwa przeciwko mieniu w kodeksie karnym...*, op. cit., s. 8 i n.; B. Michalski, *Przestępstwa przeciwko mieniu...*, op. cit. Zob. jednak B. Michalski, w: A. Wąsek (red.), *Kodeks karny...*, op. cit., wyd. 2, Warszawa 2005, s. 981–982.

³⁸ Por. P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, op. cit., s. 57; zob. też powołany tam B. Michalski, *Przestępstwa przeciwko mieniu...*, op. cit., s. 221. Zob. również B. Michalski, w: A. Wąsek (red.), *Kodeks karny...*, op. cit., s. 981–982 i wyd. 3, Warszawa 2006, s. 1042.

³⁹ P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, op. cit., s. 57.

⁴⁰ A. Adamski, *Prawo karne komputerowe...*, op. cit., s. 116.

⁴¹ Por. O. Gómiok w: O. Gómiok, S. Hoc, M. Kolitowski, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny*, s. 1185; B. Michalski, *Przestępstwa przeciwko mieniu...*, op. cit., s. 224.

⁴² K. Buchała, *Reforma polskiego prawa karnego materialnego...*, op. cit., s. 136.

⁴³ J. Wojciechowski, *Kodeks karny*, wyd. II, op. cit., s. 538.

⁴⁴ R. Korczyński, R. Koszut, *„Oszustwo” komputerowe*, op. cit., s. 35 i n.

Wymieniona alternatywnie dwójaka motywacja, o której mowa w przepisie (celem sprawcy może być osiągnięcie korzyści majątkowej lub wyrządzenie innej osobie szkody), nie daje jednak, moim zdaniem, podstaw do wyodrębnienia w tym typie przestępstwa dwóch odmian, to jest oszustwa komputerowego i szkodnictwa komputerowego⁴⁵. Natomiast trafne jest spostrzeżenie, że ów pierwszy cel zbliża to przestępstwo do oszustwa, a drugi wskazuje na pokrewieństwo z tzw. sabotażem czy szkodnictwem komputerowym⁴⁶. Co się tyczy tej drugiej sytuacji, wskazać trzeba, że tzw. sabotaż komputerowy został wydatnie poszerzony w k.k. w 2004 r. poprzez dodanie nowych przepisów, tj. art. 268a i 269a k.k. Treść tych przepisów będzie podana dalej. Zmieniono też art. 269a k.k. Zmiany te miały na celu dostosowanie prawa polskiego do Konwencji o cyberprzestępczości⁴⁷.

Na tle art. 287 k.k. nasuwa się wiele problemów interpretacyjnych. Jednym z nich jest problem kwalifikacji prawnej czynów związanych z użyciem kart płatniczych⁴⁸. Problem ten jest przedmiotem odrębnego artykułu.

Szczegółne zainteresowanie w polskich publikacjach prawnokamych wzbudziło poszukiwanie cech zbieżnych oraz różnic między oszustwem komputerowym i klasycznym oszustwem⁴⁹. Jak twierdził K. Buchała: „W oszustwie dokonanym przy posłużeniu się narzędziem, jakim jest komputer, znika kontakt z dysponentem, znika element wprowadzenia go w błąd lub wykorzystania jego błędu oraz decyzja tego podmiotu, na skutek której następuje rozporządzenie mieniem własnym lub cudzym”⁵⁰. Jak wskazuje S. Łagodziński, wszystko to, co odnosi się do błędu pokrzywdzonego oraz czynności rozporządzenia przezeń mieniem, może być zastąpione dyspozycjami zawartymi w programie komputerowym, a ponadto realizacja oszustwa komputerowego odbywa się „poza plecami” i poza świadomością pokrzywdzonego. Pokrzywdzonym przy tym najczęściej bywa osoba prawna. Stało się technicznie możliwe dokonanie bezprawnych przesunięć majątkowych⁵¹.

Zdaniem niektórych autorów, art. 287 k.k. stanowi *lex specialis* w stosunku do art. 286 k.k., czyli oszustwo komputerowe stanowi *lex specialis* w stosunku do oszustwa tradycyjnego. Jednak poglądu tego nie podzielają inni autorzy. Tak np. J. Bojarski, choć przytacza ten pogląd M. Dąbrowskiej-Kardas i P. Kardasa, to zgadza się z A. Adamskim, twierdząc, że znamiona tych przestępstw nie pokrywają się i że nie ma oszustwa komputerowego, ale tylko oszustwo z art. 286 k.k. w sytuacji, gdy sprawca wykorzystuje technologię przetwarzania danych jako narzędzie do wprowadzenia w błąd konkretnej osoby. A zatem przestępstwo

⁴⁵ Wyróżnia je S. Łagodziński, *Przestępstwa przeciwko mieniu w kodeksie karnym...*, op. cit.

