Polskie Towarzystwo Informatyczne

PTI

Społeczne aspekty informatyki

Redakcja naukowa:

Piotr Fuglewicz

Jerzy S. Nowak

Społeczne aspekty informatyki

Społeczne aspekty informatyki

Redakcja naukowa:

Piotr Fuglewicz
Jerzy S. Nowak

PTI

Polskie Towarzystwo Informatyczne – Oddział Górnośląski
Katowice 2007

Recenzenci:
Dr hab. inż. Janusz K. Grabara
Prof. dr hab. Aleksander Katkow
Dr hab. Helena Kościelniak
Prof. PW, dr hab. Kazimierz Waćkowski

Wydanie publikacji dofinansowane przez Polską Wytwórnię Papierów Wartościowych SA - Warszawa

Copyright © 2007 Polskie Towarzystwo Informatyczne Oddział Górnośląski

ISBN 978-83-60810-13-2

Redakcja techniczna dr inż. Tomasz Lis, mgr inż. Jerzy S. Nowak
Projekt okładki Marek J. Piwko

Utwór w całości ani we fragmentach nie może być powielany ani rozpowszechniany za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i innych, w tym również nie może być umieszczany ani rozpowszechniany w postaci cyfrowej zarówno w Internecie, jak i w sieciach lokalnych bez pisemnej zgody posiadacza praw autorskich.

Polskie Towarzystwo Informatyczne
Oddział Górnośląski
40-074 Katowice, ul. J. Lompy 2/10
tel. (0 32 251 9811) , e-mail: Katowice@pti.org.pl
www.katowice.pti.org.pl

Fotokopie, druk i oprawę
Wykonano w Zakładzie Graficznym Politechniki Śląskiej w Gliwicach
Zam. 106/09

POLSKA
WYTWÓRNIA
PAPIERÓW
WARTOŚCIOWYCH S. A.

PWPW S.A.

**Wydawcy składają podziękowanie
Polskiej Wytwórni Papierów Wartościowych SA
za pomoc w wydaniu niniejszej publikacji**

SPIS TREŚCI

CZĘŚĆ 1 – SPOŁECZNE PROBLEMY INFORMATYKI

CZĘŚĆ 2 – ZASTOSOWANIA

CZĘŚĆ 3 – PROBLEMY BEZPIECZEŃSTWA

CZĘŚĆ 1
SPOŁECZNE PROBLEMY INFORMATYKI

ROZDZIAŁ I

PRAWNOKARNE ASPEKTY DZIAŁAŃ INFORMATYCZNYCH. CZY POLSKIE TOWARZYSTWO INFORMATYCZNE JEST „ZORGANIZOWANĄ GRUPĄ PRZESTĘPCZĄ"

Wojciech Rafał WIEWIÓROWSKI

Prawo karne a działalność informatyka

Prawo karne komputerowe nie ma zbyt wiele szczęścia w ostatnich latach w naszym kraju. Tzw. „duża cybernowelizacja" kodeksu karnego przeprowadzona w Polsce na przełomie lat 2003 i 2004 była dyskutowana niejako wspólnie z innymi „europejskimi" aspektami prawa i procedury karnej. Ustawa nowelizująca kodeks karny w zakresie przestępstw komputerowych – w tym będącego implementująca rozwiązania proponowane w nie ratyfikowanej jeszcze budapeszteńskiej konwencji o cyberprzestępczości[1] - była procesowana wspólnie z przepisami o europejskim nakazie aresztowania. To ta druga kwestia – znacznie bardziej nośna – zdominowała dyskusję w Sejmie, powodując, że zagadnienia prawa komputerowego zeszły na drugi plan i nie uzyskały wystarczającej atencji posłów. Doprowadziło to do uchwalenia (wbrew opiniom doktryny prawa karnego) rozwiązań niedopracowanych, lub po prostu błędnych. Również nowelizacja proponowana w 2007 r. nie miała szczęścia do politycznych decyzji. Polska była zobowiązana do wprowadzenia do swego prawa do kwietnia 2007 r. przepisów implementujących decyzję ramową Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[2]. Tym razem włączono propozycje nowelizacji kodeksu karnego do tzw. „dużej nowelizacji kodeksu karnego" przygotowanej przez zespół powołany przez Ministra Sprawiedliwości Zbigniewa Ziobrę. Bardzo ciekawe propozycje znalazły się jednak „w koszu" w momencie zmiany ekipy rządowej i przejęcia resortu sprawiedliwości przez prof. Zbigniewa Ćwiąkalskiego. Nowa Rada Ministrów powróci zapewne do idei wdrażanych w tym projekcie w zakresie przestępstw komputerowych. Na razie jednak polskie

