Marek Kolecki

Przestępstwa komputerowe w ustawodawstwie federalnym Stanów Zjednoczonych A.P.

Palestra 36/5-6(413-414), 52-63

1992

Marek Kolecki

Przestępstwa komputerowe w ustawodawstwie federalnym Stanów Zjednoczonych A.P.

Komputery stały się obecnie głównym środkiem przyspieszonego uzyskiwania i przetwarzania informacji na skalę dotychczas nie spotykaną. Przez wiele lat dane uzyskiwane za pośrednictwem komputera miały charakter danych prawdziwych. Jednakże komputer staje się w coraz większym stopniu narzędziem przestępstwa mogącego przynieść nieobliczalne skutki. Dlatego też w wielu krajach zagadnienie to jest już regulowane w poszczególnych ustawach, a w innych zgłoszono już odpowiednie propozycje do kodeksów karnych.

O przestępstwach komputerowych w ustawodawstwie amerykańskim można mówić na podstawie przepisów prawa federalnego, jak i stanowego. Obecnie omówię to zagadnienie na podstawie ustawodawstwa federalnego, natomiast w następnym artykule spróbuję rozwinąć ten temat na podstawie ustawodawstwa stanowego.

Problem ten pragnę przedstawić na podstawie literatury amerykańskiej, a dla pełniejszej ilustracji chciałbym na wstępie przytoczyć przebieg zdarzenia, które ma już swoje stałe miejsce w literaturze przedmiotu. Zdarzeniem tym był pierwszy o tak dużym zasięgu i skutkach atak wirusa komputerowego, który ujawnił nieznaną dotychczas skalę zagrożenia, jakim mogą być w przyszłości przestępstwa komputerowe. *Cornell virus*, bo tak właśnie nazwano w literaturze przedmiotu ten przypadek, dał podstawę do przyjęcia odpowiednich sformułowań prawnych zarówno w przepisach ustaw, jak i w orzecznictwie. Również w przyszłości na ten właśnie *casus* będą się powoływali z pewnością sędziowie sądów amerykańskich, orzekając w podobnych sprawach.

1. Wirusy komputerowe - nowe, nieznane źródło zagrożenia

Zaskakujacy atak wirusa komputerowego, nazwanego później *Cornell virus*, rozpoczął się pomiędzy godz. 21 a 22 w nocy 2 listopada 1988 r. w Stanach Zjednoczonych A.P. Pierwszym miejscem ataku były dwa najważniejsze centra naukowo-badawcze: Berkeley w Kalifornii oraz Cambridge w stanie Massachuseths. O godz. 22^{34} atakujący dalej wirus blokuje ośrodek komputerowy w Pinceton University, a następnie tak poważne obiekty, jak: NASA (*National Aeronautics and Space Administration*, czyli Narodowy Zarząd Lotniczy i Kosmiczny), Centrum Naukowe w Silicon Valley w Kalifornii oraz Narodowe Laboratorium Los Alamos w Nowym Meksyku. O godz. 12^{31}, 3 listopada 1988 r. wirus atakuje systemy komputerowe uniwersytetu J. Hopkinsa w Baltimore, a o godz. 1^{15} uniwersytetu Michigen w Ann Arbor.[1] O godz. 2^{28} oblegany przez wirusa naukowiec w Berkeley (podobnie jak atakowany na pierwszej linii żołnierz) wysłał do wszystkich komunikaty: „aktualnie jesteśmy pod ata-

kiem". W ten sposób zaczął się jeden z najbardziej koszmarnych dni komputerowej epoki.

Od czasu tego zaskakującego wydarzenia „wirusy komputerowe" śmiało wkraczają na pierwsze strony gazet oraz innych publikacji nie koniecznie związanych z informatyką. *Cornell virus* swoją działalnością upowszechnił znane dotychczas tylko nielicznym informatykom określenie „wirus komputerowy".

Służby specjalne, składające się z informatyków i elektroników z FBI (Federalne Biuro Śledcze), CIA (Centralnej Agencji Wywiadowczej) i Pentagonu, przeprowadziły superszybkie dochodzenie, które wykazało, że sprawcą tego gigantycznego zamieszania był ... student Uniwersytetu Cornell, 23-letni Robert Morris[2] (stąd nazwa wirusa - *Cornell virus*).

Coraz więcej poważnych instytucji obawia się kłopotów związanych z działalnością wirusów komputerowych. Dotyczy to nawet sił zbrojnych Stanów Zjednoczonych. Urzędnicy do spraw bezpieczeństwa USA obawiają się, że wirusy komputerowe są „zaszczepione" w komputerach Ministerstwa Obrony. Urzędnicy ci są zaniepokojeni, że w przypadku uaktywnienia się wirusa podczas kryzysów militarnych mogłyby one spowodować porażenie elektroniczne ośrodków dowodzenia USA.[3]

Wirusy komputerowe próbuje się wykorzystywać do zmagań militarnych. I nie ukrywają tego nawet supermocarstwa, wręcz przeciwnie. Ministerstwo Obrony USA ogłosiło konkurs na zaprojektowanie wirusa komputerowego, który drogą łączności radiowej mógłby zostać przesłany do komputerów przeciwnika i tam sparaliżować (obezwładnić) ośrodki dowodzenia. O tym, że jest to poważne przedsięwzięcie niech świadczy fakt, że armia amerykańska przeznaczyła ponad pół miliarda dolarów na prace badawcze nad wirusami komputerowymi.

