Marek T. Kolecki

Przestępstwa komputerowe w USA w ujęciu prawa stanowego : (cz. 2)

Palestra 37/9-10(429-430), 98-106

1993

PRAWO za granicą

Marek T. Kolecki

Przestępstwa komputerowe w USA w ujęciu prawa stanowego (cz. 2)

Przedmiotem tej części opracowania jest ochrona obiegu komputerowej informacji. Zanim jednak przejdę do omówienia wybranych elementów tego zagadnienia, chciałbym tytułem wprowadzenia poruszyć kilka nie mniej istotnych a jednocześnie ściśle związanych z całością tego zagadnienia kwestii.

Otóż bezpieczeństwo obiegu komputerowej informacji jest bezsprzecznie zagadnieniem niezwykle trudnym i złożonym. Jego szeroki interdyscyplinarny zakres przedmiotowy, obejmujący przede wszystkim wiele nowych wąsko wyspecjalizowanych dziedzin nauki powoduje, iż w toku prowadzonych nad tym tematem badań często spotykamy się z problemami, które na pozór nie zawsze wydają się mieć istotny związek z naukami penalnymi. Mam tu na myśli między innymi pewien szerszy socjologiczny aspekt tego zagadnienia, a mianowicie potrzebę tworzenia nowych zasad kultury informacyjnej i informatycznej.

Nie umniejszając w niczym ogromnej roli, jaką spełniają zabezpieczenia techniczne, trzeba zwrócić uwagę, że zawsze jednak decydujące znaczenie dla ochrony systemu będzie miał jego użytkownik – człowiek, a zwłaszcza ukształtowanie jego świadomości co do wagi i znaczenia informacji, jaką się posługuje.

Z dnia na dzień coraz wyraźniej odczuwamy ogromny wpływ informatyki na rozwój bez mała wszystkich dziedzin światowej gospodarki. Z tego też względu można już dziś z całą odpowiedzialnością powiedzieć, że jesteśmy świadkami narodzin nowej ery, ery informatyzacji, która stwarza coraz większe możliwości potencjalnego zagrożenia przestępczością komputerową. W związku z tym, problem ochrony obiegu komputerowej informacji stanie się w niedalekiej przyszłości problemem numer jeden społeczeństwa żyjącego na przełomie wieków, stwarzając tym samym również realne zagrożenia w zakresie obronności i bezpieczeństwa państwa. Brak należytej oceny tego problemu, lub co gorsza lekceważenie

go, jest poważnym błędem, o nie dających się przewidzieć w przyszłości skutkach.

Swoje być może zbyt daleko idące w tym zakresie wnioski, opieram, jak mi się wydaje, na słusznym założeniu, że w przypadku, gdy podstawowym elementem przyszłej infrastruktury będą sieci komputerowe wspomagane telekomunikacyjnymi technikami przesyłania informacji, nastąpi niewątpliwy wzrost zagrożenia przestępczością komputerową. Miałoby to miejsce również w odniesieniu do tej najpoważniejszej grupy przestępstw, jakimi są przestępstwa przeciwko państwu.

Kwestie takiej czy innej oceny danego zjawiska mogą być zawsze przedmiotem licznych kontrowersji, czy też bardziej lub mniej zasadnej krytyki. Ale nie o to bynajmniej mi chodzi.

Uważam natomiast, że jest rzeczą wielce pożądaną, aby one były i wynikały z rzeczywistej woli rozwiązywania problemów, których, jak sądzę, ominąć się nie da.

O ile przestępczość komputerowa, jako używany obecnie termin dla określenia tego zjawiska, jest terminem stosunkowo nowym w ustawodawstwie amerykańskim, o tyle same działania przestępne dotyczące komputera, jak i jego oprogramowania, znane są już od bardzo dawna. Przez ostatnie kilkanaście lat w USA w ślad za nowoczesną technologią prowadzono przygotowawcze prace legislacyjne[1] w celu bieżącej eliminacji czynów przestępnych, wyrastających, z możliwości użycia nowych technik. Metodologia klasyfikacji czynów przestępnych stosowana przy wyodrębnianiu przestępstw komputerowych, a znajdująca swoje odzwierciedlenie w rozwiązaniach stanowych kodeksów karnych, w dużej mierze pokrywa się lub uwzględnia tak federalne, jak i po części międzynarodowe standardy w tym zakresie.