---

[1] Konwencja Rady Europy o cyberprzestępczości podpisana została w Budapeszcie 23 listopada 2001 r. Przepisy Konwencji omawiają A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń TNOiK 2001, S. Bukowski, *Kodeks karny a Konwencja o cyberprzestępczości - Przed wejściem do Unii Europejskiej*, „Gazeta Sądowa", nr 3 z 2004 r., s. 55 i część druga pt. *Projekt zmian Kodeksu karnego - Dostosowanie do Konwencji o cyberprzestępczości*, „Gazeta Sądowa", nr 4 z 2004 r., s. 53 oraz P. Kruszyński , *O niektórych propozycjach rządowego projektu ustawy o zmianie ustawy - kodeks karny, ustawy - kodeks postępowania karnego oraz ustawy - kodeks wykroczeń (w redakcji z dnia 19 sierpnia 2003 r.)*, „Prokuratura i Prawo" nr 2 z 2004

[2] Decyzja ramowa 2005/222/WSiSW Dz.U. UE seria L Nr 69 , ss. 67 - 71

prawo karne klasyczne przestępstwa komputerowe reguluje w sposób zaproponowany w 2003 r.

Regulacja ta jest dla informatyków i kryptologów[3] bardzo niekorzystna. Powoduje ona, że *de facto* każdy informatyki i każdy kryptolog może zostać uznany z założenia za przestępcę. W podobny sposób każda organizacja środowiskowa informatyków czy kryptologów może zostać potraktowana jako co najmniej zorganizowana grupa przestępcza, albo nawet jako związek przestępczy na podstawie tegoż samego kodeksu karnego. Choć takie twierdzenie jest absurdalne i nikt jak dotąd nie zaczął postępowania przeciwko np. Polskiemu Towarzystwu Informatycznemu jako „związkowi przestępczemu", ale w niniejszym artykule wykażę, że polskie przepisy są w tej kwestii dość jednoznaczne. Nawet jeśli na co dzień taką sugestię traktować będziemy humorystycznie, nie należy zapominać, że problem jest bardzo poważny. To właśnie organizacja środowiskowa taka jak PTI powinna bowiem dbać o interesy swych członków m.in. poprzez sugerowanie władzom publicznym, że pozostawianie w polskim prawie karnym przepisów praktycznie martwych (choć zobaczymy za chwilę, że nie do końca „martwych"), które penalizują normalną działalność osób wykonujących te zawody jest działaniem sprzecznym z interesem społecznym. Taka sytuacja ma również – co z prawniczego punktu widzenia jest bardzo ważne – charakter demoralizujący. Wskazuje bowiem obywatelom, że prawo karne nie jest jednoznaczne i zakres jego stosowania zależy od uznania organów ścigania i organów wymiaru sprawiedliwości.

Klasycznym przykładem takiego błędnego rozwiązania istniejącego w polskim prawie karnym jest wprowadzenie do prawa polskiego w 2004 r. art. 269b kodeksu karnego. Norma wynikająca z owego przepisu zakazuje wytwarzania, pozyskiwania, zbywania lub udostępniania innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia szeregu przestępstw przeciwko informacji (w tym podsłuchu elektronicznego i haking), a także dokonywania tych czynności wobec haseł komputerowych, kodów dostępu lub innych dane umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej.