A oto kilka pytań związanych z omawianym zagadnieniem:

Czym są wirusy komputerowe?

Jak duże zagrożenie może nieść ze sobą ich pojawienie się w sytemie komputerowym?

Jak się przed nimi bronić?

Jak opracować najskuteczniejsze zabezpieczenia?

I wreszcie najważniejsze pytanie:

Czy wobec faktu wykorzystania wirusów komputerowych w dziedzinie militarnej, mogą one w przyszłości realnie zagrozić lub mieć znaczący wpływ na globalne bezpieczeństwo?

Na cały szereg tych i podobnych pytań od wielu lat próbują znaleźć odpowiedź specjaliści odpowiedzialni za zabezpieczenia komputerowe.

Wirusy komputerowe z roku na rok śmielej atakują coraz to poważniejsze obiekty. Ich „twórcy" już nie zadowalają się atakowaniem poszczególnych użytkowników. Swoimi atakami usiłują objąć coraz szersze kręgi użytkowników, paraliżując niekiedy całe lokalne systemy informatyczne. Duże możliwości szybkiego rozprzestrzeniania się wirusów, anonimowość ich „twórców", wreszcie poczucie bezkarności wynikajace z prawie zerowej wykrywalności, powodują ciągłą eskalację tego negatywnego zjawiska, jakim jest przestępczość komputerowa. O tym, że przestępstwa komputerowe są trudne do wykrycia niech świadczy fakt, że wykrywa się zaledwie 1% ogólnej liczby przestępstw komputerowych (nie uwzględniając w tym danych tzw. ciemnej liczby). Przestępstwa te są przez kryminologów oceniane jako niemal doskonałe, a większość z nich

jest ujawniana przez przypadek. Według danych amerykańskich, w 1990 r. FBI przeprowadziło ponad 30 dochodzeń przeciwko komputerowym „włamywaczom". W Polsce problem ten nie występuje na razie tak jaskrawo, a to ze względu na stosunkowo niski poziom komputeryzacji życia codziennego naszego społeczeństwa.

Nie ochłonęliśmy jeszcze po wiadomości o ataku wirusa komputerowego na elektrownię atomową na Litwie, a już światowe agencje alarmowały o zapowiedzianym na 6 marca br. ataku wirusa komputerowego o imieniu „Michał Anioł" na komputery całego świata.

Wiadomo było tylko, że wirus ten działał już od około roku, a wykryto go między innymi w ośrodku komputerowym Kongresu Stanów Zjednoczonych.

Alarmujące ostrzeżenia napływały z różnych stron świata, gdyż zagrożonych było ok. 70 mln komputerów na całym świecie. Przy okazji tego wydarzenia uaktualniono światowe statystyki dotyczące występowania i klasyfikacji wirusów komputerowych. Okazuje się, że wirusów komputerowych z roku na rok przybywa coraz więcej. Obecnie sklasyfikowano około 1200 wszystkich odmian wirusów łącznie, z czego wyróżniono około 350 najbardziej aktywnych.

Według informacji przekazanych przez Federalny Urząd Bezpieczeństwa Techniki Informacyjnej (BSI) w Niemczech wirus „Michał Anioł" rezydował w tzw. sektorze inicjującym (*boot sector*). Dr Frank Felzmann, jeden z szefów sekcji BSI, określił „Michała Anioła" jako prawdziwego „zabójcę informacji". Natomiast według danych amerykańskich, „Michał Anioł" atakował głównie tzw. twarde dyski komputerów firmy IBM PC AT i XT, pracujące w sytemie operacyjnym DOS.

Wydaje się, że nie mamy obecnie poczucia rzeczywistego zagrożenia, jakim może być użycie wirusów komputerowych przez sfrustrowanych informatyków, wojskowych, czy też terrorystów.

1.1. Badania nad wirusami komputerowymi

Samo zjawisko, polegające na wykorzystaniu wirusów komputerowych, nie jest zjawiskiem aż tak młodym, jakby się to mogło wydawać, chociaż z pewnością jego nasilenie w ostatnich latach jest znaczne. Możliwość istnienia destrukcyjnych programów komputerowych była już znana w latach sześćdziesiątych, natomiast intensywne prace badawcze nad wirusami komputerowymi trwały od połowy lat siedemdziesiątych, kiedy to Xerox Corporation z Rochester (USA) w 1974 r. opracowała i wywołała po raz pierwszy typ samopowielającego się wirusa komputerowego z szyfrem. Wszystkie te eksperymenty były przeprowadzone z zachowaniem pełnej kontroli, która, jak się później okazało, musiała być niezbyt szczelna, skoro w połowie lat osiemdziesiątych częstotliwość wyrządzanych przez wirusy szkód nieustannie rosła. Przykładem bardzo wymownie świadczącym o ciągłej ofensywie wirusów może być fakt, że w ciągu pierwszych 7 miesięcy 1988 r. miało miejsce ponad 300 ataków różnego rodzaju wirusów na ponad 50 tysięcy komputerów.[4]

1.2. Definicja wirusa komputerowego według prof. Freda Cohena

Autorytetem nie budzącym żadnych wątpliwości w dziedzinie badań nad wirusami komputerowymi jest prof. Fred Cohen, wykładowca elektroniki i informatyki Uniwersytetu Cincinnati w stanie Ohio w USA. W swojej pracy doktor-

skiej, właśnie na temat wirusów komputerowych, dokonał analizy naukowej działania wirusów, które określa jako programy:

a) zdolne do rozmnażania, a więc samodzielnego kopiowania się i dołączania do innych programów stających się nosicielami wirusa,

b) zdolne do „przechwytywania" podczas pracy „programu gospodarza" i kontroli nad komputerem w celu wykonania swego zadania.

