Maria Szczepaniec

Komputer jako narzędzie przestępstwa

Zeszyty Prawnicze 12/2, 167-180

2012

Zeszyty Prawnicze
12.2/2012

Maria Szczepaniec

Uniwersytet Kardynała Stefana Wyszyńskiego

KOMPUTER JAKO NARZĘDZIE PRZESTĘPSTWA

1. Uwagi wprowadzające

Celem niniejszego opracowania jest analiza wybranych aspektów dotyczących przestępczości komputerowej. Pierwsza poruszana kwestia związana jest z definiowaniem przestępczości komputerowej. Kolejne zagadnienie dotyczy rodzaju przestępstw możliwych do popełnienia z wykorzystaniem komputera. W związku z tym, że na przestępstwa komputerowe składają się rozmaite rodzaje zachowań, należy dokonać pewnej kategoryzacji w tym zakresie ze wskazaniem klasyfikacji przestępstw komputerowych na gruncie polskiego prawa karnego. Analizie poddane zostaną także wybrane przestępstwa, w których komputer stanowi narzędzie do ich popełnienia.

Następny problem badawczy, niezwykle istotny z punktu widzenia poruszanego zagadnienia, dotyczy ochrony cyberprzestrzeni. Przestępstwa, do popełnienia których wykorzystywany jest komputer, zwłaszcza należące do kategorii przestępstw internetowych, sprawiają spore trudnościami na etapie wykrywczym oraz dowodowym, co czyni aktualnym kwestię nieustannej aktualizacji stosowanych metod w walce z tym zjawiskiem.

Komputer może odgrywać w aktywności przestępnej co do zasady trojaką rolę:

a) może być celem popełnienia przestępstwa (np. *hacking* czy wprowadzenie wirusa komputerowego),

b) może być narzędziem umożliwiającym popełnienie czynu zabronionego, np. kradzież, rozpowszechnianie pornografii itp.

c) może mieć jedynie incydentalne znaczenie w trakcie dokonywania przestępstwa, np. służyć jako baza danych.[1] Przestępczość komputerowa będzie więc obejmować rozmaite rodzaje zachowań.

W odniesieniu do pojęcia przestępczości komputerowej w doktrynie można natknąć się na różne definicje tego zjawiska. W szerokim znaczeniu przyjmuje się, iż jest to przestępczość obejmująca wszelkie zachowania przestępcze pozostające w związku z funkcjonowaniem elektronicznego przetwarzania danych. Są to więc czyny, które polegają na naruszaniu uprawnień do programu komputerowego, ale także przejawiające się bezpośrednim godzeniem w przetwarzaną informację, jej nośnik oraz obieg w komputerze, jak też w cały system połączeń komputerowych oraz w sam komputer. Będą to czyny popełnione z użyciem elektronicznych systemów przetwarzania danych, a więc komputer stanowić będzie narzędzie do popełnienia przestępstwa, jak również czyny skierowane przeciwko systemowi przetwarzania danych.[2]

Do przestępczości komputerowej zaliczane są również wszelkie prawnokarne konstrukcje kryminalizujące bezprawne zachowania, które polegają na godzeniu w gromadzone, przetwarzane i przesyłane za pomocą nowoczesnych technologii cyfrowych informacje.[3]

Jednak określenie „przestępczość komputerowa" nie odnosi się tylko do wszelkich zamachów mających postać różnego rodzaju komputerowych manipulacji, sabotażu, *hackingu* itp. Coraz częściej jest to nadrzędna nazwa przestępstw, które polegają na zamachach na rozma-

---

[1] M. KLIŚ, *Przestępczość w Internecie. Zagadnienia podstawowe*, «CzPKiNP» 1/2000, s. 6.

[2] K.J. JAKUBSKI, *Przestępczość komputerowa – zarys problematyki*, «Prokuratura i Prawo» 12/1996, s. 34.