Innym przypadkiem jest przygotowywany przez Ministerstwo Kultury i Dziedzictwa Narodowego projekt zmian w ustawie o prawie autorskim i prawach pokrewnych proponował nową treść art. 118^1 ustawy. Wprowadzenie w proponowanym w 2006 r. projekcie sformułowania „urządzenia, ich komponenty lub programy komputerowe" nie pozostawia wątpliwości, że karalne będzie posiadanie „oprogramowania" służącego do przełamywania tzw. „skutecznych zabezpieczeń". Takie rozwiązanie stawia przez informatykami, kryptologami i zwykłymi użytkownikami komputerów wiele pytań, na które nie można znaleźć

---

[3] Więcej o problemów kryptologów z tymi samymi przepisami: W.Wiewiórowski, *Czego nie może posiadać kryptolog ? Odpowiedzialność karna za posiadanie „narzędzi, komponentów i programów do usuwania skutecznych zabezpieczeń"* [w:] *XI Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2007. Materiały konferencyjne*, Enigma, Warszawa 2007

jednoznacznych odpowiedzi, co jest niedopuszczalne w przepisach karnych.

Zakaz posiadania oprogramowania hakerskiego

Wprowadzając w 2004 r. do polskiego kodeksu karnego art. 269b § 1[4] zakazano wytwarzania i wprowadzania do obrotu[5] urządzeń i oprogramowania, które mogły być wykorzystane przy popełnianiu szerokiej gamy przestępstw komputerowych. Nowy artykuł Kodeksu jest praktycznie przetłumaczonym (z niewielką zmianą) odpowiednim przepisem wyżej konwencji budapeszteńskiej.

Art. 269b

§ 1 Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 2, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej,

podlega karze pozbawienia wolności do lat 3

Takie sformułowanie przepisu art. 269b kodeksu karnego powoduje dziś, że każdy szanujący się administrator sieci posiada nielegalne oprogramowanie i dane służące do przełamywania zabezpieczeń, a tym samym jest przestępcą. Oczywiście dotyczy to również każdego kryptologa zajmującego się systemami ochrony dostępu do danych elektronicznych. Fakt, że przepis ten jest w praktyce całkowicie martwy nie wpływa na złagodzenie jego oceny. Przepis ten bowiem zobowiązuje Policję do podejmowania działań, mających służyć realizacji norm płynących z niego.

Teoretycznie regulację taką należy uznać za bardzo wskazaną. Jej pojawienie się w polskim prawie było sporym zaskoczeniem *in plus*. Jak zawsze w takich przypadkach nie ustrzeżono się jednak drobnych – acz istotnych z praktycznego punktu widzenia – błędów. Pierwszym jest użycie niedookreślonego zwrotu „inne dane". Biorąc pod uwagę, że karalne jest „pozyskiwanie, zbywanie

---

[4] Szersze omówienie problemów prawnych związanych z tzw. „cybernowelizają 2004" w A. Adamski, *Buszujący w sieci. Cybernowelizacja prawa karnego*, „Rzeczpospolita. Prawo co dnia" nr 251 z 27 października 2003 r. oraz W.R.Wiewiórowski, *Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych* [w:] *Bezpieczeństwo sieci komputerowych a hacking. Internetki V. Materiały z konferencji naukowej, Lublin 4-5 marca 2005 r.*, Wyd. UMCS, Lublin 2005, s. 38-47

[5] Oczywiście zdaję sobie sprawę, że posiadanie jest równoznaczne z wytwarzaniem i wprowadzaniem do obrotu i udostępnianie takich danych i programów. Sam jestem właścicielem i posiadaczem oprogramowania tego typu nabytego przed 1 maja 2004 r. i nie jestem tym samym przestępcą. Nie mogę wszakże udostępniać swej własności innym osobom, gdyż to byłoby już czynem zabronionym. W dalszej części artykułu posługuje się niekiedy ze względów czysto redakcyjnych sformułowaniem „posiadanie" zdając sobie sprawę z czynionego uproszczenia.

lub udostępnianie innym osobom[6]" takich danych, każdy posiadacz literatury dotyczącej zagadnienia łamania zabezpieczeń jest przestępcą. Udostępnianie znajomym książki takiej jak „Anti-Hacker Toolkit"[7] może stać się w świetle omawianego przepisu „znaczącym błędem". Podobnie kwalifikowane powinno być zakupienie kolejnego numeru czasopisma „Hakin9" czy „XPloit" (przy prenumeracie mielibyśmy zaś chyba przestępstwo ciągłe).