⁴⁶ O. Gómiok w: O. Gómiok, S. Hoc, M. Koliński, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny*, s. 1185.

⁴⁷ Bliżej zob. B. Kunicka-Michalska, w: A. Wąsek (red.), *Kodeks karny...*, op. cit. Komentarz do artykułów 222–316, wyd. 2, Warszawa 2005, zwłaszcza s. 588–589, 595 i 602 i wyd. 3, Warszawa 2006, s. 625–626, 632, 639.

⁴⁸ Zob. też literatura podana w przyp. 15.

⁴⁹ Zob. m.in. R. Korczyński, R. Koszut, „Oszustwo” komputerowe, op. cit., s. 17 i n.

⁵⁰ K. Buchała, *Reforma polskiego prawa karnego materialnego...*, op. cit., s. 130.

⁵¹ S. Łagodziński, *Przestępstwa przeciwko mieniu w kodeksie karnym...*, op. cit., s. 16.

z art. 287 k.k. miałoby miejsce wtedy, gdyby sprawca uzyskał korzyść lub powodował szkodę bez oddziaływania na proces decyzyjny konkretnej osoby, natomiast gdyby za pośrednictwem wskazanych działań wprowadzał kogoś w błąd – byłoby to oszustwo tradycyjne z art. 286 k.k.⁵²

W związku z tą ostatnią sytuacją wyróżnia się też w doktrynie oszustwa komputerowe właściwe i niewłaściwe⁵³.

B. Michalski podkreśla, że między przestępstwem oszustwa tradycyjnego a oszustwa komputerowego występują istotne różnice w zakresie ich przedmiotu, sposobu działania sprawcy oraz strony podmiotowej⁵⁴.

III

Kary grożące za omawiane przestępstwo, o których była wyżej mowa, zostały przewidziane w części szczególnej k.k. Niemniej ponadto, na mocy przepisów części ogólnej k.k., sąd może wymierzyć obok kary pozbawienia wolności grzywnę, w wypadkach jeżeli sprawca dopuścił się czynu w celu osiągnięcia korzyści majątkowej lub gdy korzyść majątkową osiągnął (art. 33 § 2 k.k.). Przepis ten może mieć zastosowanie do oszustw komputerowych (choć nie do wszystkich ich przypadków objętych artykułem 287 k.k.).

Okolicznością nadzwyczajnie zaostrzającą karę jest, oprócz recydywy, także sytuacja, gdy a) sprawca uczynił sobie z popełnienia przestępstwa stałe źródło dochodu lub b) popełnia przestępstwo, działając w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa, c) a także popełnia przestępstwo o charakterze terrorystycznym. Wówczas sąd wymierza karę pozbawienia wolności przewidzianą za przypisane przestępstwo w wysokości powyżej dolnej granicy ustawowego zagrożenia, a może ją wymierzyć do górnej granicy ustawowego zagrożenia zwiększonego o połowę (art. 65 zmieniony ustawą z 16 kwietnia 2004 r. (Dz.U. Nr 93, poz. 889), która weszła w życie z dniem 1 maja 2004 r. i art. 64 § 2 k.k.).

Co się tyczy środków karnych, jest o nich mowa w rozdziale V k.k., do którego odsyłam Czytelnika. Szczególnie istotny jest środek kamy w postaci przepadku. W kodeksie karnym przewidziano przepadek przedmiotów oraz przepadek korzyści. Przepisy dotyczące przepadku były zmienione ustawą z 13 czerwca 2003 r. (Dz.U. Nr 111, poz. 1061), która weszła w życie w dniu 1 lipca 2003 r. Problematyka ta jest obszerna i ramy niniejszego artykułu nie pozwalają na jej pełne omówienie. Odsyłam przeto Czytelnika do treści art. 44 i 45 k.k. Istotną nowością, wprowadzoną w tych przepisach, jest domniemanie polegające na tym, że w razie skazania za przestępstwo, z którego popełnienia sprawca osiągnął,

⁵² J. Bojarski, *Przestępstwa gospodarcze związane z działalnością banków*, op. cit., s. 42; A. Adamski, *Przestępstwa komputerowe w nowym kodeksie karnym*, w: *Nowa kodyfikacja karna. Kodeks karny. Krótkie komentarze*, z. 17, Warszawa 1998, s. 135.

