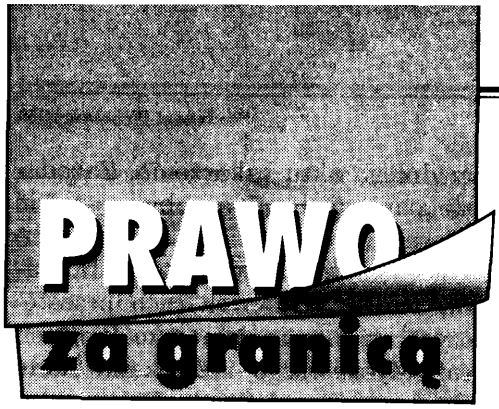
Marek T. Kolecki

Przestępstwa komputerowe w USA - w ujęciu prawa stanowego : (cz. 1)

Palestra 37/3-4(423-424), 52-58

1993



MAREK T. KOLECKI

Przestępstwa komputerowe w USA - w ujęciu prawa stanowego (cz. 1)

O przestępstwach komputerowych w ustawodawstwie amerykańskim można mówić na podstawie przepisów prawa federalnego jak i stanowego. W moim poprzednim artykule[1] omawiałem wybrane przepisy niektórych ustaw federalnych, które dotyczyły tylko i wyłącznie tzw. „komputerów federalnych", a które nie obejmowały swoją ochroną ogromnej ilości sprzętu komputerowego znajdującego się w powszechnym użyciu. To federalne ujęcie, w głównej mierze uzupełniają przepisy prawne dotyczące przestępczości komputerowej, a zawarte w kodeksach karnych poszczególnych stanów, których to interesujące fragmenty chciałbym w tym artykule zaprezentować. Można od razu w tym miejscu zapytać: czy rzeczywiście przepisy stanowe mają tak istotne dla tego tematu znaczenie? Oczywiście tak i spróbuję to zagadnienie choć częściowo przybliżyć.

W USA ponad 90% wszystkich spraw wnoszonych przed amerykańskie sądy toczy się przed sądami stanowymi, toteż jasno z tego wynika, że to właśnie przepisy stanowe są tą główną podstawą prawną dla zdecydowanej większości wydawanych orzeczeń. Dlatego też chciałbym podkreślić ich podstawową rolę jaką odgrywają we współtworzeniu systemu prawa amerykańskiego. Z czego to wynika?

Otóż Stany Zjednoczone jako państwo są przez nas postrzegane jako pewna całość – duże światowe mocarstwo, głównie poprzez pryzmat działalności zewnętrznej jego federalnych organów. I rzeczywiście, z punktu wi-

dzenia zapisu znajdującego się w Konstytucji USA mamy do czynienia z Unią, ale należy pamiętać, iż jest to Unia, w której suwerenność każdego tworzącego ją stanu wraz z jego własnymi prawami jest bardzo jasno wyartykułowana[2]. „Każdy stan zachowuje swoją suwerenność, wolność i niepodległość wraz z wszelką władzą sądowniczą i prawami, które nie zostały przez Konfederację przekazane Stanom Zjednoczonym"[3].

Jest to zapis o doniosłym znaczeniu ponieważ wynika z niego, że o ile stany mogą uczynić wszystko to, co im wyraźnie nie zakazano[4], to Unia musi się liczyć z zakazami i katalogiem kompetencji jej delegowanych. Można więc powiedzieć, że jest to pewien stały punkt odniesienia w stosunku do tych wszystkich elementów różniących poszczególne stany, zarówno w zakresie stanowienia prawa przez stanowe ciała ustawodawcze, w organizacji sądownictwa, jak też w orzecznictwie. Odmienność stanowych rozwiązań prawnych musiała przecież z czegoś wynikać i mieć gdzieś swoje korzenie, dlatego też pozwoliłem sobie zaakcentować ten niewątpliwie istotny wątek już na samym wstępie tego artykułu.

Obecnie 49 stanów[5] w USA posiada w swych stanowych kodeksach karnych przepisy dotyczące przestępstw lub nadużyć komputerowych.

Podobnie jak w ujęciu federalnym większość stanowych ciał ustawodawczych – legislatur, dążąc do ujednolicenia przepisów prawa karnego we wszystkich stanach oraz kierując się zasadą *nullum crimen sine lege*, przyjęła dla opracowanych przez siebie stanowych kodeksów karnych podział przestępstw na: zbrodnie (*felonies*), występki (*misdemeanors*) i drobne występki (*petty misdemeanors*). Całkiem odrębną grupę stanowią wykroczenia (*violations*), których ustawodawca amerykański do przestępstw nie zalicza.