Co ciekawe podobny do polskiego przepis wprowadziły do swego prawa karnego Niemcy w 2007 r. Niemiecka ustawa o zmianie ustawy kodeks karny w celu zwalczaniu przestępczości komputerowej przyjęta przez Bundestag 25 maja 2007 r. wyraźnie wskazuje w § 202 b ust. 1 na chęć implementacji konwencji Rady Europy o cyberprzestępczości oraz implementacji decyzji ramowej w sprawie ataków na systemy informatyczne. Przepis § 202c ust. 1. jest zaś idealnym odpowiednikiem przepisów polskich. Stwierdzono w nim, że:

Kto czyni przygotowania do popełnienia czynu określonego w § 202 a lub § 202 b, w taki sposób, iż:

(1) hasła lub inne kody bezpieczeństwa, które umożliwiają dostęp do danych (§ 202a ust. 2) lub

(2) programy komputerowe, których celem jest popełnienie takiego czynu, wytwarza, zdobywa dla siebie lub innej osoby, sprzedaje, przekazuje innej osobie rozpowszechnia lub umożliwia w inny sposób do nich dostęp, podlega karze pozbawienia wolności do roku lub karze grzywny.

Wspomniany wyżej § 202a niemieckiego kodeksu karnego mówi zaś o *hakingu.* To przestępstwo jest w Niemczech regulowane jako nieuprawnione umożliwienie sobie lub innej osobie dostępu do danych, które nie są dla tej osoby przeznaczone i które są w sposób szczególny zabezpieczone przeciw nieuprawnionemu dostępowi, poprzez przezwyciężenie zabezpieczeń dostępu. Jedyną poważniejszą różnicą pomiędzy polskimi a niemieckimi przepisami jest nakierowanie czynu, jakim jest zabronione posiadanie programów, haseł lub innych kodów bezpieczeństwa, na popełnienie przestępstwa (posiadanie w celu popełnienia przestępstwa). Takiego sformułowania brakuje w prawie polskim.

Tak czy inaczej pozostawia się sądom decyzje interpretacyjne. Teoretycznie nie jest to złe rozwiązanie. Na mądrość sądowej wykładni należy wszakże liczyć wówczas, gdy doświadczenie życiowe sędziów umożliwi im swobodną ocenę przedstawionych dowodów. Z taką sytuacją nie mamy jednak w Polsce (jeszcze) do czynienia w zakresie przestępstw komputerowych.

Pozostaje nam wyjaśnić, czy tak skonstruowany przepis kodeksu karnego

---

[6] O praktycznym znaczeniu zakazu i wprowadzeniu przy jego pomocy – rzadkiej w Polsce – konstrukcji nielegalnego posiadania pisze R.Koszut, *Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań konwencji o cyberprzestepczości* [w:]. J. Kosiński (red.), *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.43

[7] Jako przykład podaję klasyczny poradnik dla zwalczających hakerów, który wszakże dokładnie omawia sposoby działania przestępców. M. Shema, B. C. Johnson, *Anti-Hacker Toolkit. Pokonaj hakerów ich własną bronią,* Helion, Gliwice 2004.

jest stosowany. Oczywiście w porównaniu do skali zjawiska jakim jest wytwarzanie, nabywanie, zbywanie lub udostępnianie programów, haseł i danych, które mogą służyć do popełnienia przestępstwa polegającego na włamaniu się do systemu i uzyskaniu zeń informacji, przepis ten jest prawie martwy. Prawie, gdyż zdarza się, że stosowany jest on przez sądy w sytuacji, gdy *hakerowi* można udowodnić, że włamał się do systemu ale nie można udowodnić, że zapoznał się z informacją tam zamieszczoną. Wówczas zdarza się, że sąd orzeka w sprawie posiadania „narzędzi" do dokonania włamania. Jest to rozwiązanie złe, gdyż tak naprawdę sprowadza ono stosowanie prawa karnego komputerowego do złośliwego stwierdzenia „dajcie mi człowieka a przepis na niego się znajdzie".