⁵³ K. Buchała, *Reforma polskiego prawa karnego materialnego...*, op. cit., s. 135–136.

⁵⁴ B. Michalski, *Przestępstwa przeciwko mieniu...*, op. cit., s. 219–220. Zob. też B. Michalski, w: A. Wąsek (red.), *Kodeks karny...*, op. cit., s. 980 i wyd. 3, Warszawa 2006, s. 1040.

choćby pośrednio, korzyść majątkową znacznej wartości, uważa się, że mienie, które sprawca objął we władanie lub do którego uzyskał jakikolwiek tytuł w czasie popełnienia przestępstwa lub po jego popełnieniu, do chwili wydania chociażby nieprawomocnego wyroku, stanowi korzyść uzyskaną z popełnienia przestępstwa, chyba że sprawca lub inna zainteresowana osoba przedstawi dowód przeciwny (art. 45 § 2 k.k.). Przepis ten może być zastosowany m.in. do sprawcy skazanego za oszustwo komputerowe, jeśli osiągnął on z popełnienia tego przestępstwa, chociażby pośrednio, korzyść majątkową znacznej wartości. Jak stanowi § 3 art. 45 k.k., przewidujący dalsze domniemanie, jeżeli okoliczności sprawy wskazują na duże prawdopodobieństwo, że sprawca taki przeniósł na osobę fizyczną, prawną lub jednostkę organizacyjną niemającą osobowości prawnej, faktycznie lub pod jakimkolwiek tytułem prawnym, mienie stanowiące korzyść uzyskaną z popełnienia przestępstwa, uważa się, że rzeczy będące w samoistnym posiadaniu tej osoby lub jednostki oraz przysługujące jej prawa majątkowe należą do sprawcy, chyba że zainteresowana osoba lub jednostka organizacyjna przedstawi dowód zgodny z prawem ich uzyskania. Przepis ten także może mieć zastosowanie m.in. do sprawcy oszustwa komputerowego, jeśli spełnione będą warunki w nim przewidziane. Owe wprowadzone w 2003 r. domniemania wywołują nie tylko pochwały lecz także kontrowersje⁵⁵.

W wypadku skazania za przestępstwo przynoszące korzyść majątkową osobie fizycznej, prawnej lub jednostce organizacyjnej niemającej osobowości prawnej, a popełnione przez sprawcę działającego w jej imieniu lub interesie, sąd zobowiązuje podmiot, który uzyskał korzyść majątkową, do jej zwrotu w całości lub w części na rzecz Skarbu Państwa; nie dotyczy to korzyści majątkowej podlegającej zwrotowi innemu podmiotowi (art. 52 k.k.).

Jeśli sprawca przy popełnieniu oszustwa komputerowego nadużył stanowiska lub wykonywanego zawodu albo okazał, że dalsze zajmowanie stanowiska lub wykonywanie zawodu zagraża istotnym dobrom chronionym prawem, sąd może orzec zakaz zajmowania określonego stanowiska albo wykonywania określonego zawodu (art. 41 § 1 k.k.). Jeśli zaś skazano sprawcę za przestępstwo popełnione w związku z prowadzeniem określonej działalności gospodarczej, to jeżeli dalsze prowadzenie takiej działalności zagraża istotnym dobrom chronionym prawem, sąd może orzec zakaz prowadzenia takiej działalności (art. 41 § 2 k.k.). Zob. też wprowadzone ustawą z 27 lipca 2005 r. (Dz.U. Nr 163, poz. 1363) nowe paragrafy 1a i 1b art. 41 k.k. oraz art. 41a k.k.

IV

Przestępstwo oszustwa komputerowego znalazło się wśród przestępstw, których popełnienie przez określone osoby fizyczne, pociągnąć może za sobą odpowiedzialność podmiotów zbiorowych, na mocy ustawy z 28 października 2002 r.

⁵⁵ Por. m.in. krytykujący te domniemania artykuł A. Rybak, *Zmienione przepisy kodeksu karnego o przypadku przedmiotów służących bądź przeznaczonych do popełnienia przestępstwa. Jak udowodnić, że samochód nie jest wielbłądem*, „Rzeczpospolita” z 30 lipca 2003 r., s. C3.

o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz.U. Nr 197, poz. 1661 z późn. zm.). Skromne ramy niniejszego artykułu nie pozwalają na jej bliższe omówienie⁵⁶.

V

Oprócz art. 287 k.k., przestępstw komputerowych dotyczą też inne przepisy kodeksu karnego. Przestępstwo oszustwa komputerowego z art. 287 k.k. jest w dużym stopniu spokrewnione z innymi przestępstwami komputerowymi, które są ujęte w polskim ustawodawstwie karnym i wywołują duże zainteresowanie w polskich publikacjach prawniczych⁵⁷.