Pierwszymi stanowymi przepisami stanowionymi dotyczącymi przestępczości komputerowej były przepisy stanu Floryda, które weszły w życie z dniem 1 sierpnia 1978 r. W ślad za tym rozwiązaniem, dwa miesiące później podobne przepisy zostały wprowadzone w stanie Arkansas. Większość z tych przepisów była opracowywana przez stanowe legislatury na długo przed pojawieniem się coraz to bardziej powszechnych zagrożeń, jakimi są współczesne destruktywne programy komputerowe. Bardzo ogólnie rzecz ujmując, przełomowymi latami, w których powstała większość stanowych przepisów był koniec lat 80-tych, kiedy to *casus* „virusa Cornell" i wiele innych jemu podobnych przypadków, spowodowało podjęcie bardziej energicznych prac przez stanowe legislatury nad całym zagadnieniem przestępczości komputerowej. Jako jedne z ostatnich przyjęły rozwiązania prawne dotyczące przestępczości komputerowej stany West Virginia w roku 1989 i Maine w 1990.

Porównując między sobą przepisy stanowych kodeksów karnych dotyczące tego tematu, można łatwo nawet na pierwszy rzut oka zauważyć, że różnią się one nie tylko ilością zamieszczonych artykułów, treścią jaką w sobie niosą nawet te same pojęcia, ale i również zakresem dyspozycji jak i wielkością sankcji, które są przewidziane za ten sam czyn przestępny. Typowym przykładem ujęcia tego zagadnienia przez stanowe legislatury są przepisy *Texas Penal Code*.

Jego rozdział 33 zatytułowany „Przestępstwa komputerowe" [6] rozpoczyna się jak większość analogicznych

przepisów w stanowych k.k. od wyjaśnienia użytych w tym rozdziale pojęć. Definiowane są między innymi takie pojęcia jak: „komputer", „system bezpieczeństwa komputerowego", „dane", „program komputerowy", „szkoda". I tak np.: „wirus komputerowy" [7] oznacza niepożądany program komputerowy, czy też inny zestaw instrukcji wprowadzony do pamięci komputera, systemu operacyjnego, lub też do programu, którego celowa konstrukcja umożliwia samopowtarzalność i wpływ na inne programy lub pliki komputera, poprzez dołączenie kopii niepożądanego programu lub innego zestawu instrukcji, do plików lub programów komputerowych.

Definicję „wirusa komputerowego"

można spotkać również w przepisach stanu Maine.[8] Odmienne pojęcia, choć bardzo zbliżone w swej treści zawierają przepisy kodeksów karnych innych stanów np.: Minnesota – „destruktywny program." [9] Kalifornia – „środek zanieczyszczający komputer," [10] Illinois – „manipulowanie komputerem."[11]

W nawiązaniu do przepisów k.k. stanu Texas, chciałbym przedstawić teraz zdarzenie, które ma już swoje stałe miejsce w literaturze przedmiotu.[13] 21 IX 1985 r. jeden z pracowników firmy maklersko-ubezpieczeniowej po uruchomieniu jednego z terminali zauważył, że cały system danych wykazuje pewne nieprawidłowości. Jedynym, a zarazem wiele dającym do myślenia śladem było zarejestrowane „wejście" do komputera przez nieznanego użytkownika, o godz 3 nad ranem, w czasie kiedy nikt z personelu zatrudnionego w firmie nie mógł uruchomić systemu. Rekonstruując przebieg tego zdarzenia podczas postępowania sądowego, sprawdzono całą skomputeryzowaną księgowość, w tym szczególnie wpływające do firmy dokumenty pod kątem niszczącej instrukcji możliwej do wprowadzenia. „Mass media" relacjonując to zdarzenie informowały o wprowadzeniu do programu wirusa komputerowego. Zgodnie z oceną fachowców, wirus ten należał do grupy tzw. wirusów polimorficznych czyli takich, które zawierają w sobie fragment kodu pozwalający na ich późniejszą mutację i pojawianie się za każdym razem w innej formie. Dalsze szczegółowe badania przyczyniły się do wykrycia autora tego wirusa, którym okazał się Donald Gene Burleson. Jak ustalono podczas przewodu sądowego motywem jego działania była zemsta. Oskarżonemu udowodniono szkodliwe oddziaływanie na komputer i zakwalifikowano jego czyn jako przestępstwo trzeciego stopnia, za które według przepisów k.k. stanu Texas przewidziana jest sankcja w postaci kary pozbawienia wolności do lat 10 oraz grzywny w wysokości do 5000 USD.