Wirusy można programować dla bardzo różnych celów, wykorzystując zarówno ich pozytywne, jak i negatywne właściwosci. Programuje się je także, między innymi, dla potrzeb szkolenia, np. sztabowców wojskowych, używając do tego celu gry, tzw. *CORE WARS*. Jest to gra-test, w której samopowielające się i samorozwijające się programy usiłują się nawzajem zwyciężyć w podstępny sposób. Do tego celu wykorzystywane są specjalne komputery, takie jak *Memory Array* lub *Recode Simulator*, wraz ze specjalnym oprogramowaniem. Test ten odbywa się według dwóch podstawowych reguł:

1) współkonkurujące programy muszą zniszczyć przeciwnika zgodnie z instrukcją,

2) program, który przegrywa po prostu przestaje funkcjonować.

Wirusy komputerowe, podobnie jak i inne programy, nie muszą być koniecznie destruktywne.[5]. *Mass media* używają terminu „wirus komputerowy", aby wskazać na jego szkodliwość, co jednak nie jest zgodne do końca z prawdą. Programiści komputerowi rozwijają również twórcze, w znaczeniu pozytywnym, funkcje dla takich programów. Przykładem mógłby być program przeznaczony do kondensowania danych, czyli do magazynowania ich w mniejszych odstępach przestrzeni.

Mówiąc o pozytywnych aspektach działalnosci wirusów komputerowych warto przytoczyć opinię na ten temat, jaką wypowiedział na łamach amerykańskiego czasopisma „The Sciences" prof. Fred Cohen: „Choć nie ma wątpliwości co do tego, że trzeba zapanować nad złośliwymi wirusami, to równie ważne jest, by strach przed wirusem nie zahamował badań nad wielorakimi korzyściami, jakie mogą przynieść wirusy komputerowe". Tę wypowiedź należałoby uzupełnić informacją, że F. Cohen ustanowił nagrodę, w wysokości jednego tysiąca dolarów, dla twórcy najbardziej użytecznego wirusa roku. I choć propozycja ta nie uzyskała dużego aplauzu wsród specjalistów od zabezpieczeń komputerowych, to jednak sam pomysł należy ocenić pozytywnie.

2. Przestępstwa komputerowe w ustawodawstwie federalnym Stanów Zjednoczonych A.P.

Szeroki zasięg problemu, jakim są przestępstwa komputerowe, przekracza oczywiście skromny zakres tego opracowania, z konieczności więc zajmę się tylko podstawowymi ustawami oraz projektami ustaw, które dotyczą tego zagadnienia.

Jak już była o tym mowa, o przestępstwach komputerowych w ustawodawstwie amerykańskim można mówić zarówno na podstawie przepisów prawa federalnego, jak i stanowego. Samo pojęcie „przestępstwo komputerowe" jest bardzo pojemne, a przy tym nieostre; w jego zakres wchodzić może zarówno kradzież informacji z komputera, zmiana lub zniszczenie danych komputerowych, czy choćby fizyczne zniszczenie

komputera, lub współpracujacego z nim osprzętu.

„Destruktywne programy komputerowe" (często takim pojęciem określa się w literaturze przedmiotu wirusy komputerowe) mogą być również wykorzystywane jako narzędzie służące do dokonania innych przestępstw komputerowych. Kradzież komputerową, sabotaż komputerowy, oszustwo komputerowe oraz szpiegostwo komputerowe może poprzedzać wcześniejsze użycie wirusa komputerowego, który po „uzyskaniu dostępu" do komputera umożliwi dokonanie kolejnych czynów przestępnych (kradzieży, sabotażu, oszustwa). W tym przypadku sprawca nie musi koniecznie użyć do tego celu wirusa komputerowego. Może to być również inny mniej skomplikowany od wirusów „program destruktywny" wykorzystany np.: tylko jeden raz. Jak z tego wynika możliwości użycia wirusów komputerowych są bardzo duże, dlatego też w artykule tym skoncentruję się głównie na analizie wprowadzenia wirusów komputerowych do obiegu komputerowej informacji.

Te nowe, negatywne zjawiska przestępczości komputerowej zmusiły ustawodwcę amerykańskiego do podjęcia bardziej zdecydowanych działań w celu ich ograniczenia.

Uświadamiając sobie z niepokojem zagrożenia spowodowane przestępczością komputerową Kongres Stanów Zjednoczonych przyjął projekty ustaw dotyczące:

a) działalności wirusów komputerowych, a konkretnie ich wytępienia, co dobitnie wyraża tytuł ustawy „Computer Virus Eradication Act of 1989",[6]

b) ochrony zarówno komputera, jak i sprzętu komputerowego przed sabotażem (ustawa „Computer Protection Act of 1989").[7]

Procedura ustawodawcza w USA nie należy do najprostszych, lecz przypadek „wirusa Cornell" i blokada w wyniku tego ponad 6000 komputerów[8] na terenie całych Stanów Zjednoczonych z pewnością przyczyniły się do tego, że kongresmeni zaczęli poważniej spoglądać na problem przestępczości komputerowej.