Informatycy a Digital Rights Management

Duże zagrożenia dla polskiego środowiska informatycznego wiążą się z planowanymi w najbliższym czasie nowelizacjami prawa autorskiego zmierzającymi do implementowania do prawa polskiego rozszerzonej ochrony utworów związanej z zastosowaniem technik łącznie nazywanych *digital rights management* (dalej powoływanych jako DRM). Zaproponowany system możliwych do zastosowania przez twórców – a w praktyce przez ich wydawców – obostrzeń w dostępie do treści utworów jest dziś poddawany często krytyce. Co prawda pierwsze podejście do zmian zakończyło się z punktu widzenia Ministerstwa Kultury i Dziedzictwa Narodowego porażką w związku z bardzo krytycznymi uwagami zgłoszonymi jeszcze na poziomie konsultacji międzyresortowych między innymi przez Ministerstwo Spraw Wewnętrznych i Administracji oraz Urząd Ochrony Konkurencji i Konsumentów. Ministerstwo Kultury i Dziedzictwa Narodowego jak na razie dokonało więc zmian do ustawy w wymaganym przez Unię Europejską zakresie pozostawiając sprawę DRM do dalszych konsultacji. Ponieważ jednak nie wyzbyło się planów implementacji ochrony DRM, należy poddać krytycznej analizie zaproponowane zmiany.

Trudno w krótkim artykule rozważać wszystkie argumenty za i przeciw stosowaniu DRM oraz wszystkie problemy prawne, jakie może rodzić nowa regulacja w tym zakresie. Warto wszakże zwrócić uwagę środowiska informatycznego na proponowaną nową treść art. 118^1 ustawy o prawie autorskim i prawach pokrewnych. Doktryna prawa miała praktycznie od zawsze uwagi do tego przepisu. Kwestionowano jasność norm karnych, które z niego wypływają[8]. Niestety proponowane zmiany nie wyjaśniają owych wątpliwości. Wprowadzają natomiast dodatkowy chaos pojęciowy[9].

---

[8] J.Barta, R.Markiewicz, *Śluzy szeroko otwarte*, „Rzeczpospolita. Prawo co dnia" nr 145 z 23 czerwca 2000 r.

[9] Biorąc pod uwagę główny temat rozważań pomijam w niniejszym artykule omawianie paradoksu sformułowania „niedozwolone usuwanie lub obchodzenie skutecznych technicznych zabezpieczeń". Z punktu widzenia zwykłych zasad logiki „usuwanie i omijanie skutecznych zabezpieczeń" może budzić niepokój, ale z punktu widzenia logiki definicji prawnych jest sformułowaniem poprawnym

W pierwszej redakcji przepisu art. 118^1 zamieszczono pojęcie „przedmioty" w miejscu, gdzie dziś stosuje się pojęcie „urządzenia lub ich komponenty". Doktryna prawa karnego nie miała wątpliwości, że za „przedmioty" uznawać należało m.in. programy komputerowe (jakkolwiek rozumiane). To oznaczało karalność wejścia w posiadanie (np. samego „ściągnięcia" z sieci) programu dekodującego niezależnie od świadomości sprawcy lub jej braku, że dany program może zostać użyty przez kogoś z jego użytkowników do przełamywania zabezpieczeń[10]. Zdając sobie z tego sprawę ustawodawca w 2004 r. dokonał zmiany tego przepisu i ograniczył zakres odpowiedzialności jedynie do posiadania „urządzeń i ich komponentów". Takie sformułowanie też można poddać krytyce, ale w praktyce bzo ono rozumiane poprawnie przez sądy o organy ścigania.

Po zmianach z 2004 r. przepis brzmi następująco:

„Art. 118^1.

