Andrzej Adamski

Podstawy prawne zatrzymania sprzętu komputerowego przez Policję w sprawach o piractwo komputerowe

W roku 2001 media informowały o wielu przypadkach zatrzymania przez policję sprzętu komputerowego w celu zabezpieczenia materiału dowodowego w sprawach o tzw. piractwo komputerowe. Okoliczności, w jakich dochodziło do tych zatrzymań wywoływały protesty organizacji branżowych i krytykę prasową[1]. Niejednokrotnie kierowała się ona przeciwko samej idei „akcji antypirackiej" oraz jej promotorom (BSA, Microsoft Polska). Znacznie częściej dotyczyła jednak stosowanych metod zwalczania piractwa przez przedstawicieli organów ścigania i organizacji reprezentujących producentów programów komputerowych:

> *„Po wkroczeniu do firmy i machnięciu legitymacją służbową, wszystkim osobom pracującym przy komputerach każe się natychmiast odejść od stanowisk pracy, po czym komputery zaczyna badać ekspert, m.in. uruchamiając z przyniesionej dyskietki nieznany bliżej program. Jeżeli na którymś komputerze zostanie wykryte nielicencjonowane oprogramowanie, komputer zostaje "aresztowany", tzn. zapakowany i wywieziony z firmy. Przez cały okres badania komputerów nikomu z firmy nie wolno wyjść ani zatelefonować. Czasami, gdy bojówka jest łaskawa, pozwala się skopiować trochę dokumentów z aresztowanego komputera, dając na to 10-15 minut. Na zakończenie operacji szef firmy otrzymuje protokół-wspomnienie po komputerach, którym będzie musiał się zadowolić przez kilka miesięcy. Po tygodniu do firmy przychodzi "Postanowienie", w którym prokurator zatwierdza zatrzymanie "... rzeczy, przeszukanie przeprowadzone bez polecenie prokuratora w wypadku nie cierpiącym zwłoki".*[2]

Poniższe uwagi są próbą odpowiedzi nad kilka pytań natury prawnej, jakie nasuwa lektura cytowanego fragmentu artykułu oraz innych publikacji poruszających zagadnienie aktualnie stosowanych w Polsce metod walki z piractwem komputerowym - rozpowszechnionym wśród tzw. korporacyjnych użytkowników końcowych (ang. *corporate end-user piracy*)[3].
Zacznijmy od wyjaśnienia tego pojęcia.

1. Na czym polega piractwo komputerowe użytkowników korporacyjnych?

[1] A. Horodeński, Szwadrony informatycznej śmierci, „Rzeczpospolita" – dodatek „Rzecz w sieci"(2001.03.22.), tenże, Piraci i stróże prawa, „Rzeczpospolita" – dodatek „Rzecz w sieci" (2001.05.17), M. A. Zieliński, Czy wiesz, co masz na dysku, „Rzeczpospolita" (2001.12.24.), P. Krawczyk, Zdrowy rozsądek, a zabezpieczenie sprzętu komputerowego, Linux-News http://hedera.linuxnews.pl/_news/2001/06/19/_long/419.html

[2] A. Horodeński, Szwadrony informatycznej śmierci, j.w.

[3] Wg raportu Business Software Alliance „Software Piracy in the European Union", January 1999, organizacja ta w 1998 r. podjęła w Europie 2. 154 różnego rodzaju działań prawnych skierowanych przeciwko piractwu korporacyjnemu, w tym 280 niezapowiedzianych kontroli legalności oprogramowania w siedzibie jego użytkowników. 71 tego rodzaju kontroli (najwięcej w Europie) przeprowadzono w Polsce (s. 66).

Najprościej mówiąc, na używaniu nielicencjowanego oprogramowania w komputerach należących osób prawnych, podmiotów gospodarczych lub innych jednostek organizacyjnych nie posiadających osobowości prawnej. Najczęściej „piractwo korporacyjne" jest skutkiem: 1) używania oprogramowania w lokalnej sieci komputerowej na większej liczbie stanowisk niż na to zezwala umowa licencyjna; 2) wykonania, wbrew licencji, dodatkowych kopii programu na stanowiskach używanych przez pracowników.

2. Czy używanie nielegalnych kopii prawnie chronionych programów komputerowych jest w Polsce przestępstwem?

Nie. Polski ustawodawca nie przyjął takiego rozwiązania (zalecanego przez rekomendację Rady Europy nt. Przestępstw Komputerowych z 1989 r.). Zdecydował się natomiast na objęcie zakazem karnym szeregu innych form naruszeń autorskich praw majątkowych w odniesieniu do programów komputerowych, takich jak ich nieuprawnione: zwielokrotnianie [art. 117 ustPrAut], kopiowanie [art. 278 § 2 k.k.], rozpowszechnianie [art. 116 ustPrAut] oraz paserstwo [art. 118 ustPrAut , art. 293 k.k.].