Prekursorem parlamentarnej walki z wirusami komputerowymi jest członek Izby Reprezentantów, kongresmen Wally Herger[9] z Kalifornii. 3 stycznia 1989 r. kongresmen W. Herger, wraz z 33 innymi sponsorami, przedstawili w Kongresie projekt ustawy, nazwany „Computer Virus Eradication Act of 1989", jako poprawkę do (obowiązującej w momencie zgłoszenia tej inicjatywy ustawodawczej) ustawy o oszustwach i nadużyciach komputerowych, znanej jako „Computer Fraud and Abuse Act of 1986".[10]

Poprawka do federalnej ustawy „Computer Fraud and Abuse Act of 1986" składała się z dwóch odrębnych projektów ustaw „A" i „B", z których pierwszy „A" - to wyżej wymieniony już „Computer Virus Eradication Act of 1989", oznaczony jako dokument Izby Reprezentantów symbolem H.R.55. Drugi „B" - to „Computer Protection Act of 1989", którego autorem był kongresmen Mc Millen ze stanu Maryland, a który został również przedstawiony w Kongresie w dniu 3 stycznia 1989 r. i oznaczony symbolem H.R.287. Obydwa wyżej wymienione projekty ustaw składają się na całość poprawki do ustawy o oszustwach i nadużyciach komputerowych z 1986 r.

Jak już wspomniałem, procedura ustawodawcza w Stanach Zjednoczonych jest równie ciekawa, co i skomplikowana. Podstawową strukturę wewnętrzną obu izb Kongresu, czyli Senatu

i Izby Reprezentantów, stanowią stałe komisje. Bardzo istotną ich rolą jest udział w procesie prawotwórczym. Każda zainicjowana ustawa jest już po pierwszym czytaniu przesyłana do odpowiedniej, stałej komisji Kongresu. Jedną z powszechnie stosowanych form pracy stałej komisji w toku legislacji jest tzw. *hearings*,[11] czyli publiczne przesłuchanie, prowadzone przez komisję w związku z przedstawionym jej do zaopiniowania projektem ustawy. Bardzo często te publiczne przesłuchania w Kongresie są transmitowane przez telewizję. Można więc zapytać, jaki jest cel tych przesłuchań? Przede wszystkim „hearings" daje nie tylko okazję do publicznej prezentacji projektu ustawy przez ich inicjatorów, ale również umożliwia bezpośrednie przedstawienie na forum Kongresu swego stanowiska przez osoby lub grupy nacisku spoza Kongresu. Przez taką procedurę przechodził również projekt ustawy W. Hergera „Computer Virus Eradication Act of 1989". Referentem tego projektu przed jedną z podkomisji Izby Reprezentantów był przewodniczący sekcji American Bar Association, pan Joseph B. Tompkins Jr.[12] Po zakończeniu przesłuchań projekt tej ustawy nie był głosowany zarówno w Izbie Reprezentantów, jak i w Senacie.

2.1. „Computer Virus Eradication Act of 1989"

Ustawa „Computer Virus Eradication Act of 1989" jest w literaturze przedmiotu określana w skrócie jako „Computer Virus Act of 1989". Jednakże, poza samą nazwą ustawy, nie zawiera ona w treści swych przepisów takiego sformułowania, jak „wirus komputerowy".

„(a)(7)(A) Każdy, kto świadomie wprowadza do programu przeznaczonego dla komputera lub do samego komputera informacje lub polecenia, wiedząc lub przypuszczajac, że taka informacja lub takie polecenie może spowodować stratę, wydatek lub ryzyko dla zdrowia lub dobra:

- użytkowników takiego komputera lub komputera, na którym pracuje taki program, lub osób, które polegają na informacji przetworzonej przez taki komputer, lub

- użytkowników innego komputera, lub osób, które polegają na informacji przetworzonej przez jakikolwiek inny komputer, lub

(B) dostarcza (wiedząc o istnieniu takiej informacji lub poleceń) taki program lub taki komputer osobie w okolicznościach, w których taka osoba nie jest świadoma takiej (informacji lub poleceń) lub jej skutków,

jeżeli wprowadzanie lub dostarczenie takiej informacji lub poleceń wpływa na międzystanowy lub zagraniczny handel.[13]

Każdy, kto popełnia lub usiłuje popełnić przestępstwo podpadające pod punkt (a)(7)(A)(B) będzie ukarany: karą grzywny, lub karą pozbawienia wolności do lat 10, lub obiema tymi karami łącznie."

To, że pojęcie „wirus komputerowy" nie jest użyte w treści tej ustawy może, między innymi, wynikać z faktu napotkania trudności w określeniu zakresu definicji samego wirusa, którego to potencjalnych możliwości do końca nie zbadano. W odróżnieniu od ustawodawcy federalnego przepisy niektórych kodeksów stanowych definiują jednak, jakkolwiek w różny sposób, wirusa komputerowego.