1. Kto wytwarza urządzenia lub ich komponenty przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami lub ich komponentami, albo reklamuje je w celu sprzedaży lub najmu,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

2. Kto posiada, przechowuje lub wykorzystuje urządzenia lub ich komponenty, o których mowa w ust. 1,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Propozycja Ministerstwa Kultury i Dziedzictwa Narodowego z 2004 r. miała za zadanie uzupełnienie tego przepisu tak by dotyczył on „urządzeń, ich komponentów lub programów komputerowych". Tym samym nie pozostawiano wątpliwości, że tym razem posiadanie odpowiedniego oprogramowania będzie karalne. Jednoczenie wszakże postawiono przez użytkownikami komputerów wiele pytań, na które nie można znaleźć jednoznacznych odpowiedzi, co jest niedopuszczalne w przepisach karnych.

Prawo polskie nie zawiera bowiem dziś jasnej definicji tego czym jest program komputerowy. Oczywiście definicja programu komputerowego jest formułowana na potrzeby prawa autorskiego, tym niemniej nie wydaje się by jej – cywilistyczna z założenia – treść była możliwa do zaakceptowania na gruncie prawa karnego w odniesieniu do „narzędzi" które mogą służyć do przełamywania technicznych zabezpieczeń utworów. Sama ustawa podobnie jak dyrektywa wspólnotowa z 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych, nie zawiera definicji programu komputerowego. Zdaniem

---

[10] M.Kliś, *Przestępstwa elektroniczne w aspekcie prawa autorskiego*, „Czasopismo Prawa Karnego i Nauk Penalnych" nr 2 z 2003 r. oraz P.Sedlec, *Przestępstwa naruszające prawa autorskie*, „Przegląd Sądowy" nr 7-8 z 2003 r.

twórców projektu polskiej ustawy szybki rozwój techniki powoduje, że sformułowanie takiej definicji na potrzeby prawa autorskiego jest niemożliwy[11]. Normy wynikające z ustawy nie mają zresztą za zadanie definiowania pojęcia programu komputerowego. Regulacja nakierowana jest jedynie na programy komputerowe, które są jednocześnie utworami w rozumieniu prawa autorskiego, gdyż jedynie o aspekt ochrony utwory chodzi ustawodawcy. Tym samym ustawodawca skupia się na stwierdzeniu, że dzieło informatyczne ma status utworu, jeśli jest przejawem działalności twórczej o indywidualnym charakterze oraz zostało „ustalone" w jakiejkolwiek formie[12].

Pojęcie „program komputerowy" jest w prawie polskim rozumiane kontekstowo. W sytuacji, w której oprogramowanie, które może służyć do przełamywania skutecznych zabezpieczeń jest dziś w dużej mierze tworzone poprzez kompilowanie powszechnie dostępnych komponentów programistycznych, nie ma możliwości jednoznacznego stwierdzenia czy posiadanie konkretnego komponentu jest już zabronionym przez prawo posiadaniem „programu", czy też jeszcze nie mamy do czynienia z „programem". Powoduje to nieusuwalną niejasność niedopuszczalną w przepisach karnych. Warto przy okazji wskazać, że implementowana dyrektywa zaleca w preambule podejmowanie działań zapobiegających „posiadaniu w celach handlowych urządzeń, produktów lub części składowych" (art. 6.1 dyrektywy w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym), podczas gdy polska ustawa ma generalnie zabraniać posiadania takich produktów lub ich części składowych. Co prawda dyrektywa nie wyklucza takiej możliwości (teza 49 preambuły), lecz wprowadzenia takiego rozwiązania przy całkowitym braku wyłączeń powoduje nielegalność posiadania odpowiedniego oprogramowania przez wszystkich użytkowników niezależnie od ich świadomości co do możliwości, jakie oprogramowanie mogłoby stwarzać.

