

# **Przestępstwa przeciwko prawom własności intelektualnej. Scena warez. Modus operandi.**

**Tomasz Rychlicki**

Jedynej Annie

## **1. Wstęp, pojęcie przestępczości komputerowej, piractwa komputerowego, praw własności intelektualnej**

Regulacje prawne, w szczególności w europejskim systemie prawa stanowionego, nie zawsze nadążają za szybko zmieniającą się codziennością<sup>1</sup>. Jaskrawym tego przykładem jest dziedzina naukowej i technicznej aktywności człowieka zwana informatyką. Istnieje duża liczba zdarzeń zawartych w działalności informatycznej, które zostały uregulowane, ale nadal są w ciągłym dynamicznym rozwoju, lub zdarzenia wymagające prawnych regulacji. Stwarza to potrzebę wnikliwego rozeznania ze strony prawodawcy oraz kompetentnie przygotowanej kadry prawniczej zajmującej się tą materią. Niniejsze opracowanie ma za zadanie wyjaśnić istotę działań przestępczych przeciwko prawom własności intelektualnej<sup>2</sup>, z wyszczególnieniem praw autorskich. Działania, które popularnie, choć niezbyt precyzyjnie, określane są mianem piractwa komputerowego. Przestępstwa te objawiają się w specyficznej formie zachowań. Przez ich sprawców nazywane są sceną warez.

Na wstępie podkreślić należy, że w literaturze prawniczej brak jest jednoznacznej i w pełni zaakceptowanej definicji przestępstw komputerowych. Można przyjąć na potrzeby niniejszego opracowania za K.J. Jakubskim, że przestępstwem komputerowym jest wszelkie zachowanie przestępcze związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące

---

1 J. Jabłońska-Bonca, Podstawy prawa dla ekonomistów, Warszawa 2002, s. 264 i n.

2 Termin własności intelektualnej zawiera m.in. porozumienie TRIPS będące integralną częścią Porozumienia Ustanawiającego Światową Organizację Handlu (WTO). Por. Obwieszczenie Ministra spraw Zagranicznych z dnia 12 lutego 1996 r. w sprawie publikacji załączników do Porozumienia ustanawiającego Światową Organizację Handlu (WTO), Dziennik Ustaw z 1996 r. Nr 32, poz. 143.

bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także sam komputer<sup>3</sup>. Na marginesie dodać należy, że pojawiają się definicje i klasyfikacje odmienne od prawniczych. Takim przykładem jest chociażby przyjęta przez zespół FIRST (Forum of Incidents Response and Security Teams, należy do niego m.in. CERT Polska<sup>4</sup>) nazwa „incydenty” i próba opracowania własnej spójnej taksonomii i nomenklatury określającej zgłaszane przez użytkowników sieci incydenty naruszające bezpieczeństwo sieci<sup>5</sup>.

W polskiej doktrynie prawnej za najbardziej odpowiadające specyfice przestępstw komputerowych rozumianych jako scena warez, uważam pojęcie piractwa komputerowego ujętego jako kopiowanie, reprodukcja, używanie i wytwarzanie bez zezwolenia produktu chronionego przez prawo autorskie<sup>6</sup>. W systemie prawnym USA, Departament Sprawiedliwości definiuje piractwo komputerowe jako: nieautoryzowaną reprodukcję i/lub dystrybucję prac chronionych prawem autorskim, takich jak programy komputerowe, filmy, muzyka<sup>7</sup>.

Sugerowałbym, aby definicję piractwa komputerowego pojmować szeroko, w szczególności, gdy następuje połączenie czynów przestępczych naruszających prawa z patentów, prawa ochronne na znak towarowy lub tzw. tajemnice handlowe z naruszeniem praw do dzieła chronionego na podstawie przepisów prawa autorskiego, a dokonanie czynu przestępczego przeciwko tym prawom powiązane jest z użyciem komputera<sup>8</sup> i/lub taką działalność można „umiejscowić” w sieci komputerowej.