[3] P. KARDAS, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, «CzPKiNP» 1/2000, s. 32.

ite tradycyjne dobra prawne, a dokonywane są za pomocą nowoczesnej techniki komputerowej.[4]

Jak przyjmuje B. Fischer przestępstwa komputerowe to „czyny skierowane zarówno przeciwko systemowi komputerowemu (komputer-cel), jak i popełnione przy jego użyciu (komputer-narzędzie)".[5]

Systematyzując rozważania należy zauważyć, iż na przestępstwa komputerowe składają się rozmaite rodzaje zachowań, które można pogrupować na trzy podstawowe kategorie. Pierwsza kategoria dotyczy przestępstw przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji. Są to czyny zabronione *stricte* komputerowe, w których przedmiot ochrony stanowi informacja.[6]

Druga kategoria czynów obejmuje zachowania, w których przedmiotem zamachu są dobra prawne tradycyjnie chronione przepisami prawa karnego, a do ich naruszenia dochodzi w drodze wykorzystania nowoczesnych technologii gromadzenia i przetwarzania informacji. To właśnie te typy przestępstw, w których komputer stanowi narzędzie przestępstwa, czy nieco szerzej ujmując, narzędzie popełnienia przestępstwa stanowią elektroniczne technologie gromadzenia i przetwarzania danych, precyzyjnie określone w ustawowym opisie danego przestępstwa rodzajowego.[7]

Wyróżnia się również i trzecią kategorię przestępstw, obejmującą zamachy na tradycyjne dobra prawne dokonywane za pomocą nowoczesnych urządzeń, służących do cyfrowego gromadzenia i przetwarzania danych, przy czym sposób popełnienia przestępstwa (z wykorzystaniem tychże technologii) nie jest wskazany w ustawowym opisie danej odmiany przestępstwa rodzajowego. W tej grupie wymienia się m.in. zniesławienie, zniewagę, groźbę karalną, czy rozpowszechnianie treści pornograficznych przez Internet.[8]

---

[4] P. KARDAS, *Prawnokarna ochrona*…, s. 50.

[5] B. FISCHER, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 24.

[6] A. ADAMSKI, *Prawo karne komputerowe*, Warszawa 2000, s. 30, P. KARDAS, *Prawnokarna ochrona*…, s. 51.

[7] P. KARDAS, *Prawnokarna ochrona*…, s. 51-52, zob. także A. ADAMSKI, *op. cit*., s. 31.

[8] P. KARDAS, *Prawnokarna ochrona*…, s. 52.

2. KLASYFIKACJA PRZESTĘPSTW KOMPUTEROWYCH NA GRUNCIE POLSKIEGO PRAWA KARNEGO

Pierwszą kategorię przestępstw komputerowych stanowią czyny skierowane przeciwko ochronie informacji, zawarte w XXXIII rozdziale kodeksu karnego z 1997 r. Są to:
– *hacking* komputerowy (art. 267 § 1 k.k.)
– nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych (art. 267 § 2 k.k.)
– naruszenie integralności zapisu informacji (art. 268 § 2 k.k.)
– niszczenie danych informatycznych (art. 268a § 1 k.k.)
– sabotaż komputerowy (269 § 1 i § 2 k.k., 269a i 269b).

Kolejna grupa to przestępstwa przeciwko mieniu. Tutaj można wskazać:
– nielegalne uzyskanie programu komputerowego (art. 278 § 2 k.k.)
– paserstwo programu komputerowego (293 §1 k.k.)
– oszustwo komputerowe (art. 287 k.k.)
– oszustwo telekomunikacyjne (art. 285 k.k.).

Przestępstwa przeciwko wiarygodności dokumentów oraz obrotowi gospodarczemu i pieniężnemu:
– fałszerstwo komputerowe (art. 270 § 1 k.k.)
– zniszczenie lub pozbawienie mocy dowodowej dokumentu elektronicznego (art. 276 k.k.)
– wyłudzenie z art. 297 § 1
– nierzetelne prowadzenie dokumentacji działalności gospodarczej (303 k.k.)
– fałszerstwo kart płatniczych (art. 310 k.k.).

Inne typy przestępstw komputerowych:
– sprowadzenie powszechnego niebezpieczeństwa na skutek zakłócenia procesów automatycznego przetwarzania danych informatycznych (165 § 1 pkt 4 k.k.)
– szpiegostwo komputerowe (art. 130 § 2 k.k.)
– rozpowszechnianie, przechowywanie, oraz posiadanie treści pornograficznych przedstawiających małoletniego (art. 202 § 4b)

– grooming (art. 200a k.k.).[9]

Przepisy karne dotyczące przestępczości komputerowej zawarte są także w innych ustawach. Wskazać należy tutaj następujące akty:

* ustawę z 1994 r. o prawie autorskim i prawach pokrewnych,
* ustawę z 1997 r. o ochronie danych osobowych,
* ustawę z 2001 r. o podpisie elektronicznym,
* ustawę z 2002 r. o świadczeniu usług drogą elektroniczną,
* ustawę z 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym.

