Mariusz Nowak
Wyższa Szkoła Bankowa w Poznaniu

Cybernetyczne przestępstwa - definicje i przepisy prawne

Ostatnie dekady XX w. charakteryzował niewątpliwie gwałtowny rozwój Internetu i procesy związane z globalizacją. To właśnie Internet stał się dla nas synonimem cyberprzestrzeni. Samo pojęcie cyberprzestrzeń pojawiło się pierwszy raz ponad 25 lat temu w opowiadaniu *Burning Chrome* Williama Gibsona[1]. Ten amerykański pisarz (uważany za twórcę nurtu cyberpunku w literaturze science fiction) użył pojęcia *cyberprzestrzeń* do określenia wirtualnej rzeczywistości, w której umiejscowił swoich bohaterów. Choć znaczenie tego pojęcia ulegało stopniowo zmianie, to jego obecna definicja nie odbiega znacząco od pierwotnej funkcji. Obecnie mianem tym określa się przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie. Definicję taką sformułował Pierre Delvy w tekście *Deuxieme Deluge* (*Drugi Potop*) napisanym na zlecenie Komisji Kultury Rady Europy w 1996 r.[2] Warto podkreślić, że definicja uwzględnia wszystkie systemy komunikacji elektronicznej (w tym również sieci telefonii komórkowej). Jednak trudno mówić o jednej, powszechnie obowiązującej definicji cyberprzestrzeni. Łatwiej wskazać pewne istotne cechy, które ją charakteryzują:

- niematerialny charakter,
- brak możliwości określenia granic,
- zdecentralizowanie,
- brak ośrodków kontroli i nadzoru nad jej całością,
- płynny i plastyczny charakter,
- powszechna dostępność,
- przetwarzanie i dokładne obliczanie w czasie rzeczywistym.

Powyższe cechy, choć wpłynęły bez wątpienia na gwałtowny rozwój Internetu (pojęcie cyberprzestrzeni bywa często używane jako synonim Internetu) stanowiły i stanowią wyzwanie dla systemów prawnych poszczególnych państw. *Internet jako sieć komputerowa charakteryzuje się kilkoma cechami, które mają znaczenie w płaszczyźnie prawnej. W pierwszej kolejności podkreśla się globalny zasięg sieci, który powoduje, że sieć przez swój ogólnoświatowy charakter nie może zostać przyporządkowana danemu państwu lub być kontrolowana przez jedno państwo*[3]. Bardzo ważną cechą jest także jej interaktywność umożliwiająca wymianę informacji i porozumiewanie się na odległość. Nie może być ona traktowana jako podmiot prawa i nie jest też przedmiotem praw. Fakt, że nie istnieje żadna osoba bądź firma odpowiedzialna za zdarzenia występujące w sieci (jako całości) powoduje, że na gruncie prawnym trudno o sformułowanie wyczerpującej definicji Internetu.

Funkcjonowanie bibliotek w cyberprzestrzeni pozwala na uzyskanie bardzo wielu korzyści, zwłaszcza w zakresie promocji swoich zasobów i oferowanych usług. Niestety wiąże się z tym także wiele zagrożeń. Biblioteki tworzą i udostępniają w sieci rozmaite cyfrowe bazy danych. Tym samym stają się narażone na ich kradzież i utratę dorobku wieloletniej pracy. W celu zapewnienia ich należytej ochrony, w lipcu 2001 r., Sejm RP implementował do polskiego prawa *Dyrektywę 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych*[4]. Wcześniej z ochrony prawnej na mocy *Ustawy o prawie autorskim i prawach pokrewnych*[5] korzystały wyłącznie te bazy danych, które spełniały kryterium twórczego charakteru w rozumieniu wspomnianej ustawy. Istniało jednak bardzo wiele baz, które z różnych powodów nie spełniały tego kryterium i tym samym nie były objęte ochroną prawną. Przykładem takiej bazy, której ochronę prawną zapewniła wspomniana ustawa o ochronie baz danych może być chociażby cyfrowy katalog biblioteczny. Wszelkie bazy danych mogą być przedmiotem zainteresowania przestępców. Dlatego bardzo ważna jest świadomość bibliotekarzy w zakresie zagrożeń wynikających z pracy w sieci. Dynamiczny rozwój nowych technologii a także znaczne upowszechnienie korzystania z komputerów przyczyniło się do szybkiego rozwoju działalności przestępczej w cyberprzestrzeni. Wraz z rozwojem Internetu pojawiło się wiele, dotychczas nieznanych, form działalności przestępczej. Jest to zjawisko bardzo groźne, ponieważ sieć komputerowa staje się najważniejszym kanałem informacyjnym, a w państwach rozwiniętych stanowi wręcz niezbędny element funkcjonowania zarówno społeczeństwa, jak i państwa.