Prawa wyszczególnione w ustawie z dnia 20 czerwca 2000 r. Prawo własności przemysłowej (tekst jednolity: Dziennik Ustaw z 2003 r. Nr 119, poz. 1117) łącznie z prawami zawartymi w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, (tekst jednolity: Dziennik Ustaw z 2000 r. Nr 80, poz. 904), określane są w języku prawniczym mianem dóbr niematerialnych<sup>9</sup> lub prawami własności intelektualnej. Przy tym ostatnim określeniu pozostają w dalszej części opracowania<sup>10</sup>.

---

3 K. J. Jakubski, *Przestępczość komputerowa – podział i definicja*, Problemy Kryminalistyki nr 217/1997, s. 31, oraz podana tam literatura przedmiotu.

4 Do końca roku 2000 pod nazwą CERT NASK – więcej wiadomości na temat tego zespołu znajdzie czytelnik na stronie internetowej: <http://www.cert.pl>.

5 M. Maj, K. Siłicki, *Klasyfikacja i terminologia incydentów naruszających bezpieczeństwo sieci*, [w:] *Internet 2000*, pod red. R. Skubisza. Lublin 2000, s. 239 i n.

6 B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno kryminalistyczne*, Kraków 2000, s. 71.

7 Departament Sprawiedliwości USA, *Computer Crime & Intellectual Property Section*. Strona internetowa: <http://www.cybercrime.gov>.

8 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 99.

9 A. Adamczak, *Słowo wstępne*, [w:] *Naruszenie praw na dobrach niematerialnych*, pod red. T. Szymanka, Warszawa 2001, s.17 i n.

10 Termin własności intelektualnej jest w polskiej doktrynie prawniczej dyskutowany. Posługuje się nim prof. T. Szymanek, *Postępowanie cywilne w sprawach własności przemysłowej i intelektualnej*, Warszawa 2001. Mniej problemu z zaakceptowaniem tego pojęcia miała doktryna systemu prawa common law.

## **2. Ustawowe regulacje odpowiedzialności prawnej za czyny naruszające prawa własności intelektualnej w nawiązaniu do specyfiki sceny warez**

Na wstępie chciałbym zaznaczyć, że celem niniejszego opracowania nie jest szczegółowa analiza normatywna obowiązujących regulacji prawnych. W precyzyjny sposób dokonało tego wcześniej wielu polskich autorów<sup>11</sup>. Poniżej prezentuję tylko podstawowe założenia i akty prawne, w których przewidziana została ochrona praw własności intelektualnej.

### **2.1. Odpowiedzialność karna na podstawie przepisów ustawy z dnia 6 czerwca 1997 r. Kodeks Karny**

Przedmiotem ochrony w rozdziale XXXV Kodeksu Karnego (Dziennik Ustaw z 1997 roku. Nr 88, poz. 553, z póź. zmianami) jest mienie, rozumiane zgodnie art. 44 k.c., czyli własność i inne prawa majątkowe. Rozdział zawiera cztery podstawowe typy przestępstw, które naruszają prawa własności intelektualnej: nielegalne uzyskanie programu komputerowego (art. 278 § 2), przywłaszczenie prawa majątkowego (art. 284) paserstwo programu komputerowego (art. 293 § 3) i oszustwo komputerowe (art. 287). Zagadnienie kradzieży samego nośnika (corpus mechanicum), na którym może być utrwalony program komputerowy lub inne dzieło (art. 278 § 1). Piractwo komputerowe jako działalność przestępcza zorganizowana (taka formę posiada scena warez) stanowi podstawę nadzwyczajnego obostrzenia kary na podstawie przepisu art. 65 k.k.

### **2.2 Ochrona przewidziana w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych**

Ochronę autorskich praw osobistych przewidują przepisy rozdziału 8 ustawy (tekst jednolity: Dziennik Ustaw z 2000 r. Nr 80, poz. 904), autorskie prawa majątkowe chronione są przez przepisy rozdziału 9. Odpowiedzialność karną zawierają przepisy rozdziału 14. Przedmiotem ochrony są prawa autorskie lub prawa pokrewne. Wszystkie przestępstwa uregulowane w artykułach 115-119 mają charakter powszechny i są przestępstwami umyślnymi (wyjątek stanowi przestępstwo określone w art. 116 ust 4)<sup>12</sup>. W literaturze podkreśla się zbieżność przepisów ustawy z przepisami kodeksu karnego w przypadku przestępstw dotyczących programu komputerowego<sup>13</sup>.