Orzeczeniem sądu Donald G. Burleson został skazany na karę 7 lat więzienia w zawieszeniu i 2500 USD grzywny. Ponadto został zobowiązany do zapłacenia firmie odszkodowania za poniesione straty w wysokości 11 800 USD.

Kryterium decydującym o zakwalifikowaniu danego czynu jako przestępstwo

drugiego lub trzeciego stopnia, lub jako występku jest wartość szkody spowodowanej określonym czynem przestępnym.

I tak według postanowień §33.03(b) *Texas Penal Code*:

– z przestępstwem drugiego stopnia mamy do czynienia wtedy, gdy wartość strat spowodowanych czynem przestępnym wynosi 20 000 USD i powyżej,

– z przestępstwem trzeciego stopnia, jeżeli wartość szkody wynosi 750 USD i powyżej, nie przekraczając jednak kwoty 20 000 USD,

– szkoda nie mniejsza niż 200 USD, a nie przekraczająca wartości 750 USD traktowana jest jako występek kategorii A.

Innym bardzo interesującym w swej treści zapisem jest punkt 5 §33.03 (a). Otóż w świetle tego przepisu przestępstwem jest również:

„dokonywane za pomocą komputera: usunięcie, zmiana lub kopiowanie zbywalnych papierów wartościowych"

W czasie kiedy w samej technice druku zrobiono ogromny postęp, a komputery i drukarki laserowe stały się już sprzętem powszechnie wykorzystywanym, wprowadzenie tego przepisu wydaje się być w pełni uzasadnione.

Należy przy tym wspomnieć o nowej propozycji nowelizacji przepisów *Texas Penal Code*, która przewiduje między innymi wprowadzenie konfiskaty sprzętu komputerowego użytego do przestępstwa, jak i szereg innych ciekawych rozwiązań.

Pomimo iż mamy do czynienia zarówno z federalnymi jak i stanowymi przepisami prawa, które obejmują swym kodeksowym zakresem większość czynów przestępnych to nie można wykluczyć i takich sytuacji, kiedy to orzeczenia sądowe będą mogły zapadać nie na podstawie przepisów ustawy, lecz w oparciu o stanowe „common law".[13]

Zdarzają się w praktyce i takie sytuacje, kiedy ten sam czyn przestępny może być uznany za przestępstwo zarówno na podstawie przepisów stanowych jak i federalnych. W takim przypadku o właściwości sądu decyduje przeważnie to, który z sądów: stanowy czy federalny, jako pierwszy rozpoczął postępowanie.

Jedną z poważnych trudności na jakie napotyka prawie każdy stanowy ustawodawca zajmujący się przestępczością komputerową jest problem określenia zakresu użytych w przepisach pojęć, jak i praktycznego ich zastosowania podczas postępowania sądowego. W literaturze amerykańskiej często podnoszony jest ten właśnie problem, którego wymownym przykładem jest bardzo szerokie, a przy tym nieostre pojęcie „mienia".

Kilka stanów dokonało tylko nowelizacji swoich przepisów włączając w zakres tego pojęcia jedynie informację znajdującą się na dyskach.

Zgromadzenie Ustawodawcze stanu Montana – (*Legisaltive assembly*) określa to pojęcie znacznie szerzej, włączając do niego „... elektroniczne impulsy, oprogramowanie komputera, elektroniczne przetwarzanie informacji ..."

Podobne ujęcie prezentuje legislatura stanu Massachusetts (*General Court*) określające „mienie" między innymi jako „... elektroniczne przetwarzanie lub przechowywanie danych ..."

Pomimo iż legislatury wielu stanów definiując mienie włącza do tego pojęcia szeroko rozumiany obieg komputerowej informacji, to jednak nie prowadzi to do zasadniczego rozwiązania problemu, jaki mają sędziowie przy orzekaniu w sprawach karnych o sabotaż, szpiegostwo czy też kradzież komputerową.