...decydujące znaczenie dla ochrony systemu będzie miał jego użytkownik – człowiek, a zwłaszcza ukształtowanie jego świadomości co do wagi i znaczenia informacji jaką się posługuje...

W § 502 *California Penal Code* stanowy ustawodawca wyjaśnia, iż intencją stanowienia niniejszego paragrafu jest rozszerzenie zakresu ochrony udzielanej osobom fizycznym, przedsiębiorstwom i instytucjom państwowym przed manipulowaniem, ingerencją, uszkodzeniem i innymi nieuprawnionymi formami dostępu do komputerów, systemów komputerowych oraz danych komputerowych (które oznaczają informację, wiedzę, fakty, koncepcje, oprogramowanie komputerowe bez względu na rodzaj użytego nośnika czy też pamięci).

Jednym z ważnych elementów, mającym na celu zapewnienie bezpieczeństwa obiegu komputerowej informacji, jest prawna ochrona tzw. dokumentacji wspierającej. Ustawodawca stanu Kalifornia definiuje ją jako:

...wszelką informację w jakiejkolwiek formie, która dotyczy projektu, konstrukcji, klasyfikacji, realizacji, użytkowania czy też modyfikowania komputera, systemu komputerowego, sieci komputerowej, programu lub oprogramowania komputerowego[2]...

Równie istotnym dla całości tego zagadnienia jest także nowo wprowadzone do przepisów kodeksu karnego stanu Teksas pojęcie „systemu bezpieczeństwa komputerowego"[3]. Oznacza ono: projekt, konstrukcję, procedurę lub inne środki stosowane przez osobę odpowiedzialną za działanie i użytkowanie komputera w celu ograniczenia jego użytkowania jedynie dla ściśle określonych podmiotów lub celów[4]. Wymownym tego przykładem jest § 33.03./a/3/A/ *Texas Penal Code*, w którym jako działanie przestępne traktuje się wykorzystanie komputera do: „...manipulowania, dokonywania zmian w oficjalnych rejestrach i aktach rządowych, medycznych lub oświatowych..."

Jak już wcześniej wspomniałem, biorąc pod uwagę interdyscyplinarny charakter tego opracowania, wydaje mi się w pełni zasadne wyodrębnienie i zaprezentowanie choćby w skromnym zakresie problemu ochrony informacji, również od strony technicznej, która jest bardzo ważną częścią składową tego zagadnienia. Jest to zasadne choćby z tego względu, że obecnie coraz częściej sama wiedza prawnicza jest już niewystarczająca, nie daje bowiem możliwości przyjęcia prawidłowej optyki dla tak złożonych problemów, nie mówiąc już o współudziale w ich rozwiązywaniu, czy też wnoszeniu racjonalnych propozycji uregulowań prawnych.

Mówiąc o komputerowym obiegu informacji, o jej przesyłaniu i mając na myśli informację w ogóle, bierzemy głównie pod uwagę jej najważniejsze atrybuty, którymi są: szybkość, dokładność, wiarygodność i w określonych sytuacjach bezwzględne bezpieczeństwo. Niczym stają się walory pierwszych trzech, gdy tajna lub poufna informacja nie jest adekwatnie do swej wagi zabezpieczona. Stąd też wymóg zapewnienia odpowiedniej tak technicznej, jak i prawnej ochrony nabiera w wielu przypadkach decydującego znaczenia.

Ze względu na tajność i poufność przetwarzanych, jak i przekazywanych informacji za pomocą komputerów, sieci komputerowych oraz innych specjalistycznych urządzeń telekomunikacyjnych, muszą istnieć takie mechanizmy, które nie pozwalałyby na swobodny dostęp do danych osobom do tego nie upoważnionym. Problemem tym zajmuje się kryptografia, czyli ta gałąź wiedzy w ramach informatyki, która przy wykorzystaniu odpowiednich urządzeń lub programów pozwala odpowiednio szyfrować przechowywane i przesyłane wiadomości w postaci tzw. kryptogramów.

Nowe, nie znane dotąd możliwości w tej dziedzinie otwiera tak zwana kryptografia kwantowa[5], wykorzystująca jako nośnik informacji światło w postaci jego elementarnych cząstek[6] – fotonów[7]. Jeszcze do niedawna wydawałoby się, że jest to przedsięwzięcie całkiem nierealne, mogące zaistnieć tylko na gruncie teoretycznych rozważań.