---

11 Por. A. Adamski, op.cit., s. 100 i n.

12 Z. Cwiąkański, Odpowiedzialność karna, [w:] Komentarz do ustawy o prawie autorskim i prawach pokrewnych, pod red. J. Barty, R. Markiewicza, Warszawa 1996, s. 472 i n.

13 Ibidem, s. 103 i n.

### **2.3. Ochrona przewidziana w ustawie z dnia 23 kwietnia 1964 r. Kodeks Cywilny**

Ochronę osobistych praw autorskich zapewniają artykuły 23 i 24 Kodeksu Cywilnego<sup>14</sup> (Dziennik Ustaw z 1964 r. Nr 16, poz. 93 z późn. zmianami). Ustalają minimalny standard ochrony przysługujący każdej osobie fizycznej<sup>15</sup>. W celu ochrony interesów majątkowych, twórca może skorzystać z roszczeń wynikających z ogólnych zasad odpowiedzialności cywilnoprawnej. Jest to odpowiedzialność odszkodowawcza zarówno deliktowa, jak i kontraktowa, przewidziana w art. 415 i następujących k.c.<sup>16</sup>

### **2.4. Ochrona przewidziana w innych przepisach prawnych**

Dodatkowo ochronę karną praw własności intelektualnej przewidują przepisy ustawy z dnia 30 czerwca 2000 r. Prawo własności przemysłowej (tekst jednolity: Dziennik Ustaw z 2003 r. Nr 119 poz. 1117<sup>17</sup>), przepisy ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity: Dziennik Ustaw z 2003 r. Nr 153 poz. 1503). Należy mieć na uwadze także ratyfikowane przez RP umowy międzynarodowe<sup>18</sup> i obowiązujące bezpośrednio od 1 maja 2004 r., prawo Unii Europejskiej.

## **3. Niektóre z powszechnie rozpoznanych form piractwa komputerowego**

Opracowania naukowe, klasyfikacje i statystyki w swej metodologii ujmują piractwo komputerowe na podstawie różnych kryteriów<sup>19</sup>. Poniżej prezentuję trzy najbardziej popularne podziały uzupełnione o krótki komentarz.

1) Piractwo komputerowe wyszczególnione ze względu na miejsce dokonania:

- bazy, stoiska, przy których oferuje się sprzedaż, ewentualnie nieuprawnione kopiowanie „na miejscu”. To zjawisko zaczyna być w fazie zaniku na terytorium Polski (pozostaje jeszcze duży problem stadionu X lecia), w związku z aktywnym działaniem służb celnych, policyjnych i inicjatywą prywatnych organizacji zajmujących się zwalczaniem naruszeń praw własności intelektualnej (m.in. BSA),
- piractwo domowe, czyli sprzedaż, dystrybucja, łamanie zabezpieczeń, nielegalne kopiowanie, dokonywane w warunkach domowych,

14 Z. Radwański, Prawo cywilne – część ogólna, Warszawa 2003, s. 155 i n.

15 Ibidem, s. 174.

16 W. Czachórski, Zobowiązania, Zarys Wykładu, Warszawa 1994.

17 Z. Ćwiąkański, Wybrane zagadnienia ochrony prawno-karnej w prawie autorskim i prawie własności przemysłowej, [w:] Naruszenia praw na dobrach niematerialnych, pod red. T. Szymanka, Warszawa 2001.

18 M.in. Akt paryski konwencji berneńskiej o ochronie dzieł literackich i artystycznych sporządzonym w Paryżu dnia 24 lipca 1971 r. Dziennik Ustaw z 1990 r. Nr 82, poz. 474. Pozostałe umowy wymienia A. Matlak, Prawo Mediów, Program Lex Polonica, Warszawa 2004 r.