Istotne podobieństwa do ujęcia oszustwa komputerowego daje się zauważyć w sposobie określenia strony przedmiotowej przestępstw przeciwko ochronie informacji, ujętych w art. 267, 268, 268a i 269 k.k.⁵⁸ Chodzi tu o przestępstwa komputerowe polegające na naruszeniu tajemnicy korespondencji i cudzej tajemnicy, niszczeniu zapisu informacji i niszczeniu informacji komputerowej (sabotażu komputerowym)⁵⁹. Trafnie A. Adamski twierdzi, że z uwagi na to, iż podstawowa różnica tkwi w stronie podmiotowej (w przypadku art. 287 k.k. chodzi o chęć osiągnięcia korzyści majątkowej lub wyrządzenia szkody innej osobie), art. 287 k.k. stanowić będzie w wielu przypadkach *lex specialis* w stosunku do wymienionych przepisów dotyczących zamachów na bezpieczeństwo elektroniczne przetwarzanej informacji⁶⁰. Na możliwość pozostawiania czynu z art. 287 k.k. w pewnych wypadkach w zbiegu kumulatywnym z czynem z art. 268 § 2 k.k., wskazuje J. Wojciechowski. Jednak, jak pisze ten Autor, zakresy tych przepisów są różne. Czyn z art. 287 k.k. może, ale nie musi, jak czyn z art. 268 § 2 k.k., polegać na utrudnianiu odczytania informacji⁶¹. O. Gómiok zwraca uwagę na to, że zachodzi zbieg z art. 268 § 2 k.k., z którym to przepisem omawiany przepis się krzyżuje, art. 268 § 2 k.k. może być pochłonięty (choć nie musi) przez art. 287 § 1 k.k.⁶² Zdaniem B. Michalskiego, w przypadkach gdy dokonanie oszustwa komputerowego możliwe jest dopiero po pokonaniu przez sprawcę zabezpieczeń

⁵⁶ Z najnowszej literatury na ten temat zob. J. Warylewski, J. Potulski, *Odpowiedzialność podmiotów zbiorowych w prawie polskim i europejskim. Komentarz*, Bydgoszcz–Gdańsk 2007, s. 190–191.

⁵⁷ Zob. literatura dotycząca przestępstw komputerowych podana w: B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz*, Warszawa 2000, s. 379 i n. oraz B. Kunicka-Michalska, w: A. Wąsek (red.), *Kodeks karny...*, op. cit., s. 445–447 i wyd. 3 (2006 r.), s. 478–481, w tym polskie referaty przygotowane na spotkanie w Katanii w ramach Programu Grotius II Penal (A. Adamskiego, B. Kunickiej-Michalskiej, B. Świątkiewicz, J. Jakubowskiej-Hara, C. Nowak, R.A. Stefańskiego, A. Łopatki, A. Wiśniewskiego), opublikowane w *Studiach Prawniczych* 2005, nr 4, s. 49–140 i podana tam literatura, a także nowa literatura podana w referacie B. Kunickiej-Michalskiej, ibidem, s. 87, przypis 31.

⁵⁸ Por. A. Adamski, *Prawo karne komputerowe*, op. cit., s. 116–117.

⁵⁹ Bliżej o tych przestępstwach zob. B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości...*, op. cit., s. 487 i n.

⁶⁰ A. Adamski, *Prawo karne komputerowe*, op. cit., s. 117.

⁶¹ J. Wojciechowski, *Kodeks karny*, wyd. II, op. cit., s. 538.

⁶² O. Gómiok w: O. Gómiok, S. Hoc, M. Kolitowski, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny*, s. 1185.

w postaci hasła, kodów itp., to jest gdy sprawca po „włamaniu” się do systemu komputerowego (hacking), czyli po rozszyfrowaniu hasła lub kodu zabezpieczającego system, realizuje znamiona czasownikowe występuku z art. 287 k.k., to czyn taki należy kwalifikować dodatkowo również na podstawie art. 267 § 1 k.k., który pozostaje wtedy w kumulatywnym zbiegu⁶³. Nie podzielam tego poglądu, sądzę bowiem, że wówczas art. 267 § 1 k.k. zostaje pochłonięty przez art. 287 k.k. Zdaniem M. Dąbrowskiej-Kardas i P. Kardasa przepis art. 287 § 1 k.k. stanowi *lex specialis* w stosunku do art. 268 k.k., co wyklucza możliwość przyjęcia kumulatywnego zbiegu⁶⁴.