Z treści przepisów tej ustawy wynika, że taką samą sankcją objęte jest zarówno dokonanie czynu przestępnego, jak i jego usiłowanie. Rzeczą dyskusyj-

ną wydaje się natomiast górna granica kary pozbawienia wolności, zwłaszcza że w przypadku powrotu do przestępstwa, ustawodawca przewiduje możliwość zagrożenia karą pozbawienia wolności do lat 20. Chcąc uzyskać w miarę obiektywne spojrzenie na ten problem, należy również, a może nawet przede wszystkim, pamiętać o możliwości nieobliczalnych skutków, jakie może przynieść ze sobą nagły atak wirusa komputerowego na systemy obronne państw czy też centra finansowe. Dlatego też taki, a nie inny, dobór wysokości sankcji świadczyć może o poważnym traktowaniu przez ustawodawcę problemu przestępstw komputerowych. O wyborze rodzaju sankcji, jak i jej wysokości decyduje sędzia, który, biorąc pod uwagę amerykański system sądownictwa, ma sporo możliwości kształtowania przepisów prawa. Jest to bardzo istotny i charakterystyczny element pozycji sędziego w sądownictwie amerykańskim. Innym elementem różniącym sądownictwo europejskie od sądownictwa amerykańskiego jest to, że sędziowie sądów amerykańskich mają prawo do badania zgodności ustaw z Konstytucją USA oraz z konstytucjami stanowymi. Jest to instytucja określana jako *judical review*. Kolejnym charakterystycznym elementem amerykańskiego wymiaru sprawiedliwości jest również ława przysięgłych (*jury*), która trafiła na kontynent amerykański jeszcze w czasach kolonialnych, podobnie jak system prawa *common law*. Jest to bardzo ważna instytucja, u której podstaw leży zapis w Konstytucji Stanów Zjednoczonych w artykule III ust. 2, a który gwarantuje wyraźnie, że „wszystkie sprawy karne, poza wszczętymi wskutek postawienia w stan oskarżenia przez Izbę Reprezentantów, rozpatruje sąd przysięgłych".

2.2. „Computer Protection Act of 1989"

Kolejnym projektem ustawy jest „Computer Protection Act of 1989" (H.R. 287), który to projekt jest poświęcony w całości przestępstwom polegającym na sabotażu komputerowym. Przepisy projektu tej ustawy nie ograniczają się jednak do ochrony samego komputera, ale również przewidują, między innymi, ochronę związanego z nim oprogramowania.

„Każdy, kto celowo sabotuje właściwe działanie osprzętu komputerowego, lub związanego z nim oprogramowania i w ten sposób powoduje: utratę danych, uszkodzenie poprawności działania komputera, lub wymierną stratę właścicielowi komputera; będzie ukarany: karą grzywny, lub karą pozbawienia wolności do lat 15, lub obiema tymi karami łącznie."[14]

Przepisy projektu tej ustawy dopuszczają także możliwość wniesienia powództwa cywilnego:

Strona, która doznała szkody z powodu naruszenia tych przepisów przez sprawcę, może w powództwie cywilnym szukać właściwej rekompensaty za szkody spowodowane przez to naruszenie.

W zależności od uznania sądu, strona wnosząca powództwo może uzyskać w całości lub w części zwrot kosztów sądowych wynikających z tytułu wniesienia powództwa.[15]

Obecnie wszelka działalność człowieka determinowana jest w szczególności poprzez informacje. Dlatego niezmiernie ważnym elementem jest jej wiarygodność, dokładność i szybkość. Łatwo więc zauważyć, że informacja ma kapitalne znaczenie w procesie kierowania państwem, firmą, czy też ośrodkiem politycznym. I tu możemy uświadomić sobie, jak duże zagrożenie może powo-

dować jakikolwiek negatywny wpływ na informację będącą w obiegu wielkich ośrodków finansowych, zbrojnych sił strategicznych o globalnym zasięgu itd., które przecież korzystają z informacji znajdującej się w obiegu wielu sieci komputerowych łączących całe kontynenty.

Reasumując, można chyba zaryzykować tezę, że przedmiotem przestępstw komputerowych jest przede wszystkim (ale nie tylko) w szerokim tego słowa znaczeniu sama informacja, jak również obieg tej informacji w komputerze oraz w całym systemie połączeń komputerowych.

Stroną podmiotową przestępstw komputerowych jest umyślność, czyli sytuacja, w której sprawca czynu przestępnego całą swoją świadomością obejmuje zarówno swój czyn, jak i jego skutki. Przestępstwa komputerowe są przestępstwami umyślnymi, choć nie można wykluczyć tu i innych form winy, jak na przykład lekkomyślne obchodzenie się z „zainfekowanym programem", jeżeli taka osoba wie, że program ten zawiera w sobie wirusa i przewiduje możliwość utraty kontroli nad takim programem, lecz bezpodstawnie przypuszcza, że jakoś uda się tego uniknąć. Takim przykładem przestępstwa nieumyślnego może być również niedbałe zabezpieczenie dostępu do komputera przez osobę do tego zobowiązaną, co w efekcie może umożliwić dokonanie przestępstwa. Przestępstwa komputerowe są przestępstwami bardzo trudnymi do wykrycia, a przez kryminologów są oceniane jako niemal doskonałe, gdyż większość z nich jest ujawniana przez przypadek.

W Polsce, jakkolwiek przestępstwa komputerowe nie są obce, to stosunkowo niski poziom komputeryzacji życia codziennego powoduje, że skala tego zjawiska nie jest aż tak niepokojąca jak w Europie Zachodniej, czy też w USA. Niemniej jednak, chcąc uniknąć przykrych niespodzianek w przyszłości, należy już dzisiaj czynić pewne kroki w kierunku prawnej regulacji tego zjawiska, jakim jest przestępczość komputerowa. W dobie przyspieszonej integracji gospodarczej i prawnej z krajami EWG będą to z pewnością kroki konieczne.

2.3. „Computer Fraud and Abuse Act of 1986" (C.F.A.A.)

