Jerzy Wojciech Wójcik

Przestępstwa komputerowe w nowym kodeksie karnym

Truizmem jest obecnie stwierdzenie, że cywilizacja informatyczna spowodowała konieczność posługiwania się systemami komputerowymi w życiu codziennym. Jednakże w krajach wysoko rozwiniętych, wraz z rozwojem komputeryzacji, zaczęto dostrzegać narastające zagrożenia.

Wykorzystanie systemów komputerowych i towarzyszące im zagrożenia, w sposób syntetyczny, można scharakteryzować następująco:

- Komputeryzacja już z początkiem lat 50. była wykorzystywana do sterowania rutynowymi czynnościami w gospodarce i administracji. Jednakże dopiero w latach 60. ujawniono pierwsze, a w latach 70. poważniejsze przypadki oszustw, sabotażu, a także szpiegostwa gospodarczego z wykorzystywaniem komputerów.
- Masowe przetwarzanie informacji z zakresu danych osobowych rozpoczęło się w latach 60. poprzez tworzenie banków danych. Wkrótce jednak brak ograniczeń związanych z dostępem do wspomnianych danych odebrano jako zagrożenie praw obywatelskich.
- Otwarte systemy sieciowe, które pojawiły się w latach 70., stały się szybko obiektem nadużyć określonych jako *hacking*.
- Upowszechnienie komputerów osobistych w latach 80. spowodowało masowe zjawisko sporządzania pirackich kopii programów.
- Rozwinięcie sieci bankomatów w latach 80. natychmiast skutkowało nadużyciami za pomocą kart magnetycznych.
- Powszechność poczty elektronicznej, maliboxów, ISDN, a także ścisłe powiązania pomiędzy systemami przetwarzania danych a telekomunikacją umożliwiło powszechne komunikowanie i wykorzystywanie również do celów przestępczych zorganizowanych grup przestępczych, zarówno kryminalnych, jak i gospodarczych, a nawet poprzez skomplikowane *modus operandi* służy do perfekcyjnego zacierania śladów przestępstwa.

Wśród wielu różnorodnych sposobów ochrony systemów informatycznych, obok zabezpieczeń technicznych i organizacyjnych, istotną rolę odgrywają przepisy karnoprawne.

Przestępstwa komputerowe w nowym kodeksie karnym

W ustawie z dnia 6 czerwca 1997 roku – kodeks karny (Dz.U. Nr 88, poz. 553)[1] zagadnienie ścigania przestępstw komputerowych zawarto w kilku rozdziałach, a mianowicie:

- rozdział XXXIII – Przestępstwa przeciwko ochronie informacji (art. 267 § 1 i 2, 268 § 2 i 296 § 1 i 2 kk),
- rozdział XXXV – Przestępstwa przeciwko mieniu (art. 278 § 2, 285 § 1, 287 § 1 i 293 § 1 kk),
- rozdział XX – Przestępstwa przeciwko bezpieczeństwu powszechnemu (art. 165 § 1 ust. 4, 165 § 2 i 167 § 2 kk),
- rozdział XVII – Przestępstwa przeciwko Rzeczypospolitej Polskiej (art. 130 § 2 i 3 oraz 138 § 2 kk),
- rozdział XXXIV – Przestępstwa przeciwko wiarygodności dokumentów (art. 270 § 1 kk).

Z powyższego wynika, że mimo istotnych głosów przedstawicieli doktryny, kodeks karny nie wyróżnia całej gamy przestępstw w jednym rozdziale „Przestępstwa komputerowe".

W rozdziale „Przestępstwa przeciwko ochronie informacji" wymienia się:

Hacking komputerowy – art. 267 § § 1 kk

Nieuprawnione wejście do systemu komputerowego przez naruszenie zastosowanych zabezpieczeń i manipulowanie w bazie danych określane jest także jako włamanie do komputera i kradzież danych. Zgodnie z cytowanym przepisem, zakazane jest uzyskiwanie informacji przez osobę nieupoważnioną lub informacji nie przeznaczonych dla tej osoby. Zatem niszczenie, uszkadzanie, usuwanie lub zmiana zapisu istotnej informacji lub udaremnienie w inny sposób albo znaczne utrudnienie osobie uprawnionej do zapoznania się z zapisem informacji jest zabronione. Ważny jest jednak sposób działania, w którym podkreśla się *„przełamując elektroniczne, magnetyczne lub inne szczególne zabezpieczenie"*. Obojętny jest zatem rodzaj pokonanego zabezpieczenia. Istotą omawianego przestępstwa jest uzyskanie informacji przez *hackera*. Nie jest karalne jedynie sprawdzenie jakości zabezpieczeń i możliwości ich przełamania.