Spośród przestępstw komputerowych, ujętych w k.k., najbardziej zbliżone do oszustwa komputerowego będzie fałszerstwo komputerowe⁶⁵.

Szczególną uwagę trzeba zwrócić na art. 268a wprowadzony do k.k. ustawą z 18 marca 2004 r. (Dz.U. Nr 69, poz. 626), która weszła w życie z dniem 1 maja 2004 r. Treść tego przepisu zostanie podana dalej. Zob. też inne przepisy, dodane do rozdziału XXXIII k.k., o których mowa dalej.

Odrębnego opracowania wymaga zagadnienie dotyczące tego, w jakim stopniu różne przestępstwa komputerowe są przestępstwami podobnymi w rozumieniu art. 115 § 3 k.k., jako przestępstwa „należące do tego samego rodzaju”. Problem ten wykracza poza ramy niniejszego artykułu. Niemniej nie ulega wątpliwości, że wszystkie przestępstwa popełnione w celu osiągnięcia korzyści majątkowej uważa się za przestępstwa podobne. A zatem oszustwo komputerowe, popełnione w celu osiągnięcia korzyści majątkowej, będzie przestępstwem podobnym do przestępstw popełnionych w celu osiągnięcia korzyści majątkowej, nawet gdyby nie były one przestępstwami komputerowymi (informatycznymi).

VI

Nie można też zapominać o licznych ustawach szczególnych, łączących się z problematyką przestępstw i wykroczeń, związanych z systemami informatycznymi. Wymienić trzeba zwłaszcza następujące ustawy: z 29 sierpnia 1997 r. – Prawo bankowe (tekst jedn. Dz.U. z 2002 r. Nr 72, poz. 665 z późn. zm.); z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jedn. Dz.U. z 2003 r. Nr 153, poz. 1503 z późn. zm.); z 28 września 1991 r. o kontroli skarbowej (tekst jedn. Dz.U. z 2004 r. Nr 8, poz. 65 z późn. zm.); z 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym (Dz.U. Nr 183, poz. 1537); z 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego warto-

⁶³ B. Michalski, *Przestępstwa przeciwko mieniu...*, op. cit., s. 224.

⁶⁴ M. Dąbrowska-Kardas, P. Kardas, w: A. Zoll (red.), *Kodeks karny...*, op. cit., s. 184.

⁶⁵ Bliżej zob. A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001, s. 46–47 i P. Kardas, który wymienia art. 270 § 1 k.k. (*Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Prawnych” 2000, rok IV, z. 1, s. 52) mówiąc o fałszerstwie komputerowego zapisu informacji stanowiącego dokument.

ści majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (tekst jedn. Dz.U. z 2003 r. Nr 153, poz. 1505 z późn. zm.); z 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (Dz.U. Nr 123, poz. 1351 z późn. zm.); z 19 listopada 1999 r. – Prawo działalności gospodarczej (Dz.U. Nr 101, poz. 1178 z późn. zm.); z 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. Nr 173, poz. 1807 z późn. zm.); z 27 maja 2004 r. o funduszach inwestycyjnych Dz.U. Nr 146, poz. 1546 z późn. zm.); z 29 sierpnia 1997 r. – Ordynacja podatkowa (tekst jedn. Dz.U. z 2005 r. Nr 8, poz. 60 z późn. zm.); z 30 czerwca 2005 r. o finansach publicznych (Dz.U. Nr 249, poz. 2104); z 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. Nr 183, poz. 1538); z 22 sierpnia 1997 r. o pracowniczych programach emerytalnych (tekst jedn. Dz.U. z 2001 r. Nr 60, poz. 623 z późn. zm.); z 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (tekst jedn. Dz.U. z 2004 r. Nr 159, poz. 1667 z późn. zm.); z 15 września 2000 r. – Kodeks Spółek Handlowych (Dz.U. Nr 94, poz. 1037 z późn. zm.); z 15 grudnia 2000 r. o ochronie konkurencji i konsumentów (Dz.U. Nr 122, poz. 1319 z późn. zm.); z 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. Nr 22, poz. 271); z 5 lipca 2001 r. o cenach (Dz.U. Nr 97, poz. 1050 z późn. zm.); z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn. Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.); z 30 czerwca 2000 r. – Prawo własności przemysłowej (Dz.U. z 2003 r. Nr 119, poz. 1117 z późn. zm.); z 27 lipca 2001 r. o ochronie baz danych (Dz.U. Nr 128, poz. 1402 z późn. zm.); z 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. Nr 112, poz. 1198 z późn. zm.); z 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz o Krajowym Systemie Informatycznym (tekst jedn. Dz.U. z 2006 r. Nr 216, poz. 1585 z późn. zm.); z 29 listopada 2000 r. o zbieraniu i wykorzystaniu danych rachunkowych z gospodarstw rolnych (Dz.U. Nr 3, poz. 20); z 22 stycznia 1999 r. o ochronie informacji niejawnych (tekst jedn. Dz.U. z 2005 r. Nr 196, poz. 1631 z późn. zm.); z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.); z 29 grudnia 1992 r. o radiofonii i telewizji (tekst jedn. Dz.U. z 2004 r. Nr 253, poz. 2531 z późn. zm.); z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800 z późn. zm.), w której to ustawie uwzględniono aż 8 dyrektyw Wspólnot Europejskich; z 29 czerwca 1995 r. o statystyce publicznej (Dz.U. Nr 88, poz. 439 z późn. zm.)⁶⁶.