A jednak przy wykorzystaniu korelacji kwantowej istnieje możliwość opracowania takiego kryptosystemu[8], który jest w stanie zagwarantować dwa najbardziej istotne dla tajnego lub poufnego przekazu informacji elementy. Chodzi tu zarówno o konieczność zapewnienia całkowitego bezpieczeństwa dystrybucji, jak i przechowywania klucza[9]. Zastosowanie właściwości fizycznych światła[10] pozwala na równoczesne uzyskanie olbrzymiej szybkości działania oraz pokonanie wielu nieprzekraczalnych do tej pory barier. Tak znaczące osiągnięcia doprowadziły do gwałtownego rozwoju nowych dziedzin nauk komputerowych tzw. *computer since.*

W konkluzji można stwierdzić, że kryptografia kwantowa to ogromny postęp techniczny w efekcie dający przede wszystkim skuteczną ochronę, gwarantem której są prawa fizyki. Sama bowiem próba infiltracji (podsłuchu kwantowego kanału informacji) układu, powoduje zakłócenia uniemożliwiające jej przechwycenie i ujawnienie.

Zarówno wysokie koszty, jak i trudności techniczne związane z budową wysokiej klasy aparatury optyczno-elektronicznej oraz specjalnego oprogramowania mogą na dzień dzisiejszy w sposób zasadniczy ograniczać praktyczne możliwości wykorzystania kryptografii kwantowej przy przesyłaniu informacji na duże odległości. Niemniej sam fakt pojawienia się tak radykalnie odmiennych w stosunku do współcześnie stosowanych rozwiązań, przyczyni się do dalszego rozwoju tej tak bardzo ważnej dla nas wszystkich dziedziny nauki.

Rozważając temat przestępczości komputerowej oraz związanej z nią ochrony informacji pod kątem ewentualnego tworzenia przyszłych przepisów prawa karnego, można zadać sobie pytanie: Czy z punktu widzenia ustawodawcy szczegółowe zagłębianie się w techniczną analizę tego zagadnienia byłoby celowe?

...problem bezpieczeństwa obiegu komputerowej informacji stanie się w niedalekiej przyszłości problemem numer jeden społeczeństwa żyjącego na przełomie wieków, stwarzając tym samym również realne zagrożenia w zakresie obronności i bezpieczeństwa państwa...

Trudno jest już dziś jednoznacznie sobie odpowiedzieć na to pytanie. Wydaje się że obydwie opcje: zarówno na „tak", jak i ta na „nie", miałyby tyle samo zagorzałych zwolenników co i przeciwników. Nie wdając się zbytnio w szczegóły, spróbujmy zastanowić się nad możliwymi argumentami obydwu stron.

Tworząc normę prawną mamy na uwadze to, aby swoją treścią obejmowała pewne zagadnienia możliwie szeroko i na wysokim poziomie abstrakcji. W tym przypadku używając w przepisach ogólnych określeń typu „informacja", „przesyłanie informacji" lub „komputerowy obieg informacji", byłoby korzystne ze względu na bardzo szeroki zakres tych pojęć, a co się z tym

wiąże, w przypadku ich zastosowania w przepisach kodeksu karnego, dawałoby większe praktyczne możliwości ich wykorzystania.

Z drugiej jednak strony postępujący rozwój naszej cywilizacji stale rozszerza krąg dyscyplin naukowych, z którymi stykają się nauki penalne, i z tego też względu nie można chyba poprzestać na proponowaniu tylko tych ogólnych pojęć, ale należałoby je wypełnić bardziej konkretną treścią. Dlatego też kazuistyka przepisów dotyczących przestępczości komputerowej jest niezbędna, ale tylko do pewnego stopnia. Problemem współczesnego stanowego jak i federalnego ustawodawcy jest także i to, że często nie orientuje się, jaka jest rzeczywista możliwość zagrożenia, a co za tym idzie nie podejmuje odpowiednich działań mogących mieć wpływ choćby na ograniczenie dalszego rozwoju tych niekorzystnych zjawisk. W sytuacji, gdy skala zagrożeń spowodowana danym zjawiskiem zbyt szybko rośnie, tworzenie odpowiednich zabezpieczeń prawnych jest nieuniknioną koniecznością. I wcale nie chodzi o to, by tworzyć zbędne przepisy, gdy mamy do czynienia z nieprzystającą do nich rzeczywistością. Chodzi natomiast o to, aby mieć na tyle zaawansowane stadium ich tworzenia, żeby bez zbędnej straty czasu w każdej chwili móc je uzupełnić i wprowadzić w życie.