Przestępstwa, w których komputer stanowi narzędzie do ich popełnienia, mogą mieć różnorodny charakter. I tak, wskazać należy m.in.:

– oszustwo komputerowe,
– kradzież,
– *grooming*,
– rozpowszechnianie pornografii,
– rozpowszechnianie, przechowywanie oraz posiadanie treści pornograficznych przedstawiających małoletniego (art. 202 § 4b k.k.),
– propagowanie faszyzmu i totalitaryzmu (art. 256 k.k.),
– handel narkotykami,
– sianie nienawiści rasowej,
– obrażanie uczuć religijnych,
– pomówienie.

To tylko przykładowe wskazanie przestępstw możliwych do popełnienia z wykorzystaniem komputera. Wyróżnić należy tutaj w szczególności przestępstwa, w których do działań sprzecznych z prawem wykorzystywany jest Internet, czyli tzw. przestępstwa internetowe. Przyjmuje się, iż przestępstwa internetowe to takie przestępstwa, w których usługi sieciowe (oferowane przez Internet) umożliwiły lub co najmniej ułatwiły sprawcy realizację zamierzonego czynu przestępnego bądź jego poszczególnych stadiów.[10] Przestępczość internetowa

---

[9] M. SZCZEPANIEC, *Typy przestępstw komputerowych*, [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, red. G. SZPOR, Warszawa 2011 s. 412-413.

[10] M. SOWA, *Odpowiedzialność karna sprawców przestępstw internetowych*, «Prokuratura i Prawo» 4/2002, s. 62.

to zatem ten rodzaj kryminalnej aktywności jednostek, który wiąże się z wykorzystaniem sieci internetowej.

3. KILKA UWAG NA TEMAT WYBRANYCH PRZESTĘPSTW POPEŁNIONYCH PRZY UŻYCIU KOMPUTERA

3.1 *Grooming*

Grooming w sensie potocznym określany jest jako uwodzenie dzieci przez Internet.[11]

To przestępstwo wprowadzone zostało do kodeksu karnego nowelizacją z 5.11.2009 r.[12] Dodano wówczas art. 200a, w następującym brzmieniu:

„§ 1. Kto w celu popełnienia przestępstwa określonego w art. 197 § 3 pkt 2 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim,

podlega karze pozbawienia wolności do lat 3.

§ 2. Kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych, i zmierza do jej realizacji,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

Przedmiotem ochrony objęto więc małoletniego, a dokładnie jego rozwój psychoseksualny. Włączanie dziecka w aktywność seksualną

[11] Przyjmuje się, że *grooming* obejmuje „działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później je seksualnie wykorzystać. Jest to także mechanizm używany, by nakłonić dziecko do prostytucji czy udziału w pornografii dziecięcej" (za Wikipedia).

[12] Ustawa weszła w życie 8 czerwca 2010 r.

stanowi zachowanie nieadekwatne w stosunku do poziomu jego rozwoju psychoseksualnego, czego skutkiem jest zaburzenie normalnego funkcjonowania u ofiar, które celem odzyskania równowagi zawsze potrzebują terapii.[13] Wykorzystywanie możliwości nawiązywania kontaktów seksualnych z dziećmi, jaką stwarza pedofilom Internet to bardzo niebezpieczna forma zachowania. Znalezienie ofiary jest bardzo łatwe i nie wymaga dużych nakładów czasowych. Wykorzystywana jest dziecięca ufność i naiwność, co jest szczególnie odrażające.

Unormowanie wprowadzone wspomnianą nowelizacją należy niewątpliwie ocenić jako pozytywny krok w walce z tym zjawiskiem. To przepis, który wzmacnia ochronę dzieci w Internecie. Pozytywnie należy ocenić również art. 200b k.k. (dodany tą samą nowelizacją), który przewiduje odpowiedzialność karną za publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim.