Podkreślić należy, że karalne jest także przekazywanie uzyskanych w ten sposób informacji innym osobom. *Hackerowi* grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Wśród nielicznych krajów, które wprowadziły karalność *hackingu* warto wymienić: USA i Wielką Brytanię oraz Danię, Francję, Szwecję i Holandię.

Podsłuch komputerowy (nieuprawnione przechwycenie informacji) – art. 267 § 2 kk

Przechwytywanie wszelkich informacji, w tym także stwarzanie poważnych zagrożeń dla systemów informatycznych, umożliwiają zdobycze współczesnej techniki. Możliwy jest nawet zdalny podsłuch i podgląd, czyli prowadzenie pełnej kontroli bez wiedzy i zgody właściciela systemu.

Omawiany przepis przewiduje karę dla tych sprawców, którzy weszli w posiadanie informacji poprzez zakładanie urządzeń podsłuchowych, wizualnych lub innych urządzeń specjalnych. Obojętny jest zatem rodzaj urządzenia, gdyż chodzi o wszystkie urządzenia, także telekomunikacyjne służące przekazywaniu informacji. Również nie jest istotny cel wejścia do sieci czy systemu komputerowego.

Powyższy przepis obejmuje także uzyskanie danych stanowiących tajemnicę państwową czy służbową. Norma tego artykułu ma charakter ogólny, bowiem powszechnie wiadomo, że prawo nie odgrywa tu specjalnej roli zapobiegawczej. Przeciwdziałanie podsłuchowi i podglądowi komputerowemu przypada przede wszystkim specjalistom w zakresie ochrony systemów teleinformatycznych. Sankcje karne dla tego typu sprawców są takie same, jak za *hacking*.

Zasadniczym celem ochrony jest poufność przekazywanych lub przesyłanych informacji przy użyciu środków technicznych, a także ochrona prywatności każdego człowieka przed różnymi formami inwigilacji jak np. podglądanie czy podsłuchiwanie. Na tym tle mogą powstać wątpliwości co do działania pracodawcy sprawdzającego lojalność swoich pracowników. Niektóre firmy ochrony mienia i osób oferują już takie usługi.

Ochrona korespondencji realizowana jest także przez prawo cywilne szczególnie zaś, gdy zaistniały określone skutki. Art. 25 kc[2)] pozwala, na żądanie, usunąć skutki, a jeśli zaistniała szkoda majątkowa, poszkodowany może żądać naprawienia jej w ramach przepisów ogólnych. W zakresie odpowiedzialności za czyny niedozwolone art. 415 kc stanowi *„Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia"*.

Omawiany problem w świetle prawa cywilnego dotyczy także ochrony nadawcy korespondencji. Może tu zachodzić np. przesłanie korespondencji bez zabezpieczenia jej treści kopertą[3)] czy odpowiednimi kodami kryptograficznymi w przypadku poczty elektronicznej. Zatem ochrona cywilnoprawna ma większy zakres niż ochrona karnoprawna.

W przypadku zaistnienia określonych skutków ujawnienia i przekazania nieuprawnionego przechwycenia informacji sprawcy grozi odpowiedzialność z innych przepisów. Przykładowo, za ujawnienie lub przekazanie danych stanowiących tajemnicę państwową z art. 265 kk, tajemnicę służbową z art. 266 kk.

Bezprawne niszczenie informacji – art. 268 § 2 kk

Chodzi o naruszenie integralności komputerowego zapisu informacji, które może nastąpić w wyniku bezprawnego niszczenia, uszkodzenia, usuwania lub zmiany zapisu istotnej informacji albo udaremnienie czy utrudnienie osobie uprawnionej zapoznania się z nią. Takie działanie zagrożone jest karą pozbawienia wolności do lat 3.

Kara przewidziana jest bez względu na sposób niszczenia zapisu informacji i rodzaju np. w bazie danych, w trakcie przetwarzania informacji, poprzez wprowadzenie (do programu czy sieci) wirusa, hasła lub zmianę albo jakiekolwiek inne utrudnienie dostępu do informacji osobie upoważnionej. Dotyczy także spowodowania zakłóceń w telekomunikacji, o ile podłączono do tej sieci urządzenia pozwalające na przetwarzanie lub rejestrowanie danych.