3. Czy „piractwo korporacyjne" narusza któryś z wymienionych wyżej zakazów ?

Biorąc pod uwagę istotę tej formy piractwa (więcej kopii lub użytkowników niż licencji) oraz sposób zdefiniowania poszczególnych przestępstw przez ustawodawcę - w zasadzie wchodzić mogą w grę tylko dwa przepisy – art.278 § 2 k.k. (nielegalne uzyskanie cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej), oraz art. 293 k.k. (umyślne lub nieumyślne paserstwo programu komputerowego).

4. Czy właścicielowi przedsiębiorstwa lub osobie pełniącej funkcje kierownicze w jednostce organizacyjnej, w której używa się nielegalnego oprogramowania komputerowego grozi odpowiedzialność karna za tolerowanie tego stanu rzeczy ?

Nie. Polskie ustawodawstwo nie przewiduje sankcji karnych ani za brak nadzoru w tej dziedzinie ani za posiadanie nielegalnego oprogramowania komputerowego w związku z prowadzaną działalnością gospodarczą. Rozwiązania takie występują w prawodawstwie niektórych innych państw, np. Austrii i Wielkiej Brytanii, gdzie dyrektorzy instytucji lub właściciele przedsiębiorstw mogą odpowiadać karnie za tego rodzaju czyny.

5. W jakiej sytuacji kierownik zakładu pracy może odpowiadać karnie za ujawnione przypadki „piractwa korporacyjnego" ?

Na kierowniku zakładu pracy nie spoczywa szczególny obowiązek prawny kontrolowania legalności oprogramowania komputerowego używanego w zarządzanym przez niego zakładzie. Nie może on zatem odpowiadać za pomocnictwo do „piractwa korporacyjnego" przez zaniechanie (art. 18 § 3 k.k.). Może natomiast ponosić odpowiedzialność karną za podżeganie lub tzw. sprawstwo polecające, w szczególności, gdy wyda podległemu sobie

pracownikowi polecenie wykonania nielegalnych kopii programów komputerowych na stacjach roboczych znajdujących się w zakładzie.

6. Czy wiadomość o używaniu w firmie „X" „pirackich" programów komputerowych stanowi wystarczającą podstawę dla Policji do dokonania przeszukania pomieszczeń tej firmy w trybie art. 219 k.p.k.?

Tak, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że w firmie „X" używa się programów komputerowych uzyskanych z naruszeniem przepisu art. 278 § 2 lub art. 293 k.k. albo art. 117 lub art. 118 ustPrAut. Tylko w wypadkach nie cierpiących zwłoki[4] przeszukanie może być przeprowadzone bez postanowienia sądu lub prokuratora.

7. Czy Policja jest uprawniona do przeszukania zasobów komputerów znajdujących się w firmie „X" w celu uzyskania dowodów wskazujących na nielegalne pochodzenie programów komputerowych ?

Kodeks postępowania karnego nie przewiduje takiej możliwości. Art. 219 § 1 k.p.k. wyraźnie mówi o „przeszukaniu pomieszczeń i innych miejsc" w celu „znalezienia rzeczy mogących stanowić dowód w sprawie". Informacja, w tym program komputerowy, nie jest rzeczą (uzasadnienie projektu k.k. z 1997 r. do art. 278 § 2). Aktualny projekt nowelizacji k.p.k. przewiduje w związku z tym wprowadzenie do polskiej procedury karnej normy (art. 236a k.p.k.), która nakazuje odpowiednie stosowanie przepisów o przeszukaniu i zatrzymaniu rzeczy do danych komputerowych i przekazów informacji przesłanych pocztą elektroniczną. Do czasu uchwalenia przez Sejm i wejścia w życie wspomnianej zmiany ustawodawczej, przeszukanie zasobów systemu informatycznego w trybie art. 219 k.p.k. nie znajduje podstaw prawnych. Na czynność taką przysługuje zatem zażalenie (art. 236 k.p.k.).

8. Czy bez przeszukania „pamięci" komputera jego zatrzymanie przez Policję jest dopuszczalne ?

W ramach przeszukania „pomieszczeń i innych miejsc" Policja ma prawo zatrzymania każdej rzeczy, w tym komputerów, urządzeń peryferyjnych i nośników informacji, jeżeli z okoliczności sprawy wynika, że mogą one stanowić dowód w sprawie lub podlegają zajęciu w postępowaniu karnym.[5] Zatrzymanie komputera podczas przeszukania pomieszczenia może zatem nastąpić nie tylko w sprawie o jego kradzież, lecz także w celu odczytania i utrwalenia do potrzeb dowodowych znajdujących się w pamięci dyskowej komputera danych, w tym programów komputerowych.