Szczególnie trudno jest określić pewne właściwości samej informacji znajdującej się w obiegu różnego rodzaju komputerowych połączeń. A przecież postać tej informacji na różnych etapach jej przekazu może być całkiem inna. Współcześnie wykorzystywane środki techniczne, w tym również nowoczesne technologie komputerowe stwarzają w tym zakresie bardzo duże możliwości. Ze względu

na to jakiego nośnika użyjemy do przesyłania informacji będzie ona mogła mieć postać: sygnałów elektrycznych, dźwięku (w tym również głosu ludzkiego), obrazu telewizyjnego, fali radiowej, tekstu, grafiki, zdjęcia, różnego rodzaju wydruku, wiązki światła lasera, pola elektromagnetycznego i ... światła w postaci elementarnej cząstki jaką jest foton.

Z tym ostatnim z wymienionych nośników wiąże się interesujące zagadnienie tzw. kryptografii kwantowej, której skromną namiastkę przedstawię w drugiej części tego artykułu poświęconej tematowi bezpieczeństwa obiegu komputerowej informacji.

Wracając jednak do zasadniczego tematu, to z prawnego punktu widzenia powstaje od razu pytanie,

czy wszystkie postacie pod jakimi może być przekazywana informacja można traktować jako mienie, czy też nie?

A jeżeli nie wszystkie to według doboru jakich kryteriów dokonać ewentualnego podziału? Jak bowiem potraktować np.: fakt rejestracji zmian w natężeniu pola elektromagnetycznego, wytwarzanego przez pracujący osprzęt – w celu późniejszego ich przetworzenia i w efekcie rozszyfrowania przekazywanej informacji? Czy może jako komputerową kradzież rzeczy ruchomej? Tu nasuwa się bardzo wiele wątpliwości wynikających choćby z pytania o to, co zaliczymy w zakres pojęcia „mienie" i bynajmniej nie są to jedyne kwestie wymagające głębszej naukowej analizy i być może nowych rozwiązań prawnych w przyszłości.

Równie ważne zagadnienie dotyczy sytuacji, w której miejsce popełnienia czynu przestępnego, jest inne niż miejsce lub miejsca wystąpienia skutku, co pociąga za sobą określone konsekwencje natury prawnej. Stwierdzenie miejsca i czasu może mieć istotne znaczenie zarówno dla kwalifikacji samego czynu, jak i z punktu widzenia właściwości miejscowej sądu. Poza tym istotne jest to, czy np. w pracy legislacyjnej nad przepisami ustawy akcentować bardziej skutek czy też działanie, co przecież nie jest bez znaczenia, zwłaszcza, że bardzo trudno jest przewidzieć ewentualne skutki, które mogą w stopniu nieporównywalnie większym wykraczać poza rzeczywisty zamiar sprawcy. Tak więc problemy tkwią nie tylko w konieczności dokładnego określenia czynu przestępnego w przepisach ustawy, ale wynikają również z pewnego specyficznego charakteru przestępstw komputerowych, o którym to już wcześniej wspomniałem.

General Court (Massachusetts), z całą należną dla tego zagadnienia powagą, potraktował problem przestępczości komputerowej przygotowując na początku 1989 r. cztery ustawy obejmujące między innymi: kradzież (*theft*), drobną kradzież (*larceny*), wirusy komputerowe[14] oraz uzyskanie nieuprawnionego dostępu do komputera.

I tak np. dla czynów przestępnych polegających na celowym uzyskaniu nieuprawnionego dostępu do komputera, ustawodawca przewiduje sankcje w postaci: kary pozbawienia wolności do 1 roku i grzywny w wysokości do 500 USD.

Dla drobnych kradzieży komputerowych (*larceny*), w wyniku których w ograniczonym stopniu nastąpiła zmiana danych, przewidziana jest sankcja w postaci: kary pozbawienia wolności do 1 roku i grzywny w wysokości do 750 USD.

W sytuacji gdy dane komputerowe zostaną całkowicie zmienione, sankcja ulega bardzo poważnemu zaostrzeniu. W tym wypadku sąd może orzekać ka-

rę pozbawienia wolności do lat 10 i nakładać grzywnę w maksymalnej wysokości do 25 000 USD.

General Court (Massachusetts) bierze również pod uwagę wprowadzenie w życie ustawy, która określałaby zasady odpowiedzialności karnej dla osób które „kradną czas pracy komputera" w miejscu swojego zatrudnienia, lub wykorzystują programy komputerowe dla innych niż określone w danej pracy celów. Wynika to z tego, że czas pracy komputera, wraz z jego specjalistycznym oprogramowaniem jest drogi, a wykorzystanie go do innych celów może przynosić właścicielowi straty. Kradzież czasu pracy komputera o równowartości większej niż 100 USD, przy założeniu że nie powstała przy tym żadna dodatkowa szkoda byłaby już podstawą do wszczęcia postępowania karnego wobec sprawcy.