Ochrona komputerowego obiegu informacji związana jest również z działaniami zmierzającymi do ograniczenia bądź całkowitej eliminacji takich zagrożeń, jak szpiegostwo gospodarcze związane z kradzieżą wysokiej klasy technologii, w tym technologii komputerowych, wyników badań naukowych, danych medycznych oraz innych ważnych danych dotyczących sfery gospodarki czy życia politycznego.

Należałoby podkreślić, że większość z tych czynów przestępnych dokonywana jest z wykorzystaniem najnowszych zdobyczy techniki komputerowej[11], przynosząc gospodarkom państw ogromne straty[12].

Dla określenia całokształtu przestępczej działalności w komputerowych systemach informatycznych, najbardziej właściwym terminem wydaje się być „infiltracja", którą można określić jako: działanie osób nieupoważnionych, mające na celu przenikanie do zastrzeżonych informacji przy wykorzystaniu różnego rodzaju środków technicznych.

Całość działań infiltracyjnych ze względu na ich złożony charakter można podzielić na przypadkowe i celowe.

Infiltracja przypadkowa polega na tym, że osoby nieupoważnione nie muszą podejmować specjalnego działania, aby uzyskać zastrzeżone informacje. Dostają się one bowiem w „niepowołane ręce" w sposób przypadkowy bądź na skutek błędnego działania systemu, zaniedbań personelu, bądź też są wynikiem innych działań".

W ramach ww. podziału, pośród działań infiltracyjnych celowych można dodatkowo wyróżnić:

– infiltrację celową pasywną, która polega na takim działaniu osób nieupoważnionych, które zmierza do przechwycenia, odczytu zastrzeżonych informacji nie podnosząc przy tym ujem-

nych skutków w dalszym ich obiegu, jak i przetwarzaniu.

– infiltrację celową aktywną, polegającą na działaniu osób nieupoważnionych, które zmierza do uzyskania zastrzeżonych informacji przy jednoczesnym negatywnym oddziaływaniu na nie.

Biorąc pod uwagę możliwość różnorodnych działań przestępnych, zarówno komputer wraz z całym osprzętem współpracującym, jak i jego oprogramowanie może być tu traktowane zarówno jako:

– przedmiot czynności wykonawczej,

– narzędzie służące do dokonania przestępstwa,

– lub łącznie, jako jedno i drugie.

Amerykanie przypuszczają, iż ich rynek podlega stałej infiltracji przez różnego rodzaju służby specjalne z ponad dwudziestu krajów i nie byłoby w tym nic dziwnego, gdyby nie fakt, że bardzo aktywnymi w tym procederze są tradycyjni sojusznicy Stanów Zjednoczonych[13].

Dlatego też obok wielu już funkcjonujących od jakiegoś czasu instytucji powołanych do ochrony informacji, takich jak: Computer System Security and Privacy Advisory Board, National Telecommunications and Information System Security Committee (NTISSC), National Security Agency (NSA), Federal Information Processing Standards (FIPS), ze względu na rosnące zagrożenia powołuje się kolejne. 7 stycznia 1993 roku ówczesny prezydent USA George Bush powołał do życia Information Security Oversight Office (ISOO), której celem jest ochrona i administrowanie poufnymi informacjami z dziedziny technologii i gospodarki.

Na szczeblu rozwiązań federalnych w tym zakresie spotykamy się z ustawą, która zasługuje na szczególną uwagę. Jest nią ustawa *Computer Security Act of 1989*, zakreślająca podstawowe ustawowe ramy działania dla wymienionych wyżej instytucji.

> ...ustawodawca często nie orientuje się, jak rzeczywista jest możliwość zagrożenia, a co za tym idzie, nie podejmuje odpowiednich działań mogących mieć wpływ choćby na ograniczenie dalszego rozwoju tych niekorzystnych zjawisk...

Współczesna wiedza o gospodarce jest nie mniej istotna niż informacje o charakterze militarnym czy politycznym. Stąd też głównym teatrem działań infiltracyjnych jest teraz właśnie szeroko rozumiana gospodarka państwa, a zwłaszcza jej system finansowy, potencjał wytwórczy, kadra, środowiska naukowe.