3.2 Oszustwo komputerowe

To nowy typ przestępstwa, który został wprowadzony do kodeksu karnego z 1997 r., wypełniając lukę kryminalizacyjną powstałą na skutek gwałtownego rozwoju technologii cyfrowych. Celem nowej regulacji było przede wszystkim wzmocnienie karnoprawnej ochrony mienia przed atakami dokonywanymi za pomocą nowoczesnych technologii teleinformatycznych.[14] Jak wskazano w uzasadnieniu: „Wprowadzenie oszustwa komputerowego jest niezbędne, gdyż tradycyjne pojęcie oszustwa zawiera znamiona (wprowadza w błąd »inną osobę«, wyzyskuje jej błąd lub »niezdolność do należytego pojmowania przedsiębranego działania«, doprowadza ją do niekorzystnego rozporządzenia mieniem), które przy komputerowym oszustwie nie są spełniane, choć nienależna korzyść majątkowa jest osiągana (art. 287)".[15] Klasyczna

[13] A. JODKO, *Tabu seksuologii. Wątpliwości, trudne tematy, dylematy w seksuologii i edukacji seksualnej*, Warszawa 2008, s. 135-144.

[14] R. KORCZYŃSKI, R. KOSZUT, *„Oszustwo" komputerowe*, «Prokuratura i Prawo» 2/2002, s. 17.

[15] Nowe kodeksy karne – z 1997 r., Uzasadnienie rządowego projektu kodeksu karnego, Warszawa 1997, s. 205-206.

formuła oszustwa nie przystawała do nowoczesnych form ataku na mienie, dokonywanych z wykorzystaniem urządzeń cyfrowych, ponadto nowa regulacja to także realizacja zobowiązań związanych z koniecznością dostosowania polskiego porządku prawnego do standardów, jakie obowiązują w państwach Unii Europejskiej.[16] Również A. Adamski wskazuje, iż ta klasyczna formuła oszustwa stanowi nieadekwatną konstrukcję „w czasach, w których na skutek automatyzacji wielu procesów wymiany dóbr i usług, miejsce interakcji interpersonalnych w coraz większym stopniu zajmuje interakcja człowieka z maszyną, którą ten pierwszy też może starać się wprowadzić w błąd, jeśli jest to dla niego opłacalne".[17]

Ustawowe znamiona przestępstwa oszustwa komputerowego różnią się w zasadniczy sposób od znamion przestępstwa klasycznego oszustwa. Przede wszystkim pomijają element odnoszący się do podmiotu oddziaływania sprawcy. Sprawca oszustwa komputerowego nie oddziałuje na inną osobę, lecz oddziałuje bezpośrednio na urządzenia bądź procesy techniczne, związane z automatycznym gromadzeniem, przetwarzaniem oraz przesyłaniem danych. W opisie typu czynu zabronionego nie ma czynności polegającej na wprowadzeniu innej osoby w błąd, czy też wykorzystania jej błędu. Inaczej określona została również czynność wykonawcza i jej związek z narażeniem na niebezpieczeństwo bądź naruszeniem mienia innego podmiotu. I tak, w przypadku oszustwa komputerowego niebezpieczeństwo dla mienia i ewentualne jego naruszenie jest wynikiem podejmowanych przez sprawcę czynności w stosunku do urządzeń służących do automatycznego gromadzenia, przekształcania i przesyłania danych. Przy czym dla dokonania przestępstwa oszustwa komputerowego nie jest konieczne faktyczne powstanie szkody, wystarczające jest już podjęcie czynności zmierzających do uzyskania takiego rezultatu.[18]

---

[16] P. KARDAS, *Oszustwo komputerowe w kodeksie karnym*, «Przegląd Sądowy» 11-12/2000, s. 44.

[17] A. ADAMSKI, *op. cit*., s. 115.

[18] P. KARDAS, *Oszustwo komputerowe*…, s. 52-53.

Na płaszczyźnie znamion strony przedmiotowej najwyraźniej widać różnice pomiędzy klasycznym oszustwem a oszustwem komputerowym. Zgodnie z art. 287 kodeksu karnego karalne są następujące czynności: wpływanie na automatyczne przetwarzanie danych informatycznych, wpływanie na automatyczne gromadzenie danych informatycznych, wpływanie na automatyczne przekazywanie danych informatycznych, zmiana zapisów na komputerowym nośniku danych, usunięcie takich zapisów lub wprowadzenie nowego zapisu danych informatycznych. Przepis zawiera więc sześć różnych sposobów karalnego zachowania.