Prawie komicznym tego efektem jest pominięcie w omawianych przepisach tzw. klauzuli niekaralności. Nie stworzono furtki do posiadania przynajmniej tych urządzeń, programów lub „innych danych", które mają na celu zabezpieczenie informacji przechowywanych w systemie komputerowym lub zabezpieczenie sieci teleinformatycznej. Powoduje to, że osoba odpowiedzialna za ochronę informacji nie może – pod groźbą odpowiedzialności karnej – poznawać sposobów działania sprawców ewentualnych włamań. Nie może również w żadnym wypadku sprawdzać bezpieczeństwa chronionej przez siebie domeny i nie może w końcu dzielić się swą wiedzą. Posuwając się do absurdu, nie może również zapisywać efektów swoich przemyśleń, bo to byłoby już „wytwarzanie".

Nie stworzono takiego kontratypu również dla ... Policji (sic !). Powoduje to, że również policjanci podążający tropem hakera w zasadzie musza łamać

---

[11] J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Dom Wydawniczy ABC*, Warszawa 2001

[12] A. Stuglik *Ochrona produktów informatycznych w prawie własności przemysłowej.* „Palestra" nr 9-10 z 2004, str. 59

prawo[13]. Jest to oczywiste niedopatrzenie, które występuje również we wprowadzonych tą samą nowelizacją przepisach o całkowitym zakazie posiadania materiałów pornograficznych[14]. Można to „niedopatrzenie" co prawda usunąć w przypadku policjanta - przy odrobinie dobrej woli - w trakcie procesu wykładni przepisu. Nie ma natomiast żadnej możliwości zastosowania owej „pozytywnej" dla uprawnionego wykładni w przypadku biegłego, obrońcy oskarżonego czy nawet sędziego lub prokuratora.

Polskie Towarzystwo Informatyczne jako zorganizowana grupa przestępcza

Jeśli przyjmiemy, że na podstawie choćby art. 269b kodeksu karnego każda osoba, która wytwarza, nabywa, zbywa lub udostępnia *exploity*, innego rodzaju „oprogramowanie *hakerskie*", hasła i dane, które mogą posłużyć do przełamywania zabezpieczeń informacji, jest przestępcą, pytanie o kwalifikację działań Polskiego Towarzystwa Informatycznego jako związku przestępczego lub co najmniej zorganizowanej grupy przestępczej nie jest takie znów absurdalne. Art. 258 kodeksu karnego wyraźnie wskazuje, że każdy, kto bierze udział w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Orzecznictwo i doktryna konkretyzują, że taki związek powinien składać się co najmniej z trzech osób, mieć względnie stałą strukturę organizacyjną oraz posiadać wspólny cel, program działania, formy współdziałania, podział funkcji i zadań jak również określone kierownictwo i ustalone zasady członkowstwa. PTI niewątpliwie odpowiada tym cechom.

Gdyby zaś czytelnicy mieli zastrzeżenia do działań PTI to niewątpliwie muszą przyznać, że Towarzystwo jest co najmniej zorganizowaną grupą przestępczą. Ta bowiem nie musi mieć długofalowego programu działania. Nie jest również konieczne dla niej posiadanie ustalonych zasad członkostwa (przynależności), a sama grupa może mieć mniejszy stopień zorganizowania.

Absurd lub nie. Zastanówcie się Państwo wszakże, czy na spotkania polskiego Towarzystwa Informatycznego należy zapraszać prawników.

---

[13] Ciekawe przypadki wykorzystywania koni trojańskich do walki z przestępcami komputerowymi i dokonywania ataków w sieci przez Policję opisuje Ł. Luzar, *Koń trojański w służbie Policji*, [w:] A.Misiuk, J. Kosiński , P.Ciszek [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VI Seminarium Naukowe – Szczytno 1-2 lipca 2003 r.* Wyższa Szkoła Policji, Szczytno 2003, s.105 i nast.

[14] A. Adamski pisze o braku takiego kontratypu w przypadku policjanta że „trudno znaleźć w prawie porównawczym przykład równie wadliwej regulacji omawianego zagadnienia" – A. Adamski, *Prawne problemy przeciwdziałania pornografii dziecięcej i pedofilii w Internecie* [w:]. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.26 oraz A. Adamski, *Zakaz dla ścigających i ściganych. Kodeks karny: Kiedy walka z pornografią dziecięcą jest przestępstwem*, „Rzeczpospolita. Prawo co dnia" nr 154 z 3 lipca 2004 r. Rozważania o prawnych problemach dotyczących błędu w obu przepisach można stosować zamiennie.