Przepisy tej federalnej ustawy z 1986 r. o oszustwach i nadużyciach komputerowych nie chronią bynajmniej wszystkich komputerów przed potencjalnymi przestępcami. Jak twierdzi komisja senacka C.F.A.A. była przewidziana dla ochrony *„komputerów federalnych"*.

Ustawa „Computer Fraud and Abuse Act of 1986" składa się z 6 punktów oznaczonych kolejnymi literami alfabetu. Punkt pierwszy (a), składajacy się z 6 podpunktów, zawiera dyspozycję ustawy. Cztery z sześciu tych podpunktów nie mają jednak zastosowania do wirusów komputerowych.

Bardzo istotnym elementem tej ustawy jest podpunkt piąty §1030 (a) (5) (A), który wprowadza nową nazwę komputera - *„komputer federalny"*. Pojawia się więc nowa kategoria komputerów, której wyodrębnienie odbywa się na podstawie swoistego kryterium, którym jest wyłączność użytkowania.

Definicja komputera federalnego zamieszczona jest w punkcie (e)(2) §1030 i brzmi następująco:

„Federalny komputer oznacza komputer przeznaczony wyłącznie do użytku instytucji finansowych lub Rządu Stanów Zjednoczonych lub komputer uży-

wany przez lub dla instytucji finansowej albo Rządu Stanów Zjednoczonych".

Nie chodzi tu oczywiście o dowolne instytucje finansowe, ale tylko o te, które ustawa o oszustwach i nadużyciach komputerowych enumeratywnie wylicza w punkcie (e)(4) §1030. Według tego punktu takimi instytucjami finansowymi są między innymi:

- bank z depozytami ubezpieczonymi przez Federal Deposit Insurance Corporation,
- Federal Reserve lub członek Federal Reserve, łącznie z każdym Federal Reserve Bank, oraz
- każda instytucja Farm Credit System wskazana przez ustawę „The Farm Credit Act of 1971".

Na podstawie przepisów ustawy o oszustwach i nadużyciach komputerowych [C.F.A.A. §1030 (a)(5)(A)] jako jeden z pierwszych stanął przed sądem Robert Morris, autor programu nazwanego *„Cornell virus"*.[16] Proces rozpoczął się 26 lipca 1989 r. przed sądem w Syrakuzach (stan Nowy Jork). Czyn R. Morrisa został potraktowany przez większość z 11 przysięgłych z całą wyrozumiałością, gdyż uwierzyli oni w to, że po uruchomieniu wirusa nie mógł on nic zrobić, żeby go zatrzymać. Po napisaniu programu wirusa, za pomocą komputera i telefonu włączył się do sieci komputerowej Instytutu Technologii Massachusetts, a poprzez nią do ogólnokrajowej sieci „Internet".[17] R. Morris, między innymi, uniemożliwił autoryzowane korzystanie z *„komputerów federalnych"*, co również jest karalne na podstawie przepisów ustawy o oszustwach i nadużyciach komputerowych.

„Każdy, kto celowo korzysta z dostępu do komputera federalnego bez upoważnienia i jednokrotnie lub wielokrotnie: zmienia, uszkadza lub niszczy informacje w którymś z komputerów federalnych, albo uniemożliwia autoryzowane korzystanie z takiego komputera lub informacji i z tego tytułu:[18]

(A) powoduje stratę, lub straty o łącznej wartości 1000 dolarów USA lub więcej w okresie jednego roku będzie ukarany:

karą grzywny lub karą pozbawienia wolności do lat 5, lub obiema tymi karami łącznie." [19]

„Cornell virus" został sklasyfikowany jako *„worm virus"*, czyli nie był on wirusem mogącym wywołać te najbardziej ujemne skutki. Był on natomiast samopowielającym się programem, przekazywanym przez sieci komputerowe, ale nie starającym się, w odróżnieniu od innych wirusów, niszczyć dane. Jego głównym celem było blokowanie pracy komputerów przez „odcinanie" ich od oprzyrządowania oraz sieci komputerowych.

Proces R. Morrisa zakończył się 22 stycznia 1990 r. Sędzia Howard G. Munson wymierzył R. Morrisowi karę 3-letniego nadzoru sądowego, 10 tysięcy dolarów grzywny, oraz 400 godzin pracy na rzecz miasta. Sąd apelacyjny podtrzymał wyrok sądu pierwszej instancji.

W sprawie R. Morrisa trudno jest jednoznacznie określić motywy jego działania. W tym konkretnym przypadku jednym z czynników motywujących działalność przestępczą, może być fakt potraktowania systemu komputerowego jako intelektualnego wyzwania dla młodego, ambitnego, dobrze wykształconego w tej dziedzinie człowieka. Łamanie szyfrów i różnego rodzaju zabezpieczeń może być traktowane na początku jako zabawa, gra czy hazard. Pozwala to zdobyć niezbędne umiejętności do wprowadzania później wirusa do systemu kom-

puterowego bez żadnego ryzyka i ze zmniejszonymi oporami moralnymi.

„*Cornell virus*" dramatycznie pokazał, że niewłaściwe użycie komputera jest poważną groźbą dla społeczeństw ery informatycznej.