19 B. Fischer, Przestępstwa komputerowe i ochrona informacji. Aspekty prawno kryminalistyczne, Kraków 2000, s. 72 i podana tam literatura.

- sprzedaż w sklepach komputerów z zainstalowanym nielegalnym oprogramowaniem, w celu podwyższenia atrakcyjności sprzedawanego towaru,
- sieci komputerowe: LAN, WAN, MAN i Internet. Trudno tutaj jednak mówić o konkretnym umiejscowieniu działania.

2) Business Software Alliance definiuje<sup>20</sup> następujące formy rozpowszechniania nielegalnego oprogramowania w Internecie:

- programy z protokołem typu peer 2 peer<sup>21</sup> (Kazaa Media Desktop, Direct Connect, WinMX, BitTorrent i wiele innych),
- poczta e-mail – kontakt pojedynczych użytkowników lub masowe e-maile,
- serwery grup dyskusyjnych,
- sieci typu Internet Relay Chat – IRC (programy tzw. boty z usługą opartą o protokół XDCC, wymiana plików pomiędzy pojedynczymi użytkownikami w oparciu o protokół DCC),
- mail order lub strony aukcyjne,
- serwery FTP (protokół transferu plików<sup>22</sup>),
- direct link – strony www, na których bezpośrednio umieszcza się nielegalne oprogramowanie lub oferuje sprzedaż,
- site links – odnośniki, bannery reklamowe kierujące na strony z nielegalnym oprogramowaniem, zachęcające do ściągnięcia lub oferujące sprzedaż.

Powyższe wyszczególnienie powinno mieć także zastosowanie do innych niż Internet sieci komputerowych. Bezdyskusyjnie przyjąć należy, że opisane formy dotyczą rozpowszechniania wszystkich rodzajów dóbr chronionych prawem autorskim (muzyka, filmy itp.).

Zauważyć trzeba, że nowym „miejscem” dokonania czynu przestępczego stają się także sieci telefonii komórkowych. Istnieje bardzo dużo aplikacji dla systemu operacyjnego telefonów komórkowych - Symbian<sup>23</sup>, programów napisanych w języku Java. Na scenie warez pojawiają się tego typu aplikacje/programy, ujęte w kategorii 0day. Tego rodzaju dzieła można rozpowszechniać za pomocą łącza IR, Bluetooth, usługi GPRS lub WAP. Sytuacja ma się tak samo do chronionych prawem autorskim plików muzycznych i wideo zapisanych w pamięci telefonów.

3) Piractwo komputerowe wyszczególnione ze względu na sposób dokonania:

<sup>20</sup> J. Sellinger, *Vehicles for theft: the form of internet software piracy*, opracowanie BSA 2001. Broszura dostępna na stronie internetowej: <http://www.bsa.org>.

<sup>21</sup> M. Szeliga, S. Nieszwiec, R. Bachman, M. Kura, T. Michalski, *Sieci P2P, Wymiana plików w internecie*, Gliwice 2004, s 405 i n.

<sup>22</sup> K. Pikoń, *ABC Internetu*, Wydanie IV, Gliwice 2003, s. 50 i n.

<sup>23</sup> Oficjalna strona internetowa: <http://www.symbian.com>.

- wykonywanie dodatkowych kopii, nieprzewidzianych w umowie licencyjnej, powielanie dokonane za pomocą nagrywarek CD/DVD,
- instalacja programu na twardym dysku, polegająca na instalacji dodatkowych kopii, takich, których nie przewiduje określona umowa licencyjna,
- fałszowanie, polegające na nielegalnym powielaniu dóbr chronionych przez prawo autorskie, często w formie mającej powodować wrażenie legalności produktu. Typowymi przykładami takiej działalności może być rozpowszechnianie programów lub płyt CD nie pochodzącego od danego producenta z jego znakami firmowymi, towarowymi lub zaopatrzenie cudzego produktu własnym znakiem firmowym lub towarowym (odpowiedzialność karną za tego rodzaju czyny przewiduje ustawa z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji, tekst jednolity: Dziennik Ustaw z 2003 r. Nr 153, poz. 1503),
- obchodzenie licencji typu: shareware i trial, poprzez instalowanie programów typu crack lub patch lub używanie do rejestracji i otrzymania w pełni działającego programu nielegalnych numerów seryjnych dla tego typu programów,
- wykorzystanie, bez zgody właściciela, kodu programu,
- przekroczenie zasady dozwolonego użytku osobistego wynikającej z art. 23 i nast. ustawy o prawie autorskim i prawach pokrewnych,
- nielegalne uzyskanie licencji poprzez zakup za pomocą carding'u (przestępstwa wyłudzenia przy użyciu nielegalnie zdobytych numerów kart płatniczych).