Karalne jest także modyfikowanie danych lub programów komputerowych. Różni się ono od niszczenia tym, że sprawca dokonuje nieuprawnionej ingerencji w treść danych, np. poprzez dopisanie nowych danych lub zmianę istniejącego zapisu. Zabronione jest zatem wprowadzanie zmian do zapisu istotnej informacji przechowywanej w systemie komputerowym. Czyn taki polega na naruszeniu integralności danych oraz naruszeniu dóbr właściciela czy osoby uprawnionej. Związane jest to z prawem do niezakłóconego posiadania zapisu informacji czy prawa do prywatności.

Jeżeli sprawca zniszczył informacje i wyrządził znaczną szkodę majątkową, zgodnie z art. 268 § 3 kk, podlega karze pobawienia wolności od 3 miesięcy do 5 lat. Mamy tu do czynienia z kwalifikowaną formą przestępstwa niszczenia informacji.

Przestępstwa z art. 267 i 268 kk są ścigane na wniosek pokrzywdzonego.

Sabotaż komputerowy – art. 269 § 1 i 2 kk

Przestępstwo polega na zakłócaniu lub paraliżowaniu funkcjonowania systemów informatycznych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli. Należy stwierdzić, że jest to kwalifikowana forma czynu z art. 268 § 2 kk, tj. niszczenia informacji z uwagi na wyższe zagrożenie karą. Sprawca tego przestępstwa, który niszczy informacje zapisane na komputerowym nośniku, a mające szczególne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej – podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Dodać należy, że ustawodawca oprócz formy sabotażu związanej z niszczeniem informacji wyróżnia także działanie polegające na zakłócaniu lub uniemożliwianiu automatycznego gromadzenia lub przekazywania informacji.

Sabotaż komputerowy może wystąpić także w formie niszczenia lub wymiany nośnika informacji, niszczenia lub uszkodzenia urządzeń służących do automatycznego przetwarzania, gromadzenia lub przesyłania informacji (art. 269 § 2 kk). Czyny te zagrożone są także karą pozbawienia wolności do lat 8.

Cytowany przepis nie przewiduje odpowiedzialności karnej za sabotaż komputerowy z winy nieumyślnej. Mam tu na uwadze ewentualność skutków, o których mowa wyżej, w przypadku nieumyślnego zawirusowania programu. Problem ten wzbudza poważne kontrowersje, gdyż niezwykle trudno będzie udowodnić umyślne zawirusowanie.

W rozdziale „Przestępstwa przeciwko mieniu" określono następujące czyny karalne:

Nielegalne uzyskanie programu komputerowego – art. 278 § 2 kk

Karalne jest uzyskanie, a mówiąc wprost, kradzież cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej. Przepis ten jest odpowiednikiem przestępstwa związanego z kradzieżą rzeczy ruchomej przewidzianego w art. 278 § 1 kk. Program komputerowy nie jest rzeczą ruchomą, lecz może stanowić przedmiot majątkowych praw autorskich. Wiadomo, że powszechne jest nielegalne kopiowanie programów komputerowych zabronione również zgodnie z art. 115 ust. 3 ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. Nr 24, poz. 83).

Art. 278 § 2 kk umożliwia bardziej radykalne ściganie piractwa komputerowego ze względu na sankcję karną. Wspomniany artykuł przewiduje karę pozbawienia wolności od 3 miesięcy do lat 5. Natomiast kwalifikowana forma przestępstw z art. 117 i 118 ustawy o prawie autorskim przewiduje karę pozbawienia wolności do lat 3, tj. w przypadkach, gdy sprawca uczynił sobie stałe źródło dochodów, organizował lub kierował działalnością przestępczą związaną z piractwem komputerowym.

Jeżeli nielegalne uzyskanie programów komputerowych dotyczy mienia znacznej wartości[4] to zgodnie z art. 294 § 1 kk sprawca dopuszcza się przestępstwa kwalifikowanego i czyn jego jest zagrożony karą pozbawienia wolności od roku do lat 10.

Paserstwo programu komputerowego – art. 293 § 1 kk

Karalne jest nabycie, pomoc w zbyciu, przyjęcie lub pomoc w ukryciu pirackiej kopii programu komputerowego w celu osiągnięcia korzyści majątkowej. Przepis ten przewiduje karę pozbawienia wolności od 3 miesięcy do lat 5. W przypadku mniejszej wagi, sprawca podlega karze grzywny, karze ograniczenia wolności albo pozbawienia wolności do jednego roku.