Pierwsza część znamion opisujących czynności wykonawcze posługuje się określeniem „wpływa". Wpływanie w tym znaczeniu należy pojmować jako ingerencję w proces automatycznego przetwarzania, gromadzenia bądź przekazywania danych informatycznych, która prowadzi do przekształcenia, zniekształcenia lub jakiejkolwiek innej transformacji tego procesu, a po zakończeniu oddziaływania sprawcy ów proces będzie inny niż byłby w przypadku braku owej ingerencji. To wpływanie może mieć postać zakłócania lub uniemożliwiania procesu automatycznego przetwarzania, gromadzenia bądź przekazywania danych informatycznych lub też może przybrać inną, podobną formę oddziaływania sprawcy na tenże proces.[19]

W drugiej części znamion przedmiotowych opisane zostały czynności polegające na zmianie, usunięciu bądź dodaniu nowego zapisu danych informatycznych.

Sposób określenia znamion czynnościowych pozwala przyjąć, że oszustwo komputerowe należy do przestępstw skutkowych. Skutek na-

[19] Wpływanie obejmuje dość szeroki zakres zachowań, które polegają w istocie na niedozwolonym oddziaływaniu przez sprawcę na proces gromadzenia, przetwarzania bądź przekazywania informacji. Może to być mechaniczna ingerencja w urządzenie, które służy do wykonywania tych operacji, np. uszkodzenie serwera, czy linii telefonicznej. Może polegać na podłączeniu się do systemu komunikacyjnego, służącego do transmisji danych informatycznych i modyfikowaniu treści kodowego zapisu tych danych. Wreszcie zachowanie polegające na wpływaniu na procesy gromadzenia, przetwarzania bądź przekazywania informacji może być połączone z wcześniejszym przełamaniem przez sprawcę tych zabezpieczeń. P. KARDAS, *Oszustwo komputerowe*…, s. 62-64.

stępuje już wtedy gdy sprawca wpłynie ma automatyczne przetwarzanie, gromadzenie lub przekazywanie danych bądź w chwili dokonania zmiany, usunięcia albo wprowadzenia nowego zapisu na komputerowym nośniku danych. Przy czym dla bytu przestępstwa nie jest konieczne spowodowanie szkody majątkowej po stronie innej osoby.[20]

4. OCHRONA CYBERPRZESTRZENI – WYBRANE KWESTIE

Wskazuje się, że podstawowym błędem na płaszczyźnie oceny zagrożeń dla procesów w cyberprzestrzeni jest twierdzenie, że na ataki narażone są tylko pewne grupy ludzi. Współcześnie każdy może być celem ataku, a analiza ogólnych trendów pokazuje, że nie ma obszarów, o których można powiedzieć, że są w 100% bezpieczne. Nie istnieje medium zapewniające bezpieczne korzystanie z oferowanych przez cyberprzestrzeń usług. Złośliwe oprogramowanie może być umieszczone w poczcie elektronicznej bądź na stronie internetowej. Infekcję może wywołać także już samo podłączenie do Internetu.[21]

Wrogie działania można skategoryzować według kryterium medium, metody i celu ataku. Jeżeli chodzi o medium, do najczęstszych metod należy infekcja przez e-mail bądź stronę internetową. Wśród metod ataku wyróżniane są przede wszystkie próby ataku bezpośredniego, atak pośredni, jak również atak socjotechniczny. Atak dokonywany jest zwykle w celu zdobycia dostępu do atakowanej maszyny, przejęcie zasobów, a także kradzież danych lub tożsamości. Inne rodzaje ataków, nie wchodzące w ramy powyższej klasyfikacji, to np. rozsyłanie spamu, co wpływa na jakość usług poczty elektronicznej. Kolejny rodzaj ataku stanowią ataki odmowy dostępu, które polegają na obciążeniu zasobów atakowanego systemu w sposób, który uniemożliwia uprawnionym użytkownikom korzystanie z usług świadczonych przez dany system. Ta metoda wrogiego oddziaływania jest

[20] I m.in. ten brak konieczności wywołania szkody w mieniu innej osoby odróżnia oszustwo komputerowe od oszustwa klasycznego. Tamże, s. 72-73.