W polskim systemie prawnym nie ma jednoznacznej definicji przestępczości komputerowej. Wg K. Jakubskiego *w szerokim rozumieniu przestępczość komputerowa obejmuje wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer. Należy tu zaznaczyć, iż będą to zarówno czyny popełniane przy użyciu elektronicznych systemów przetwarzania danych (komputer jako narzędzie do popełnienia przestępstwa), jak i skierowane przeciwko takiemu systemowi*[6]. Natomiast wg M. Sowy *przestępstwa internetowe to przestępstwa, w przypadku których usługi sieciowe (możliwości oferowane przez Internet) umożliwiły lub co najmniej ułatwiły sprawcy realizację zamierzonego czynu przestępnego albo jego poszczególnych stadiów. Innymi słowy, o przestępczości internetowej mówimy wtedy, gdy bez użycia sieci do popełnienia określonego czynu dojść by nie mogło lub jego dokonanie byłoby znacznie bardziej utrudnione*[7]. Niezależnie od przyjętej definicji pojęcia przestępstwa internetowego zawsze będą to czyny zabronione, skierowane przeciwko systemowi komputerowemu (komputer jest celem), jak i czyny dokonane przy użyciu komputera (komputer jest narzędziem).

Na gruncie prawa międzynarodowego na szczególną uwagę zasługuje definicja cyberprzestępstwa wypracowana przez X Kongres ONZ w sprawie Zapobiegania Przestępczości i Traktowania Przestępców:

- Cyberprzestępstwo w wąskim sensie (przestępstwo komputerowe) – wszelkie nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub poddawanych procesom przez te systemy danych.
- Cyberprzestępstwo w szerokim sensie (przestępstwo dotyczące komputerów) – wszelkie nielegalne działanie, popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to m.in. nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[8].

Rodzaje przestępstw

Przestępstwa dokonywane w cyberprzestrzeni mogą mieć różny charakter. Ich podział ze względu na dynamiczny rozwój Internetu (i tym samym przestępstw internetowych) ulega zmianom. Dość rozpowszechnionym jest podział dokonany przez U. Siebera oparty na kryterium wyłaniania się przestępstw wraz z postępem techniki komputerowej:

- przestępstwa w dziedzinie ochrony danych (naruszenie praw jednostki),
- przestępstwa gospodarcze z użyciem komputerów:
- manipulacje komputerowe: operacje rozrachunkowe, manipulacje bilansowe, manipulowanie stanem kont bankowych, nadużycia kart do bankomatów i innych środków płatniczych, nadużycia telekomunikacyjne,
- sabotaż i szantaż komputerowy,
- hacking komputerowy,
- szpiegostwo komputerowe,
- kradzieże software i inne formy piractwa dotyczące produktów przemysłu komputerowego.

Inne rodzaje przestępstw:
a) rozpowszechnianie za pomocą komputerów informacji pochwalających użycie przemocy, rasistowskich i pornograficznych,
b) użycie techniki komputerowej w tradycyjnych rodzajach przestępstw[9].

Natomiast według H. Cornwalla istnieją następujące grupy przestępstw komputerowych:
a) Niemożliwe do dokonania poza środowiskiem komputerowym:

- manipulacje dokonywane za pomocą komputera na zbiorach danych i oprogramowaniu,
- zamachy na urządzenia systemu informatycznego oraz ich kradzież,
- kradzież materiałów eksploatacyjnych systemów komputerowych,
- hacking.

b) Ułatwiane przez stosowanie komputerów:

- oszustwa (fałszowanie danych wejściowych, wykorzystywanie tzw. martwych dusz, realizacja fikcyjnych inwestycji),
- fałszerstwa i podszywanie się pod cudze nazwisko,
- kradzież informacji,
- podsłuch.

c) Popełniane przy biernym udziale komputerów (np. oszustwa lub wyrządzanie szkód w interesach gospodarczych oraz prywatnych).
d) Dokonywane przez profesjonalnych przestępców z wykorzystaniem komputerów[10].