Jako przypadek mniejszej wagi należy rozumieć fakt, że sprawca nie działał w celu osiągnięcia korzyści majątkowej, program zainstalował jedynie we własnym komputerze albo pomagał w zbyciu lub ukryciu programu za pośrednictwem sieci komputerowej.

Istnieje również możliwość odpowiedzialności karnej za paserstwo programu komputerowego przewidziane w art. 118 ust. 1 ustawy o prawie autorskim, który przewiduje karę łagodniejszą.

Nie są to zresztą jedyne przepisy nowego kodeksu karnego i ustawy o prawie autorskim i prawach pokrewnych, które zachodzą na siebie lub traktują rozbieżnie pewne istotne zasady prawne. Przykładowo, paserstwo z art. 293 § 1 kk ścigane jest z oskarżenia publicznego, a paserstwo z art. 118 ust. 1 z oskarżenia prywatnego.

Oszustwo komputerowe – art. 287 § 1 kk

Przestępstwo polega na osiągnięciu korzyści majątkowej lub wyrządzeniu innej szkody poprzez wpływ na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji. Formy działania mogą być zróżnicowane i polegać na zmianie, usunięciu lub na wprowadzeniu nowego zapisu na komputerowym nośniku informacji.

Przepis nawiązuje do klasycznej formy oszustwa (art. 286 § 1 kk), w której oszust, dla 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 podejmowania określonego działania.

W klasycznym oszustwie dochodzi do odpowiednich, tj. karalnych, relacji pomiędzy sprawcą a ofiarą. Natomiast w oszustwie komputerowym człowiek (przestępca) oddziałuje na komputer i odpowiedni program. Manipulacje oszusta dotyczą wprowadzenia danych, wpływania na program i wyniki uzyskanych danych. Oszustwa komputerowe występują bardzo często, a ich zakres jest praktycznie nieograniczony. Zatem art. 287 § 1 kk zabrania wszelkich form manipulacji danymi komputerowymi, które mają na celu wyrządzenie szkody majątkowej innej osobie. Klasyczne oszustwo (art. 286 § 1 kk) zagrożone jest karą pozbawienia wolności od 6 miesięcy do lat 8, a oszustwo komputerowe – karze pozbawienia wolności od 3 miesięcy do lat 5. W sprawie tej można mieć poważne wątpliwości w świetle narastających zagrożeń oszustwami komputerowymi.

W przypadku mniejszej wagi (art. 287 § 2 kk) sprawca podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do jednego roku.

W rozdziale „Przestępstwa przeciwko wiarygodności dokumentów" wyłonić należy:

Fałszerstwo komputerowe – art. 270 § 1 kk

Przestępstwo to polega na przerabianiu czy podrabianiu dokumentów w formie zapisu elektromagnetycznego, tj. czytelnego przez wyspecjalizowane urządzenia. Fałszerstwo komputerowe nie zostało wyróżnione jako odrębny typ przestępstwa. Ustawodawca nie widzi takiej potrzeby, bowiem z powo-

dzeniem może być zastosowany obowiązujący przepis, tj. art. 270 § 1 kk (fałszerstwo dokumentów).

Pojęcie dokumentu zostało określone w art. 115 § 14 kk i uwzględnia zapis na komputerowym nośniku informacji, a mianowicie:

„Dokumentem jest każdy przedmiot lub zapis na komputerowym nośniku 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".

W świetle tej definicji sprawca, który sfałszował wydruk komputerowy lub inny nośnik informacji komputerowej, podlega odpowiedzialności karnej z art. 270 § 1 kk, a jego czyn zagrożony jest karą grzywny, karą ograniczenia wolności albo karą pozbawienia wolności od 3 miesięcy do lat 5.

Inne rodzaje przestępstw

Nielegalne kopiowanie, rozpowszechnianie lub publikowanie prawnie chronionego programu komputerowego

Program komputerowy, zgodnie z art. 1 ust. 2 pkt 1 ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. Nr 24, poz. 83), jest przedmiotem prawa autorskiego, tak samo jak utwory artystyczne, literackie i fonograficzne, czyli jako utwór podlega ochronie prawnokarnej. Dotyczy to każdej formy tego programu np. dokumentacji projektowej, fazy wytwórczej czy użytkowej.