Jedną z wyspecjalizowanych dyscyplin wywiadu stał się tak zwany wywiad komputerowy. Stymulując i usprawniając pracę służb odpowiedzialnych za pozyskiwanie i ochronę informacji (np.: wywiad naukowo-techniczny, wywiad kosmiczny lub kontrwywiad), nabiera coraz większego, żeby nie powiedzieć decydującego znaczenia dla ich prawidłowego funkcjonowania. Stano-

wiąca naturalną wspólną płaszczyznę dla pozostałych dyscyplin technika komputerowa stała się obecnie nieodłącznym elementem w pozyskiwaniu, analizie i ochronie informacji.

W literaturze przedmiotu można się spotkać ze stwierdzeniem, że wywiad komputerowy jest jedną ze współczesnych odmian szpiegostwa gospodarczego. Czy aby tylko? Można przypuszczać, iż takie ujęcie w sposób istotny dla tego tematu zawężałoby wszechstronny zakres i możliwości wykorzystania technik komputerowych.

W rzeczy samej będące w potocznym użyciu pojęcie „szpiegostwo gospodarcze" ma raczej zabarwienie pejoratywne i jak sądzę niezbyt właściwie oddające istotę jego instytucjonalnych form oraz samych działań wywiadowczych, bez których w mniejszym lub większym stopniu nie jest w stanie obejść się żadne państwo. Co więcej, jest wiele przykładów na to, iż pozyskiwane tą właśnie drogą informacje stanowią poważny wkład w rozwój własnej nauki, a tym samym mają niewątpliwie znaczący wpływ na gospodarkę. Z tego też względu szpiegostwo komputerowe i technologiczne stawiane jest dziś na jednym z czołowych miejsc na liście zagrożeń gospodarki amerykańskiej.

Reasumując można stwierdzić, że naukowe kreatywne podejście zarówno do problemu zdobywania, jak i ochrony informacji, ma więc nie tylko bezpośredni wpływ na zwiększenie stopnia bezpieczeństwa państwa, ale winno być postrzegane w odpowiednio szerszym wymiarze.

Wieloaspektowość tego zagadnienia powoduje, że już dzisiaj musimy myśleć o konieczności powołania warsztatów interdyscyplinarnych, których celem byłoby koordynowanie dotychczasowych i wytyczanie nowych kierunków badań i analiz. Dla teoretyków prawa karnego szczególnie interesujące mogłyby być rozważania dotyczące pojęć, funkcji i mechanizmu kwalifikacji prawnej czynu przestępnego. Nie bez znaczenia byłoby przeprowadzenie badań empirycznych mających na celu ustalenie stanu i struktury przestępczości komputerowej oraz zebranie informacji na temat jej przyczyn, form zjawiskowych czy też danych o potencjalnym sprawcy.

Bardzo istotnym, a co najważniejsze prostym i skutecznym, sposobem ochrony informacji znajdującej się w całym jej komputerowym obiegu jest... dezinformacja. Może ona spełniać zarazem wiele różnorodnych funkcji, między innymi takich, jak wykrywanie i przeciwdziałanie potencjalnym zagrożeniom, zwłaszcza że na pewnym szczeblu utajniania informacji równoległe prowadzenie działań dezinformacyjnych wydaje się być niezbędne.

W świetle powyższego zapisu rodzi się pytanie: W jaki sposób poprzez działania dezinformacyjne chronić własne zasoby? Najogólniej rzecz ujmując, należałoby poprzez treść „udostępnianej" informacji tak inspirować podmiot infiltrujący, aby w wyniku tego podjął on takie działania własne, które po wnikliwej analizie pozwoliłyby nie tylko na identyfikację jego i jego ośrodków decyzyjnych, ale także na przyszłą

pasywną kontrolę ich poczynań lub, w zależności od potrzeb, na aktywne oddziaływanie na te ośrodki.