Zanim przedstawię dokładniej poszczególne rodzaje przestępstw oraz przepisy polskiego prawa w tym zakresie, postaram się najpierw przybliżyć metody stosowane przez komputerowych przestępców, wyjaśnię też słownictwo związane z tymi czynami. Wraz z rozwojem sieci wciąż pojawiają się nowe metody, a omówienie wszystkich byłoby bardzo trudne, dlatego przedstawię jedynie najważniejsze z nich:

- *Koń trojański* zwany także trojanem – jest to program, *który po aktywowaniu wywołuje jakieś niepożądane działania, nieprzewidziane przez użytkownika programu. Taki program może usuwać pliki, ponownie sformatować dysk lub przesłać dane wrażliwe do autora programu*[11]. Oprogramowanie może być ukryte wśród powszechnie stosowanych programów użytkowych lub w samym systemie operacyjnym. Rozpowszechnianie ich najczęściej następuje za pomocą programów pocztowych lub stron WWW.
- *Bomba logiczna* – jej cechą charakterystyczną jest realizacja negatywnego zdarzenia w wyznaczonym czasie lub z chwilą spełnienia określonych warunków. Jeśli aktywacja złośliwego kodu związana jest z określoną datą lub godziną, program taki bywa także określany mianem bomby zegarowej.
- *Robak komputerowy* – samoreplikujący się program komputerowy. Programy tego typu stanowią podstawowe narzędzie cyberprzestępców do włamań serwerowych. W przeciwieństwie do wirusów komputerowych nie potrzebują nosiciela (z reguły jakiegoś pliku wykonywalnego) i rozpowszechniają się w całej zaatakowanej sieci, paraliżując często kolejne warstwy systemu w celu przejęcia uprawnień administratora węzła sieciowego. Nazwa *robak komputerowy* (computer worm) wywodzi się z powieści Johna Brunnera *The Shockwave Rider* opublikowanej w 1975 r.
- *Wirus* – podobnie jak robak komputerowy jest programem samoreplikującym się umieszczonym w innym programie (nosicielu). Jest niewątpliwie najbardziej znaną metodą cybernetycznych ataków. Wirusy są bardzo niebezpieczne, gdyż mogą w swojej strukturze zawierać trojany czy bomby logiczne. Mają one zdolność oddziaływania na dowolny element systemu komputerowego, a w szczególności:
  a. wyświetlania nietypowych obrazów na ekranie monitora,
  b. zakłócania, zmieniania lub usuwania plików danych (np. kasowanie danych, uszkadzanie programów, zmniejszanie miejsca na dysku poprzez oznaczanie niektórych miejsc na dysku jako uszkodzonych),
  c. zakłócania lub oddziaływania na porty komunikacyjne (np. zmiana kierunku działania myszki czy inicjowanie fałszywych połączeń telefonicznych),
  d. spowalniania pracy systemu komputerowego,
  e. powodowania fizycznych uszkodzeń podzespołów systemu komputerowego[12].

Istnieje wiele typów wirusów komputerowych. Najlepszą formą zabezpieczenia bibliotek przed ich negatywnym działaniem jest używanie specjalistycznych programów antywirusowych oraz regularne tworzenie kopii zapasowych gromadzonych na twardych dyskach danych.