Dla dalszej części artykułu istotne jest to, że wspomniane wyżej klasyfikacje nie obejmują w swojej charakterystyce sceny warez. Scena warez jest obecnie głównym, częstokroć pierwotnym źródłem tworzenia i rozpowszechniania nielegalnych (pirackich) publikacji<sup>24</sup>. Szacuje się, że od 8 do 10 największych grup warezowych jest odpowiedzialnych za większość pojawiających się i już dostępnych na świecie pirackich publikacji.

## **4. Scena warez, modus operandi**

### **4.1. Krótka historia**

W dobie Internetu rozwinęło się w pełni, na szeroką i trudną do kontrolowania skalę, zjawisko określane jako scena warez. Jako takie mieści się bez wątpienia w kategorii czynów

---

<sup>24</sup> Departament Sprawiedliwości USA, Multiple Enforcement Actions Worldwide Snare Top "Warez" Leadership, publikacja prasowa z 11 grudnia 2001 r.

zabronionych przez ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych oraz przez ustawę z dnia 6 czerwca 1997 r. Kodeks Karny. W swojej specyfice scena warez łączy w sobie różne kategorie czynów prawnie zabronionych, m.in. naruszenie treści licencji, bezprawne rozpowszechnianie utworów (na serwerach FTP), manipulacja kodem programu w celu obejścia zabezpieczeń przed nieuprawnionym kopiowaniem (element tzw. reverse engineering) itp.

Pojęcie „warez” pochodzi z języka angielskiego. Wyraz wares oznacza towary i w tym właśnie znaczeniu występuje w slangu komputerowym. Scena warez w jej najprostszym założeniu wywodzi się korzeniami z subkultury hakerskiej, z tzw. demo sceny. Pierwsze oznaki działania i formowanie się zasad sceny warez odnotować można już w dobie komputerów 8 bitowych: spectrum, Atari, Commodore – maszyny te produkowane były we wczesnych latach 90.

Scena warez dotyczy swego rodzaju rywalizacji - wyścigu w obejściu lub usunięciu zabezpieczeń programów komputerowych implementowanych przez ich autorów (element crackingu), a także jak najszybszej publikacji i rozpowszechnieniu tego rodzaju programów na serwerach FTP<sup>25</sup> (wcześniej były to BBS)<sup>26</sup>. W przypadku innych dzieł chronionych prawem autorskim typu filmy, muzyka, rywalizacja dotyczy jak najszybszego ich opublikowania.

Scena warez to sporadycznie pojedyncze osoby, ale co do zasady dobrze zorganizowane grupy. Niektóre grupy lub jednostki koncentrują swoją działalność na określonych rodzajach publikacji. Venegance, Reloaded, Hoodlum zajmują się wyłącznie grami na komputery typu PC. LND (Legends never die), TDA (The Divine Alcoholics), Pantheon to grupy, które usuwają lub obchodzą zabezpieczenia i publikują programy użytkowe. Powstały odrębne grupy do publikacji gier na konsole Playstation, PS2, XBOX. Inne znowu zajmują się filmami lub muzyką.