Podobne uregulowania są zawarte w przepisach k.k. stanu Arizona, które dodatkowo jeszcze penalizują użycie lub zmianę programów komputerowych podjęte między innymi w celu defraudacji lub wprowadzenia w błąd.

Typowymi dla tej grupy stanowych legislatur, które szczególnie akcentują w tworzonych przez siebie przepisach celowe bezprawne użycie komputera są przepisy stanu Nevada.

Nowo wprowadzane do kodeksów stanowych przepisy obniżają dotychczasowe konieczne ustawowe wymogi i upoważniają odpowiednie organa do wszczynania postępowania sądowego już w przypadku narażenia na szkody lub uszkodzenia. Ma to niewątpliwie duże znaczenie dla podnoszenia efektów skutecznego zwalczania i zapobiegania przestępczości komputerowej już w jej najmniej szkodliwym stadium.

Stany Zjednoczone to największy na świecie rynek producentów jak i użytkowników najnowocześniejszych technologii komputerowych, skupiający zarazem ogromny potencjał naukowo-badawczy. Z tego chociażby względu warto się bliżej zainteresować zarówno tym co produkują, jak i tym jakie z tego technologicznego pierwszeństwa wynikają problemy natury prawnej oraz w jaki sposób można je rozwiązywać.

Komputerowe systemy sieciowe i wielodostępne rozrastają się do skali globalnej, posługując się przy tym coraz częściej technikami telekomunikacyjnymi. Z drugiej strony, telekomunikacja nie może się obejść bez powszechnego użycia technik cyfrowych. Przyszłość, to konieczność budowy takich sieci telekomunikacyjnych których wszystkie nośniki i elementy będą podporządkowane zintegrowanym systemom komputerowym.

Jako że stały postęp cywilizacji niesie za sobą również nowe zagrożenia, a przestępczość komputerowa z pewnością należy do jednego z nich, toteż dużą rolę ze względu na swoją funkcję i zakres oddziaływania mogą tu odegrać nauki penalne.

Przypisy:

[1] „Palestra" nr 5/6 1992 r.

[2] Artykuł II Konstytucji USA.

[3] W literaturze przedmiotu można spotkać różne poglądy na temat federalizmu amerykańskiego, a oto jeden z nich:
„Suwerenność Unii jest abstrakcją i istnieje realnie jedynie w odniesieniu do niewielu problemów polityki zagranicznej. Suwerenność stanowa jest namacalna, łatwo zrozumiała, zawsze widoczna. Pierwsza jest czymś nowym, druga powstała razem z narodem."
(A. de Tocqueville, O demokracji w Ameryce, ze wstępem J. Baszkiewicza, Warszawa 1976, s.129).

[4] W USA istnieją odrębne stanowe: konstytucje, kodeksy karne i cywilne oraz kodeksy obu procedur. Stanowe jest również prawo: administracyjne, ubezpieczeń, rolne, ochrony środowiska oraz podatki, cła i inne opłaty. Z przyczyn oczywistych wymieniłem tylko ich część.
Por. J. Jaskiernia: Pozycja stanów w systemie federalnym USA, Warszawa 1979 r.

[5] Oprócz stanu Vermont.

[6] *Act of Sept.* 1, 1989.

[7] *Texas Penal Code* §33.01 (9).

[8] Maine - *MRSA* §431 (9).

[9] *Act of May* 17, 1989, *Minnesota Stat. Ann.* §609.87 Subd. 12.

[10] *California Penal Code* §502 (b) (10).

[11] *Ill. Rev. Stat. Ch.* 38 §16 D-3 (4).

[12] *State of Texas v. Burleson No. 0274120 R. Tarrant Country Criminal Court, 1988.*

[13] Zgodnie z orzeczeniem S.N. USA (304 U.S. 64) od 1933 r. nie istnieje tzw. „general commmon law" czyli prawo precedensowe o zasięgu federalnym. Jest tylko „common law" stanowe. Oznacza to, że sądy federalne zobowiązane są do stosowania jedynie prawa precedensowego istniejącego w danym stanie lub grupie stanów, gdy sprawa dotyczy właściwości rzeczowej lub miejscowej szerszej niż zakres jurysdykcyjny jednego stanu. Zob. T. Langer Stany w USA, PWN 1988.

[14] *Massachusetts Senate Bill*, 1701, 176-th Leg., 1-st Sess. (1989).