3. Penalizacja przestępstw komputerowych w polskim prawie karnym

W obecnie obowiązującym w Polsce kodeksie karnym nie ma przepisów, które dotyczyłyby przestępstw komputerowych. Istnieje natomiast w projekcie nowego kodeksu karnego art. 283 (Rozdz. 35 pt. „Przestępstwa przeciwko mieniu") o następującej treści:

„§1. Kto w celu osiągnięcia korzyści majątkowej przez ukształtowanie programu komputerowego, włączenie do pamięci komputera niewłaściwych lub niepełnych informacji, albo przez inne oddziaływanie na przetwarzanie informacji wpływa na wynik opracowania, powodując tym szkodę majątkową innej osobie, podlega karze pozbawienia wolności od 3 miesiecy do lat 5.

§2. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego."

Tworzenie nowych norm prawnych, będących odpowiedzią na zagrożenie przestępczością komputerową, to w tej chwili nieunikniona konieczność. Dlatego dobrze się stało, że w projekcie nowego kodeksu karnego znalazł dla siebie miejsce art. 283.

Nawiązując do dyspozycji zawartej w art. 283 wydaje mi się, że swoim zakresem zbyt wąsko ona ujmuje nadchodzący problem przestępczości komputerowej (być może w swoim założeniu miała głównie dotyczyć oszustw komputerowych).

Moją propozycją w tym zakresie byłoby zamieszczenie w kodeksie karnym nowego, odrębnego rozdziału, w części szczególnej, zatytułowanego „Przestępstwa komputerowe". Rozdział ten mógłby w swoim założeniu skoncentrować się na kilku podstawowych problemach, jakimi są:

- oszustwa i nadużycia komputerowe,
- sabotaż komputerowy,
- dystrybucja destruktywnych programów komputerowych,
- kradzież komputerowa,
- ochrona połączeń komputerowych (systemów i sieci komputerowych).

Z tą propozycją wiąże się oczywiście konieczność opracowania nowej siatki pojęć, która łączyłaby pewne charakterystyczne określenia zarówno z dziedziny prawa karnego, jak i informatyki, telekomunikacji, czy też elektroniki. Niezbędna przy tym byłaby współpraca specjalistów z wyżej wymienionych dziedzin nauki.

Chciałbym od razu zaznaczyć, że moja propozycja nie ma charakteru krytyki rozwiązania proponowanego w projekcie nowego kodeksu karnego, czy też oceny art. 283, lecz po prostu jestem przekonany, że przestępstwa komputerowe ze względu na rangę ich potencjalnego zagrożenia powinny być jednak umieszczone w odrębnym rozdziale nowego kodeksu karnego. Oczywiście, w chwili obecnej propozycja ta jest, być może, zbyt daleko idąca,[20] lecz wydaje mi się, że wraz ze wzrostem poziomu komputeryzacji naszego życia opracowanie właściwych przepisów prawnych będzie stanowić konieczny warunek zapewnienia ochrony obiegu informacji.

Przestępstwa komputerowe mogą obejmować swoim zakresem wiele czynów przestępnych takich, jak np.: sabotaż komputerowy, kradzież komputerowa, uzyskiwanie nieuprawnionego do-

stępu do zasobów komputera, wprowadzania wirusa do programu komputera, uszkadzanie, zmianę lub zniszczenie danych komputerowych, oprogramowania, systemów lub sieci komputerowych, albo oszustwa komputerowe. Przy tak dużej liczbie różnych czynów, wydaje się niemożliwe wprowadzenie do kodeksu karnego tylko jednego artykułu, który mógłby swoją dyspozycją obejmować te wszystkie czyny przestępne.

Proponowany przeze mnie jeden z artykułów pt. „Przestępstwa komputerowe" mógłby brzmieć następująco:

Art. ...§1. Kto celowo i bez upoważnienia uzyskuje lub próbuje uzyskać dostęp do komputera i wykorzystując bądź usiłując wykorzystać ten dostęp:

a) powoduje: uszkodzenie, zmianę lub zniszczenie danych komputera, oprogramowania komputerowego, systemu lub sieci komputerowej,

b) powoduje: uszkodzenie, zmianę lub zniszczenie danych komputera, oprogramowania komputerowego systemu lub sieci komputerowej poprzez wprowadzanie do obiegu informacji komputerowej, programu destruktywnego,

c) powoduje jakąkolwiek inną zmianę lub stratę,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5 lub grzywny.

§2. Kto dopuszcza się przestępstwa określonego w §1, wykorzystując przy tym lub przekraczając zakres swojego upoważnienia,

podlega karze pozbawienia wolności od 1 roku do lat 8.

Kolejne artykuły tego rozdziału mogłyby dotyczyć wcześniej już wymienionych podstawowych problemów, np.: oszustw komputerowych, sabotażu komputerowego, kradzieży komputerowej. W związku z tym, że jest to nowe i bardzo trudne zagadnienie, celem moim było tylko zwrócenie uwagi na złożoność tego problemu.

Przy tak szybkim rozwoju technologii komputerowej, jaki obecnie można zauważyć, wiele wskazuje na to, że znajdujemy się obecnie u schyłku czwartej, a u progu piątej generacji komputerów. Wynikają z tego niewątpliwie dwa spostrzeżenia: pierwsze to oczywiście pożądany postęp, drugie to trudna do przewidzenia możliwość zagrożenia przestępczością komputerową. To, co wczoraj było wizją autorów powieści *science-fiction*, dzisiaj może stać się ponurą rzeczywistością.