Szczególnie istotne z punktu widzenia problematyki informatycznej są ustawy: z 18 września 2001 r. o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450

⁶⁶ Co do przepisów karnych wielu z wymienionych ustaw zob. bliżej M. Bojarski, W. Radecki, *Pozakodeksowe prawo karne*, tom II i III. Komentarz, Warszawa 2003.

z późn. zm.)⁶⁷; z 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. Nr 126, poz. 1068)⁶⁸; z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204 z późn. zm.), w której m.in. uznano za wykroczenie tzw. spam (czyli przesyłanie za pomocą środków komunikacji elektronicznej niezamówionych informacji handlowych (reklam)⁶⁹ oraz z 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz.U. Nr 169, poz. 1385 z późn. zm.). Zgodnie z tą ostatnią ustawą pojęcie „elektroniczny instrument płatniczy” oznacza: „każdy instrument płatniczy, w tym z dostępem do środków pieniężnych na odległość, umożliwiający posiadaczowi dokonywanie operacji przy użyciu elektronicznych nośników informacji lub elektroniczną identyfikację posiadacza niezbędną do dokonania operacji, w szczególności kartę płatniczą lub instrument pieniądza elektronicznego” (art. 2 pkt 4 ustawy). Ustawa zawiera przepisy dotyczące m.in. kart płatniczych usług bankowości elektronicznej i pieniądza elektronicznego. Przepisy karne zawarte są w art. 71–73 ustawy⁷⁰.

Zob. też uchwałę Sejmu RP z 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce (M.P. Nr 22, poz. 448) oraz ustawę z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565 z późn. zm.)⁷¹.

VII

Zdaniem A. Adamskiego, w art. 8 Konwencji o cyberprzestępczości ujęto oszustwo komputerowe w sposób węższy, niż to uczynił ustawodawca polski w k.k. z 1997 r. W Konwencji bowiem o dokonaniu tego przestępstwa decyduje wywołanie skutku w postaci utraty własności przez osobę pokrzywdzoną przestępstwem, w ujęciu zaś art. 287 polskiego k.k. istota czynu polega na usiłowaniu

⁶⁷ Bliżej o przepisach karnych tej ustawy zob. M. Bojarski, W. Radecki, *Pozakodeksowe prawo karne...*, op. cit., s. 174 i n. Z usługami certyfikacyjnymi i podpisem elektronicznym łączą się też liczne rozporządzenia.

⁶⁸ Zob. zwłaszcza art. 6–9 ustawy, zawierające przepisy karne, oraz bliżej m.in. M. Bojarski, W. Radecki, *Pozakodeksowe prawo karne. Suplement*, tom I i II: *Uzupełnienia, Aktualizacja, Nowości. Komentarz*, Warszawa 2003, s. 95 i n.

⁶⁹ Art. 287 k.k. nie obejmuje wysyłania do użytkowników Internetu materiałów reklamowych (ang. *spamming*), A. Adamski, *Prawo karne komputerowe*, op. cit., s. 118. Co się tyczy postanowień unijnych, wskazać warto, że w dniu 31 października 2003 r. weszła w życie Dyrektywa o ochronie danych osobowych w komunikacji elektronicznej, która nakłada na kraje członkowskie obowiązek wymuszenia zakazu wysyłania spamu za pomocą e-maili, SMS-ów, MMS-ów, lub faxów, jeśli odbiorca nie wyraził na to uprzednio zgody. Chronieni są przy tym tak użytkownicy indywidualni (obowiązkowo), jak i firmy i instytucje (fakultatywnie). Od 1 maja 2004 r. postanowieniami Dyrektywy objęta została Polska jako członek UE.