[21] P. DURBAJŁO, *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej 2010-2015*, [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, red. G. SZPOR, Warszawa 2011, s. 358-359.

najprostszą technologicznie i kosztowo metodą, a równocześnie bardzo trudno się przed nią obronić.[22]

Wskazać można także ataki ukierunkowane, które zazwyczaj dokonywane są celem kradzieży danych lub przejęcia kontroli nad określonym systemem teleinformatycznym. Cechą odróżniającą wcześniej wskazane ataki od ataku ukierunkowanego jest to, że w przypadku tego ostatniego nieuprawniony dostęp do systemów odbywa się najczęściej metodami socjotechnicznymi, a nie siłowymi. Często stosowane jest wówczas złośliwe oprogramowanie, którego nie wykrywają typowe antywirusy. Wszystko to rodzi konieczność podejmowania stosownych inicjatyw, aby zmniejszyć skuteczność wrogich działań. W Polsce należy wskazać na „Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej", którego współautorem jest Agencja Bezpieczeństwa Wewnętrznego. Prowadzone są działania, których celem jest stałe podwyższanie bezpieczeństwa w obszarze teleinformatyki oraz wzmacnianie odporności na ataki w cyberprzestrzeni RP.[23]

5. PODSUMOWANIE

Permanentny postęp w dziedzinie nowoczesnych technologii informatycznych przekłada się na coraz to doskonalsze sposoby i metody działań przestępnych. Sprawcy przestępstw, to grupa, która bardzo szybko dostosowuje strategie przestępne do zmieniającej się rzeczywistości społecznej, a wykrywalność przestępstw komputerowych jest niestety niska.

Wśród powodów mających wpływ na niską efektywność w zakresie wykrywalności tej kategorii przestępstw wskazuje się m.in. okoliczność, iż tego typu przestępstwa ujawniane są zazwyczaj przypadkiem, zwykle na skutek błędów popełnionych przez sprawców. Także względy ekonomiczne przesądzają o tym, iż organy ścigania nie odgrywają istotnej roli w ujawnianiu tej kategorii przestępstw. Przestępczość komputerową cechuje nadto bardzo wysoka ciemna liczba prze-

[22] P. DURBAJŁO, *op. cit*., s. 359.

[23] Tamże, s. 361.

stępstw. Wskazuje się, że sprawcy działają dość długo zwykle powodując poważne straty i często pokrzywdzeni nie są zainteresowani ich ujawnieniem.[24]

Szczególnie niebezpieczne jest wykorzystywanie Internetu do popełniania przestępstw z uwagi na ogromną liczbę potencjalnych ofiar. Dodatkowym niebezpieczeństwem i ogromnym utrudnieniem zarazem jest okoliczność, iż cyberprzestępczość nie pozostawia tradycyjnych śladów w postaci np. odcisków palców, wizerunku, DNA itp. Oczywiście ten rodzaj przestępczości także zostawia ślady, ale ich wirtualny charakter znacznie utrudnia identyfikację zarówno miejsca działania sprawcy jak i samego sprawcy. Na płaszczyźnie efektywności ścigania cyberprzestępstw nie bez znaczenia jest także niska świadomość społeczna jeśli idzie o zagrożenia związane z tego rodzaju przestępczością. Coraz to nowe możliwości technologiczne przekładają się na coraz doskonalsze i bardzo wyrafinowane metody działania cyberprzestępców. Oczywiście nie da się przewidzieć wszystkich potencjalnych zagrożeń, jakie mogą być skutkiem korzystania z systemów komputerowych, ale nieodzowne jest podejmowanie elementarnych środków bezpieczeństwa (a więc hasła dostępu, kryptografia, zapory ogniowe), które będą tak skonfigurowane, by zapobiegać najbardziej pospolitym nadużyciom, a przynajmniej zmniejszać prawdopodobieństwo ich zaistnienia.[25]

Szybka i skuteczna walka z cyberprzestepczością wymaga sprawnej współpracy międzynarodowej, a wspólna polityka karna przede wszystkim powinna chronić społeczeństwo przed zagrożeniami związanymi z cyberprzestępczością. Zapewnienie skutecznej ochrony w tym zakresie to bez wątpienia kwestia wprowadzenia stosownych regulacji prawnych, dotyczących nie tylko penalizacji określonej kategorii zachowań, ale również dostosowanie unormowań procesowych w celu sprawnego ścigania i prowadzenia postępowań karnych dotyczących przestępstw komputerowych.[26]

---

[24] B. ŚWIĄTKIEWICZ, *Przestępstwa internetowe*…, s. 110.