Mając na uwadze możliwość ujemnych, a nawet katastrofalnych skutków wprowadzenia wirusów programowych do systemów komputerowych, światowe organizacje informatyków występują z apelami i rezolucjami od kilku już lat. Jedną z takich rezolucji podjęto w 1989 r. w San Francisco (USA). W swej treści zwraca ona uwagę na możliwość zagrożenia i w związku z tym apeluje:[21]

- aby wszyscy profesjonalni informatycy na świecie uświadomili sobie niszczycielski potencjał wirusów komputerowych,

- aby wszyscy wykładowcy informatyki uświadomili swym słuchaczom niebezpieczeństwa płynące z występowania wirusów programowych,

- aby wszyscy wydawcy powstrzymali się od publikowania szczegółów dotyczących konkretnych wirusów programowych,

- aby żaden profesjonalny informatyk nie rozpowszechniał świadomie programów z wirusami, wyjąwszy przypadki legalnych badań w ściśle chronionym środowisku i aby wszyscy twórcy systemów wykrywania wirusów i ochrony

przed wirusami zaprzestali rozpowszechniania testowych programów z wirusami,

- aby rządy, uczelnie i producenci komputerów zwiększyli nakłady na badania i tworzenie nowych technik ochrony systemów komputerowych, oraz

- aby rządy podjęły kroki zmierzające do uznania rozpowszechniania wirusów komputerowych za działalność przestępczą w rozumieniu przepisów kodeksów karnych.

Przestępczość komputerowa coraz częściej dotyka najbardziej istotnych dla egzystencji człowieka dziedzin. Przeciwstawianie się tym zagrożeniom to z pewnością duże wyzwanie nie tylko dla informatyków chroniących systemy komputerowe i tworzących zabezpieczenie, ale również i dla prawników.

PRZYPISY*

[1] Hansen, Raymond L. „The Computer Virus Eradication Act of 1989: The War Against Computer Crime Continues", Vol. III, „Software Law Journal" (1990), page 717.
[2] Harold L. Burstyn „Computer Whiz Guilty", A.B.A. Journal, April 1990, page 20.
[3] Peterzell, „Spying and Sabotage by Computer" Time, March 20.1989.
[4] Hansen, Raymond L. „The Computer Virus Eradication Act of 1989: The War Against Computer Crime Continues", Vol. III Software Law Journal (1990), page 718. Mc Affe: „The Virus Cure" Datamation, February 15.1989.
[5] Hansen, Raymond L. „The Computer Virus Eradication Act of 1989: The War Against Computer Crime Continues", Vol. III Software Law Journal (1990), page 721.
[6] H.R. 55, 101 st. Cong., 1 st Sess (1989).
[7] H.R. 287, 101 st. Cong., 1 st Sess (1989).
[8] Chicago Sun-Times, November 10, 1988 col. 1.
[9] Kongresmen Wally Herger w 1988 r. przedstawił również w Kongresie projekt ustawy, dotyczący wirusów komputerowych, nazwany „Computer Virus Eradication Act of 1988". Projekt ten nie był jednak szerzej publikowany, poza zreferowaniem go na posiedzeniu stałej komisji (the House Judiciary Committee during the 100th Congress - H.R. 506i 100th Cong., 2nd, Sess 1988).
[10] 18 U.S.C. §1030 (U.S.C. - United States Code - Penal).
[11] Tomasz Langer: Stany w USA Instytucje - praktyka - doktryna, PWN 1988, s. 25.
[12] Computer Virus Legislation: „Hering Before the Subcommittee on Criminal Justice of the House Committee on the Judiciary" 101 st Cong., 1 st Sess (Nov.8, 1989).
Pan Joseph B. Tompkins Jr. brał udział w pracach legislacyjnych nad projektami ustaw dotyczącymi przestępstw komputerowych, dwukrotnie występując przed podkomisjami Izby Reprezentantów i jeden raz przed podkomisją Senatu. Autor licznych artykułów na temat przestępstw komputerowych, pracownik waszyngtońskiego biura prawnego Sidley & Austin.
[13] H.R. 55, 101 st Cong., 1 st Sess (1989).
[14] H.R. 287, 101 st Cong., 1 st Sess (1989).
[15] H.R. 287, 101 st Cong., 1 st Sess (1989).
[16] Harold L. Burstyn „Computer Whiz Guilty" A.B.A. Journal April 1990, page 20.
[17] „Internet" to główna sieć komputerowa wykorzystywana przy badaniach naukowych w USA, związana z ponad 500 narodowymi, regionalnymi i lokalnymi sieciami komputerowymi. *„Cornell virus"* przedostał się także do dwóch innych sieci komputerowych (ARPANET i MILNET), wykorzystując je do ataku na kolejne obiekty. ARPANET - jest systemem komputerowej łączności między ośrodkami akademickimi na terenie USA, MILNET jest siecią używaną przez Departament Obrony USA.
[18] 18 U.S.C. §1030(a)(5)(A).
[19] 18 U.S.C. §1030(c)(3)(A).
[20] Nie wszystkie państwa, nawet te wysoko uprzemysłowione, mają obecnie przepisy prawne dotyczące np. wirusów komputerowych. Przykładem może tu być Republika Włoska, która takich przepisów nie ma (na podstawie listu otrzymanego od pana prof. Gianclaudio De Cesare, Camera dei Deputati - Servizio Informazione Parlamentare e Relazioni Esterne 16, kwiecień 1991). Prot. 9104160014/IRE.
[21] Cyt. za: „Informatyka" 1990, nr 8, s. 30.