⁷⁰ Zob. bliżej M. Bojarski, W. Radecki, *Pozakodeksowe prawo karne. Suplement...*, op. cit., s. 86 i n.

⁷¹ Zob. także J. Kosiński (red.), *Przestępczość teleinformatyczna. VIII Seminarium naukowe*, Szczytno 2005; A. Godlewski, *Trendy w przestępczości elektronicznej*, „Przegląd Policyjny” 2006, nr 3, s. 93 i n., a także podana tam literatura oraz publikacje zamieszczone w: „Prawo mediów elektronicznych”, dodatek do „Monitora Prawniczego” 2006, nr 2, 2005, nr 3 i 12 oraz 2004, nr 4.

uzyskania korzyści majątkowej lub spowodowania szkody⁷², przez manipulowanie zapisem danych informatycznych, albo też na innym oddziaływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych. Toteż A. Adamski dochodzi do wniosku, że nie zachodzi potrzeba zmiany przepisów prawa polskiego ze względu na treść art. 8 Konwencji⁷³ w związku ze wskazaną kwestią. Pogląd ten zasługuje na poparcie.

Istotna z punktu widzenia zawartych tu rozważań jest ostatnia zmiana przepisu k.k., zawierającego definicję dokumentu. Chodzi o ustawę z 18 marca 2004 r. (Dz.U. Nr 69, poz. 626), którą oprócz wprowadzenia innych zmian zmieniono także definicję dokumentu zawartą w art. 115 § 14 k.k. Obecnie przepis ten stanowi: „Dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne”.

Co się zaś tyczy fałszerstwa komputerowego, o którym była wyżej mowa, oraz w odniesieniu do wytwarzania, rozpowszechniania, posiadania itd. tzw. „narzędzi hakerskich”, odsyłamy Czytelnika do rozważań A. Adamskiego⁷⁴.

Ustawą z dnia 18 marca 2004 r. poważnie zmodyfikowano rozdział XXXIII k.k., dotyczący przestępstw przeciwko ochronie informacji, o czym już była wyżej mowa. Dodano m.in. nowe przepisy to jest artykuły: 269a, 269b. Nowy art. 269a k.k. stanowi: „Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5”. Natomiast, zgodnie z nowym art. 269b § 1, karze pozbawienia wolności do lat 3 podlega ten, kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 2, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej. Zob. też § 2 art. 269b k.k. Jak widać, wśród wymienionych przestępstw nie znalazło się przestępstwo z art. 287 k.k. Wspomniane tu przestępstwo z art. 268a, także dodane do k.k. wymienioną ustawą popełnia ten, kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych. Postacią kwalifikowaną czynu jest wyrządzenie znacznej szkody majątkowej⁷⁵.

⁷² Por. też K. Buchała, *Reforma polskiego prawa karnego materialnego...*, op. cit., s. 136 oraz S. Łagodziński, *Przestępstwa przeciwko mieniu...*, op. cit., s. 16–17.

⁷³ A. Adamski, *Przestępczość w cyberprzestrzeni...*, op. cit., s. 48. Zob. też s. 46–47.

⁷⁴ Ibidem, s. 46–47 oraz s. 121 i 128.

⁷⁵ Bliżej zob. B. Kunicka-Michalska, w: A. Wąsek (red.), *Kodeks karny...*, op. cit., s. 451 i n., s. 588 i n. oraz wyd. 3, Warszawa 2006 r., s. 485 i n., s. 625 i n. i podana tam literatura; zob. też K. Gienas, *Zwalczanie cyberprzestępczości w świetle art. 269b kodeksu karnego – problem tzw. hacking*

W końcu marca 2006 r. wpłynął do Sejmu Obywatelski projekt ustawy – Kodeks karny z 11 lipca 2002 r. Na 15 posiedzeniu Sejmu nowej kadencji w dniu 7 kwietnia 2006 r. skierowano go do Komisji Nadzwyczajnej do spraw zmian w Kodyfikacjach. Do reprezentowania Komitetu Inicjatywy Ustawodawczej został upoważniony poseł Arkadiusz Mularczyk. Według intencji projektodawców projekt proponuje kompleksową reformę kodeksu karnego. Artykuł 294 w projekcie, odpowiednik obecnego art. 287 k.k. (oszustwo komputerowe), ma treść następującą: „§ 1. Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przysyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na elektronicznym nośniku informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 2. W wypadku mniejszej wagi sprawca podlega karze pozbawienia wolności do lat 2, ograniczenia wolności albo grzywny. § 3. Jeżeli czyn określony w § 1–2 popełniono na szkodę osoby najbliższej, ściąganie następuje na wniosek pokrzywdzonego”. Jak widać znamiona przestępstwa ujęte zostały w taki sam sposób jak w k.k. przed ostatnią zmianą art. 287 k.k., jedynie dawne sformułowanie „komputerowy nośnik informacji” zostało zastąpione sformułowaniem „elektroniczny nośnik informacji”. W projekcie podwyższono też karę za to przestępstwo. Zapewne w toku prac legislacyjnych przepis ten zostanie unowocześniony (jeśli projekt będzie miał szansę stać się nowym kodeksem karnym)⁷⁶.