Literatura

1. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń TNOiK 2001,
2. Adamski, *Buszujący w sieci. Cybernowelizacja prawa karnego*, „Rzeczpospolita. Prawo co dnia" nr 251 z 27 października 2003 r.
3. Adamski, *Prawne problemy przeciwdziałania pornografii dziecięcej i pedofilii w Internecie* [w:]. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.26
4. Adamski, *Zakaz dla ścigających i ściganych. Kodeks karny: Kiedy walka z pornografią dziecięcą jest przestępstwem*, „Rzeczpospolita. Prawo co dnia" nr 154 z 3 lipca 2004 r.
5. Adamski, *Cyberprzestępczość - aspekty prawne i kryminologiczne.* „Studia Prawnicze" St.Prawn. nr 4 z 2005 r. s.
6. J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Dom Wydawniczy ABC*, Warszawa 2001
7. J. Barta, R. Markiewicz, *Śluzy szeroko otwarte*, „Rzeczpospolita. Prawo co dnia" nr 145 z 23 czerwca 2000 r.
8. S. Bukowski, *Kodeks karny a Konwencja o cyberprzestępczości - Przed wejściem do Unii Europejskiej*, „Gazeta Sądowa", nr 3 z 2004 r., s. 55
9. S. Bukowski, *Projekt zmian Kodeksu karnego - Dostosowanie do Konwencji o cyberprzestępczości*, „Gazeta Sądowa", nr 4 z 2004 r., s. 53
10. K. Gienas, *Hak na hakera,* „Rzeczpospolita. Prawo co dnia" nr 176 29 lipca 2005 r.
11. M. Kliś, *Przestępstwa elektroniczne w aspekcie prawa autorskiego*, „Czasopismo Prawa Karnego i Nauk Penalnych" nr 2 z 2003 r.
12. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004
13. R. Koszut, *Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań konwencji o cyberprzestepczości* [w:]. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.43
14. P. Kruszyński, *O niektórych propozycjach rządowego projektu ustawy o zmianie ustawy - kodeks karny, ustawy - kodeks postępowania karnego oraz ustawy - kodeks wykroczeń (w redakcji z dnia 19 sierpnia 2003 r.),* „Prokuratura i Prawo" nr 2 z 2004
15. Ł. Luzar, *Koń trojański w służbie Policji*, [w:] A.Misiuk, J. Kosiński, P.Ciszek [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VI Seminarium Naukowe – Szczytno 1-2 lipca 2003 r.* Wyższa Szkoła Policji, Szczytno 2003, s.105

16. A. Misiuk, J. Kosiński, P. Ciszek [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VI Seminarium Naukowe – Szczytno 1-2 lipca 2003 r.* Wyższa Szkoła Policji, Szczytno 2003, s.105
17. P. Sedlec, *Przestępstwa naruszające prawa autorskie*, „Przegląd Sądowy" nr 7-8 z 2003 r.
18. M. Shema, B. C. Johnson, *Anti-Hacker Toolkit. Pokonaj hakerów ich własną bronią,* Helion, Gliwice 2004.
19. Stuglik, *Ochrona produktów informatycznych w prawie własności przemysłowej*. „Palestra" nr 9-10 z 2004, str. 59
20. W. Wiewiórowski, *Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych* [w:] *Bezpieczeństwo sieci komputerowych a hacking. Internetki V. Materiały z konferencji naukowej, Lublin 4-5 marca 2005 r.*, Wyd. UMCS, Lublin 2005, s. 38
21. W. Wiewiórowski, *Informatyka prawnicza. Technologia informacyjna dla prawników i dla administracji publicznej*, Zakamycze, Kraków 2006
22. W. Wiewiórowski, *Czego nie może posiadać kryptolog ? Odpowiedzialność karna za posiadanie „narzędzi, komponentów i programów do usuwania skutecznych zabezpieczeń"* [w:] *XI Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2007. Materiały konferencyjne*, Enigma, Warszawa 2007