Takie wykorzystanie informacji wiąże się z jeszcze jedną kwestią, na którą trzeba koniecznie zwrócić uwagę. Jest to mianowicie problem nadużycia zakresu dostępu i celowości wykorzystania, zarówno danych osobowych, jak i danych medycznych przez upoważnione do ich gromadzenia instytucje i organy państwa. I co się z tym wiąże, istnieje możliwość naruszania praw człowieka. Powstaje tu również problem zdefiniowania i ustawowego określenia zakresu tajemnicy państwowej, zawodowej. Problematykę tą ujmuje w swoich przepisach federalna ustawa o wolności informacji: *Freedom of Information Act of 1966*. Mając na myśli ochronę informacji, trzeba brać pod uwagę przede wszystkim kwestie związane z ochroną zarówno samych komputerów (*hardware*), jak i równoległą ochronę oprogramowania komputerowego (*software*). Problem ochrony programów komputerowych w Stanach Zjednoczonych na podstawie prawa autorskiego ma doniosły wpływ na całokształt prawnej ochrony informacji[14].

Ze względu na ogromny zakres tematyczny oraz doniosłość autorskoprawnej ochrony programów komputerowych chciałbym zaprezentować tę problematykę w odrębnym kolejnym opracowaniu, zawierającym postanowienia konwencji berneńskiej (poświęconej ochronie dzieł literackich i artystycznych), do której w roku 1989 przystąpiły również Stany Zjednoczone.

Przypisy:

[1] *The Computer Security Act of 1987*; *Computer Virus Eradication Act of 1989*; *Computer Protection Act of 1989*; *Computer Fraud and Abuse Act of 1989*.

[2] 502 (6) *California Penal Code*.

[3] 502 (7) *California Penal Code*.

[4] 33.01 (5) *Texas Penal Code*.

[5] Jednym z prekursorów w zakresie prac nad tym interesującym zagadnieniem był Stephen J. Weisner autor opracowania pod tytułem: *Conjugate Coding* z roku 1970, które to z „niewiadomych" przyczyn przez kilkanaście lat, aż do roku 1983, nie mogło doczekać się oficjalnej publikacji.

[6] Cząstka – to pojedynczy spójny obiekt, który ma określoną indywidualność i który może być w danej chwili zlokalizowany w ograniczonym obszarze przestrzeni. Cząstki elementarne dzieli się na 4 klasy: fotony, leptony, mezony i bariony.

[7] Kwant energii elektromagnetycznej; cząstka (porcja) promieniowania elektromagnetycznego o energii i masie spoczynkowej równej zero. Pojęcie „kwant energii" wprowadził po raz pierwszy w roku 1900 Karl Max Planck, fizyk niemiecki, twórca podstaw klasycznej teorii kwantów, laureat nagrody Nobla. Wysunął hipotezę, że energia promieniowania, podobnie jak i materia, ma strukturę nieciągłą i może być przekazywana określonymi porcjami.

[8] Kryptosystem taki opiera się na opisanej przez Davida Bohma wersji słynnego efektu (EPR) Einsteina – Podolskyego – Rosena Bernard d'Espagnat w: *The Quantum Teory and Reality*.

[9] Samo kodowanie klucza odbywa się za pomocą fali świetlnej, wykorzystując zjawisko optyczne zwane generacją parametryczną.

[10] Opierając się na praktycznym zastosowaniu tzw. zasady nieoznaczoności Heisenberga, Carl Werner Heisenberg (1901–1976) w roku 1927 podał jedną z najważniejszych zasad fizyki atomowej – zasadę nieoznaczoności. Laureat nagrody Nobla za pracę z mechaniki kwantowej.

[11] Peterzell: *Spying and Sabotage by Computer* „Time", March 20 1989; John Markoff and Kate Hafner: *Cyberpunk – Outlaws and Hackers on the Computer Frontier* Simon & Schuster 1991; Harold L. Burstyn: *Computer Whiz Guilty* „ABA Journal" April 1990; Hansen L. Raymond: *The Computer Virus Eradication Act of 1989* „The War Against Computer Crime Continues" Vol. III, „Software Law Journal 1990".

[12] Według oceny CIA straty, jakie poniosła gospodarka amerykańska w wyniku działań tajnych służb innych państw, oszacowane tylko za ubiegły rok, wyniosły ponad 100 miliardów dolarów. Peter Schweizer *Frendling Spies* 1993.

[13] Francuska Direction Generale de la Securité Exterieure (DGSE), zachodnioniemiecka BND, Japończycy, Chińczycy oraz tradycyjnie już Rosjanie.

[14] Nowelizowana w latach 1989 i 1990 federalna ustawa *Copyright Act of 1976* sytuuje programy komputerowe jako tak zwane *literary works*, czyli jako dzieła literackie piśmiennicze.