W projekcie ustawy o zmianie ustawy – Kodeks Karny oraz niektórych innych ustaw, opracowanym w Ministerstwie Sprawiedliwości (projekt z dnia 23 listopada 2006 r.), nie przewidziano zmian w aktualnej treści art. 287 k.k.

Zagadnieniem wymagającym odrębnego rozważenia, nieobjętym niniejszą publikacją, jest problem ochrony interesów finansowych Unii Europejskiej za pomocą omówionych przepisów karnych⁷⁷.

tools, „Edukacja Prawnicza” 2006, nr 4, s. 40 i n.; W. Grzeszczyk, *Zmiany prawa karnego wprowadzane ustawą z dnia 18 marca 2004 r.*, „Prokuratura i Prawo” 2004, nr 7–8, s. 77 i n.; S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych. Wybrane zagadnienia*, Opole 2006, s. 299–311.

⁷⁶ Natomiast o propozycjach tzw. prezydenckiego projektu zmian k.k. zob. B. Kunicka-Michalska, *Ochrona informacji w Kodeksie karnym z 1997 r.* w: R. Budzinowski (red.), „Prawo i Administracja”, I. 1, Piła 2002, s. 19–22 i 26.

⁷⁷ Z bogatej literatury na temat ochrony interesów finansowych Unii Europejskiej por. szczególnie polskie referaty na temat *Oszustw godzących w interesy finansowe Unii Europejskiej*, wygłoszone na konferencji, która odbyła się w dniach 13–15 marca 2003 r. w Hiszpanii (Salamanka), w ramach programu UE „Grotius II Penal”, opublikowane w „Przeglądzie Prawa Karnego” 2005, nr 24, a zwłaszcza następujące: B. Kunicka-Michalska, *Wyłudzenia i przestępstwa zbliżone godzące w budżety wspólnotowe. Regulacje polskiego prawa karnego*, s. 7 i n.; L. Paprzycki, *Corpus Iuris 2000 – wersja florencka z 1999 r. a polski kodeks postępowania karnego z 1997 r. Problematyka harmonizacji*, s. 23 i n.; R.A. Stefański, *Wyłudzenia na szkodę budżetu Unii Europejskiej (analiza praktyki)*, s. 39 i n.; J. Wojciechowska, A. Wiśniewski, *Oszustwa na szkodę interesów finansowych Wspólnot Europejskich a polski kodeks karny i kodeks karny skarbowy*, s. 43 i n.; C. Nowak, *Corpus Iuris – wersja florencka a polskie prawo karne materialne*, s. 58 i n.; J. Skupiński, *Współpraca Polski z europejskim Biurem do Walki z Oszustwami (OLAF)*, s. 66 i n.; B. Świątkiewicz, *Wyłudzenia środków finansowych w praktyce policyjnej*, s. 70 i n. i podaną w tych referatach literaturę. Zob. też B. Srebro, *Ochrona interesów finansowych Unii Europejskiej*, Kraków 2004 oraz M. Hudzik, C. Nowak (red.), *Materiały międzyna-*

COMPUTER FRAUD: PROVISIONS OF THE POLISH LAW

The Polish Penal Code provides for a separate offence of Computer fraud, which constitutes a modern solution. This offence has a basic and a more favourable form (Art. 287 Par. 1 and 2 of the PC), as well as aggravated one (Art. 294 of the PC). It is an offence directed against property.

rodowej konferencji naukowej *Instytucje i instrumenty prawne w walce z przestępczością przeciwko interesom finansowym Unii Europejskiej – prawo krajowe i perspektywa europejska*, Warszawa, 4–6 grudnia 2003, Warszawa 2004, a także Materiały międzynarodowej Konferencji naukowej *Ochrona interesów finansowych rozszerzonej Unii Europejskiej: nowe wyzwania, stare problemy* Sopot, 16–19 marca 2006 r. (jeszcze niepublikowane). Zob. też podaną w tych pozycjach literaturę.