#### **4.2. Grupa, hierarchia, działanie grupy i publikacja**

Hierarchia i metody działania grup są zróżnicowane i zależą w wielu przypadkach od rodzaju działalności, kategorii, do których zaliczają się publikowane dzieła. W niniejszym opracowaniu posłużę się przykładem grupy zajmującej się publikacją i rozpowszechnianiem gier na komputery typu PC. Grupą kieruje przywódca (leader)<sup>27</sup>. Zwykle, lecz niekoniecznie, to najstarszy stażem członek lub założyciel. Zarządza jej sprawami organizacyjnymi, ma w wielu przypadkach decydujący głos. Rada (council) służy do pomocy w nadzorze nad licznymi działaniami, sprawuje kontrolę nad większą liczbą członków, nad istniejącymi serwerami FTP. W skład rady wchodzi

<sup>25</sup> O sieciach komputerowych obszernie piszą: K. Krysiak, Sieci komputerowe. Kompendium, Gliwice 2003, M. Sportack, Sieci komputerowe. Księga eksperta, Wydanie II poprawione i uzupełnione, Gliwice 2004.

<sup>26</sup> M. Gramatyka, Piractwo komputerowe – Modus Operandi, Problemy Kryminalistyki nr 217/1997, s. 11 i n. Obszerny opis sceny warez w BBS (Bulletin Board System). Niestety z biegiem czasu artykuł stracił w dużej mierze na aktualności.

<sup>27</sup> Departament Sprawiedliwości USA, Operation Fastlink, Publikacja prasowa No. 04-263 z 22 kwietnia 2004 r.

seniorzy, byli przywódcy itp. Swoją podstawową działalność grupa opiera na crackerach, – czyli osobach dokonujących analizy kodu źródłowego pozyskanego programu w celu wyszukania metod, jakimi został zabezpieczony, oraz opracowanie cracka (zestawu poleceń zapisanych w pliku samowykonalnym - EXE), który umożliwi uruchomienie danego programu przy obejściu zastosowanych przez autora/producenta zabezpieczeń. Podobny w działaniu do cracka jest tzw. patch. W zabezpieczone programy i gry zaopatrują grupę dostawca (supplier) – osoba mająca kontakty w sklepach komputerowych, tłoczniach płyt CD/DVD i firmach produkujących oprogramowanie, a także sięgająca do innych metod pozyskiwania określonych dzieł, takich jak kupno, pożyczanie, kradzież, carding itp. W grupie istnieje zwykle funkcja testera, jego działalność polega na sprawdzeniu, czy wersja programu przerobiona przez crackera działa poprawnie na wszystkich systemach operacyjnych, dla których jest dedykowana. Paker (j. angielski - to pack) to osoba, której działanie polega na skompresowaniu (programem typu Rar) i podzieleniu sprawdzonego przez testera programu na pliki o 15 lub 20 megabajtowej objętości. Pakowanie i podział jest uzasadnione tym, że program zapisany na nośniku CD/DVD jako tzw. obraz (ISO image) to jeden plik i ma zbyt dużą objętość, aby go rozpowszechniać w całości oraz tym, że protokół FTP nie obsługuje sum kontrolnych. Jeżeli jakiś plik jest uszkodzony, prościej ponownie przetransferować część, zamiast całej publikacji ujętej w jednym pliku.

Paker nadaje wszystkim powstałym z podziału plikom i publikacji, która łączy podzielone pliki w określonym katalogu, odpowiednią nazwę. Do tej publikacji dołącza się plik informacyjny (rozszerzenie NFO) zawierający zwykle dane o grupie, instrukcje, jak zainstalować lub nagrać daną publikację, numery seryjne potrzebne do uruchomienia, itp. Przykładowo gra Doom 3 stworzona przez przedsiębiorstwo ID Software, została pozbawiona zabezpieczenia przez grupę Reloaded. Nazwa ich publikacji (główny katalog) brzmi: DOOM.3-RELOADED. Publikacja zawarta jest w formie przeznaczonej dla trzech płyt CD, składa się ze 125 plików skompresowanych programem RAR o objętości 15 megabajtów każdy. Plik informacyjny dołączony do tej publikacji nosi nazwę reloaded.nfo<sup>28</sup>. Paker dokonuje załadowania (upload) tak przygotowanej publikacji na serwery FTP, na których grupa dokonuje oficjalnej publikacji (tutaj określanej jako PRE). Osoby odpowiedzialne za zsynchronizowaną publikację to Preers.

---

<sup>28</sup> Strona <http://theisonews.com>, sekcja games.