W związku z powyższym w zakresie ochrony programów komputerowych karalne jest:

- przywłaszczenie autorstwa lub wprowadzenie w błąd co do autorstwa całości lub części utworu (art. 115 ust. 1);
- rozpowszechnianie cudzego utworu, czyli programu bez podania nazwiska lub pseudonimu twórcy (art. 115 ust. 2);
- inne naruszenie cudzego prawa autorskiego w celu uzyskania korzyści majątkowej (art. 115 ust. 3);
- rozpowszechnianie bez upoważnienia albo wbrew jego warunkom cudzego programu (art. 116 ust. 1);
- utrwalanie lub zwielokrotnienie bez uprawnienia lub wbrew jego warunkom cudzego programu (art. 117 ust. 1);
- paserstwo przedmiotu będącego nośnikiem programu (art. 118);
- uniemożliwienie lub utrudnienie wykonywania prawa do kontroli korzystania z programu (art. 119).

Sprawcy powyższych przestępstw, którzy działali w celu osiągnięcia korzyści majątkowej, podlegają karze grzywny, ograniczenia wolności oraz pozbawienia wolności do lat 5, a jeżeli czynili z tego stałe źródło dochodu – do lat 8.

Nielegalne kopiowanie układów scalonych zabronione jest zgodnie z art. 42 ustawy z dnia 30 października 1992 roku o ochronie topografii układów scalonych (Dz.U. Nr 100, poz. 498).

Warto wyjaśnić, że przez topografię półprzewodnika należy rozumieć takie rozwiązanie, które polega na przestrzennym, wyrażonym w dowolny sposób rozplanowaniu elementów, z których co najmniej jeden jest elementem aktywnym w stosunku do wszystkich lub części połączeń układu scalonego.

Wybrane problemy ujawniania i ścigania przestępstw komputerowych

Dotychczasowa praktyka śledcza oraz orzecznictwo sądowe wskazują na ograniczone możliwości ścigania sprawców omawianych przestępstw. Przyczyny takiego stanu rzeczy są bardzo zróżnicowane, a wynikają przede wszystkim ze specyfiki przestępstw komputerowych.

Specyfika tych przestępstw polega przede wszystkim na niekonwencjonalnym sposobie działania sprawców, a w związku z tym konieczne są nowe, niekonwencjonalne, tj. inne niż w klasycznej kryminalistyce, metody wykrywania.

Specyfika przestępstw komputerowych polega przede wszystkim na:

- ponadnarodowym charakterze czyli transgranicznym działaniu sprawców,
- możliwości zdalnego działania sprawców,
- możliwości łatwego kamuflowania swojego czynu.

Ponadto, sprawca przestępstwa nie musi być obecny na miejscu przestępstwa, a zatem nie zostawia śladów (daktyloskopijnych, mechanoskopijnych, traseologicznych itp.). Natomiast posiada możliwość usuwania śladów przestępnego działania w ramach procedury likwidacji dokonanego zapisu.

Trudności związane ze ściganiem nawet ujawnionych już sprawców przestępstw komputerowych spowodowane są różnorodnymi trudnościami dotyczącymi zarówno problemów natury ogólnej, jak np. ciągły brak jeszcze świadomości występujących zagrożeń oraz natury szczegółowej, jak np.:

- różnorodność systemów operacyjnych oraz oprogramowania użytkowego,
- trudności związane z umiejętnym zabezpieczaniem materiałów dowodowych, a także brak odpowiednich (specjalistycznych) procedur w tym zakresie,
- trudności z uzyskaniem specjalistycznych opinii kryminalistycznych.

Wszystkie te elementy związane są z brakiem odpowiednio przygotowanej profesjonalnej kadry w organach ścigania i wymiaru sprawiedliwości.

Jerzy Wojciech Wójcik

PRZYPISY

[1] Obowiązuje od dnia 1 września 1998 r.

[2] Ustawa z dnia 23 kwietnia 1964 roku – kodeks cywilny (Dz.U. Nr 16, poz. 93 z późn. zm.).

[3] Wyrok Sądu Apelacyjnego Nr I A Cr 529/95 z dnia 7 listopada 1995 roku. Patrz glosa J. Panowicz-Lipskiej (OSP Nr 7–8 z 1996 r., poz. 143).

[4] Zgodnie z art. 115 § 5 kk mieniem znacznej wartości jest mienie, którego wartość w chwili popełnienia czynu zabronionego przekracza dwustukrotną wysokość najniższego miesięcznego wynagrodzenia.

Autor – dr nauk prawnych – kryminolog.