9. Czy polskie prawo procesowe zezwala na zatrzymanie danych komputerowych przez ich skopiowanie?

---

[4] Tj. w sytuacji, gdy zwłoka spowodowana uzyskaniem postanowienia sądu lub prokuratora mogłaby doprowadzić do ukrycia lub utraty rzeczy podlegających zatrzymaniu.

[5] Wg Regulaminu prokuratury (§ 122) - zatrzymanie rzeczy jest dopuszczalne, jeżeli: 1) służyła ona lub była przeznaczona do popełnienia przestępstwa, 2) zachowała na sobie ślady przestępstwa, 3) pochodzi bezpośrednio lub pośrednio z przestępstwa, 4) może służyć jako środek dowodowy do wykrycia sprawcy czynu lub ustalenia przyczyn i okoliczności przestępstwa, 5) jej posiadanie bez zezwolenia jest zabronione.

Nie. Takiej alternatywnej metody zabezpieczenia dowodów przestępstwa, która nie wymaga zatrzymania sprzętu komputerowego, nie przewidują przepisy polskiej procedury karnej. „Zatrzymanie przez skopiowanie" zostało uznane za standard międzynarodowy przez Konwencję Rady Europy w sprawie Cyberprzestępczości. Ratyfikacja tej konwencji przez Polskę będzie wymagała dostosowania prawa polskiego do jej postanowień.

10. Jakie są zalety tej nowej, dostosowanej do środowiska komputerowego, metody gromadzenia materiału dowodowego w sprawach przestępstw związanych z technologią informacyjną?

Dwie podstawowe. „Zatrzymanie przez skopiowanie" : 1) umożliwia szybkie i efektywne zebranie „elektronicznych dowodów" przestępstw, gdy przedmiotem przeszukania jest rozbudowany lub odległy system komputerowy, 2) pozwala na respektowanie tzw. zasady proporcjonalności, czyli prowadzenie czynności procesowych opartych na środkach przymusu bez wyrządzania niepotrzebnych szkód i dolegliwości podmiotom dotkniętym tymi czynnościami. Na przykład pozbawienie redakcji gazety możliwości korzystania z komputerów wyposażonych w pirackie programy komputerowe nie jest konieczne, jeśli materiał dowodowy w sprawie o nielegalne skopiowanie tych programów można zabezpieczyć w inny sposób.

11. Czy polskie prawo zna „zasadę proporcjonalności" ?

Tak. W celu wzmocnienia konstytucyjnych gwarancji praw i wolności osobistych i gospodarczych do kodeksu postępowania karnego z 1997 r. wprowadzono przepis (art. 227), który nakazuje władzom publicznym zachowanie umiaru i poszanowanie godności osób oraz nie wyrządzanie niepotrzebnych szkód i dolegliwości przy stosowaniu takich środków przymusu procesowego jak przeszukanie i zatrzymanie.

12. Jakie konsekwencje prawne może powodować naruszenie nakazu „zachowania umiaru"?

Nie wywołuje bezpośrednich skutków w sferze skuteczności przeszukania i zatrzymania rzeczy. Zgodnie z art. 236 k.p.k., jest podstawą do złożenia zażalenia na sposób przeprowadzenia tych czynności. Może też uzasadniać wystąpienie z roszczeniem o odszkodowanie od Skarbu Państwa za szkody wyrządzone przez funkcjonariuszy, jeżeli zatrzymanie sprzętu komputerowego było niewspółmierne do wagi przestępstwa lub długotrwałe i wyrządziło przedsiębiorstwu lub instytucji niepotrzebne szkody majątkowe.[6]

[6] Wg orzeczenia Trybunału Konstytucyjnego z 5 grudnia 2001 r., każdy ma prawo do wynagrodzenia szkody, jaka została mu wyrządzona przez niezgodne z prawem działanie organu władzy publicznej. Wina funkcjonariusza nie ma znaczenia dla zasądzenia odszkodowania. Wystarczy niezgodność decyzji z przepisami prawa. (J. Kroner, Kodeks cywilny bez art. 418 k.c., „Rzeczpospolita" z 2001.12.05; I. Lewandowska, Wystarczy bezprawność decyzji, aby żądać odszkodowania od władzy, „Rzeczpospolita" z 2002.01.09.).