[25] A. ADAMSKI, *op.cit*., s. 27.

[26] M. SZCZEPANIEC, *op.cit*., s. 417.

Komputer jako narzędzie umożliwiające popełnienie przestępstwa stwarza bardzo szerokie spectrum możliwości działania potencjalnych przestępców, którzy coraz częściej i chętniej urzeczywistniają swoje przestępne zamiary w wirtualnej rzeczywistości. Oszacowanie skali zjawiska jest niezwykle trudne. Szczególnie niebezpieczne jest wykorzystywanie dzieci przez Internet, zwłaszcza iż mimo powszechnego uznania łatwości dostępu do np. pornografii dziecięcej i istnienia pedofilskiej działalności w systemach P2P[27] nadal nie istnieją dostępne techniki filtrowania zawartości oraz systemy ocen ochrony użytkowników P2P (w szczególności dzieci) od szkodliwych zachowań i treści. Niewielka jest także liczba narzędzi zdatnych pomóc organom ścigania i innym organizacjom chronić dzieci przed pedofilią, wynikającą z wymiany plików w P2P. Pojawiają się wprawdzie różne profilaktyczne akcje społeczne, nagłaśniane są akcje operacyjne policji w odniesieniu do dziecięcej pornografii, jednak w przypadku np. sieci P2P są one niezwykle utrudnione.[28]

Należy więc popierać wszelkie inicjatywy, zarówno o charakterze technologicznym, jak i prawnym, aby walkę z przestępczością komputerową uczynić skuteczniejszą. Wprawdzie tak jak w przypadku przestępstw popełnianych w tradycyjny sposób nie da się wyeliminować tego zjawiska, konieczne jest jednak kontrolowanie sytuacji, aby nie dopuścić do nadmiernej eskalacji problemów. Postęp, jaki nastąpił w dziedzinie informatycznej, pociąga za sobą nie tylko znaczne ułatwienie w wielu aspektach ludzkiej aktywności, ale wiąże się także, a może przede wszystkim z niesłychanym zagrożeniem ze strony przestępców, dla których komputer stanowi również narzędzie ułatwiające ich przestępną działalność.

---

[27] Technologia P2P łączy ze sobą bezpośrednio indywidualnych użytkowników, bez centralnego punktu zarządzania. Uzyskanie dostępu do sieci P2P wymaga pobrania i zainstalowania aplikacji klienta P2P. Miliony osób mają aktualnie zainstalowane w swoich komputerach programy P2P, co stwarza możliwości wyszukiwania plików na innych komputerach każdego innego użytkownika P2P i ewentualne pobranie różnych plików. Szerzej zob. J. CYTOWSKI, *Sieci Peer-toPeer- problemy bezpieczeństwa*, [w:] *Internet. Ochrona wolności…*, s. 391 i n.

[28] Tamże, s. 397.

Przestępstwa z użyciem komputera, zwłaszcza należące do kategorii przestępstw internetowych wiążą się z trudnościami na etapie zarówno wykrywczym jak i dowodowym. Regulacje prawne winny być dostosowane do wirtualnej rzeczywistości i wynikających zeń problemów. Przed ustawodawcą więc trudne zadanie, pewien proces związany z udoskonalaniem prawa cybernetycznego, którego nie da się zakończyć, gdyż stale dokonujący się rozwój technologii cybernetycznych sprawia, że i procedury walki z cyberprzestępczością muszą mieć dynamiczny charakter.

THE COMPUTER AS THE TOOL OF THE CRIME

Summary

The article presented the classification of computer crimes on the basis of Polish criminal law and some issues concerning computer crime. Was also presented a brief analysis of selected computer crime, such as: grooming and computer cheating. The article describes also questions concerning security of cyberspace.