- *Backdoor* (tylne wejścia) – metoda polegająca na umyślnym tworzeniu luk w zabezpieczeniach systemu w celu ich późniejszego wykorzystania. Często jej głównym celem jest stworzenie możliwości zalogowania się z maksymalnymi uprawnieniami i tym samym uzyskanie nieograniczonego dostępu do zgromadzonych danych.
- *Metoda salami* – polega na kradzieży drobnych sum z różnych źródeł, które są przekazywane następnie na rachunek przestępcy. Z reguły pojedyncze zdarzenie przy jej wykorzystaniu dotyczy bardzo drobnej sumy, której utraty właściciel nie dostrzega lub przelewania na rachunek bankowy przestępcy różnic wynikających z zaokrągleń. Jej istotą jest bazowanie na wielu drobnych operacjach finansowych.
- *E-mail bombing* – przesyłanie w krótkim czasie bardzo dużej liczby wiadomości pocztowych do określonego adresata w celu zablokowania jego poczty elektronicznej.
- *Sniffing* (podsłuch) – polega na przechwytywaniu pakietów danych przesyłanych w sieci, nawet tych, które nie są adresowane do komputera, na którym działa przestępca. Sniffer jest programem, który zmienia tryb pracy wybranego interfejsu sieciowego, dzięki czemu może przechwytywać i analizować wszelkie pakiety docierające do danego interfejsu sieciowego. Sniffing można więc wykorzystać do podsłuchu i np. przechwycenia identyfikatora i hasła innych użytkowników[13]. Programy takie są także wykorzystywane legalnie jako narzędzie administracyjne przy zarządzaniu i usuwaniu problemów z siecią.
- *Spoofing (phishing) – podszywanie się pod inny komputer w sieci. Stosuje się to np. dla uzyskania pewnych przywilejów (np. podszywając się pod jakiś zaufany dla ofiary komputer), lub też dla ukrycia swojego prawdziwego adresu IP w celu zachowania anonimowości*[14]. Przykładem wykorzystania takiej metody jest wysyłanie, do dużej liczby odbiorców, listów z prośbą o dokonanie zmian na swoim koncie bankowym i przekierowywanie ich na specjalnie stworzone strony internetowe, na których przestępcy pozyskują poufne informacje. Metoda ta jest często wykorzystywana do zdobycia danych dotyczących kart kredytowych lub innych poufnych danych. Szczególną jego odmianą jest *SMiShing* polegający na rozsyłaniu wiadomości tekstowych do użytkowników telefonów komputerowych w celu skłonienia ich do podjęcia działań pożądanych przez przestępcę.
- *DDoS* (Distributed Denial of Service) – forma ataku na system komputerowy lub usługę sieciową w

celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. W atakach tego typu wykorzystuje się jednocześnie bardzo wiele komputerów (także komputerów wcześniej zainfekowanych, których właściciele nie mają świadomości, że są wykorzystywane do takich ataków tzw. zombie). Ataki tego typu są wykorzystywane także dla celów politycznych (przykładem może być atak na serwery urzędowe Estonii w 2007 r. po ochłodzeniu stosunków z Rosją).

Cyberprzestępcy mogą wykorzystywać sieć informatyczną do wielu celów, korzystając z różnych metod. Pragnę zaznaczyć, że wykorzystywanie komputera do symulowania procesów określających możliwość powodzenia planowanego przestępstwa także jest nielegalne.

Polskie przepisy prawne

W polskim systemie prawnym przepisy dotyczące przestępczości komputerowej nie są zebrane w całość w jednym akcie normatywnym. Przestępstwa te w układzie systemowym mogą zostać podzielone na dwie zasadnicze grupy:

a. przestępstwa ujęte w przepisach części szczególnej *Kodeksu karnego*[15],
b. przestępstwa uregulowane w ramach przepisów karnych poszczególnych ustaw[16].

W pierwszej kolejności przedstawię przestępstwa komputerowe regulowane przez *Kodeks karny*. W rozdziale XVII dotyczącym *przestępstw przeciwko Rzeczypospolitej Polskiej* uregulowano m.in. kwestie związane ze szpiegostwem komputerowym. Szpiegostwo jest działaniem przestępczym na szkodę określonego państwa polegającym na gromadzeniu, przechowywaniu i przekazywaniu informacji obcemu wywiadowi. Jedną z jego form jest szpiegostwo komputerowe polegające na zdobywaniu danych zawartych na komputerowych nośnikach informacji. Głównym celem takiej działalności jest z reguły pozyskanie cennych informacji dotyczących nowoczesnych technologii oraz danych z zakresu wojskowości. Na mocy art. 130 § 3 k.k. czyn taki zagrożony jest karą pozbawienia wolności od sześciu miesięcy do ośmiu lat. Karalne jest także szpiegostwo na rzecz państwa sojuszniczego. Obecnie zdecydowanie częściej mamy do czynienia ze szpiegostwem o charakterze ekonomicznym.

Kolejną wyodrębnioną w *Kodeksie karnym* grupą przestępstw są *przestępstwa przeciw ochronie informacji*. Są to przestępstwa szczególnie często występujące i dotyczyć mogą wielu polskich bibliotek. W grupie tych przestępstw wyróżniamy:

- hacking,
- nieuprawnione przechwytywanie informacji (podsłuch),
- niszczenie informacji,
- sabotaż komputerowy.

Choć w literaturze brak jest powszechnie obowiązującej definicji *hackingu*, to jednak większość autorów przyjmuje, że jest to bezprawne wejście do systemu komputera w celu kradzieży jego czasu pracy i informacji. Warunkiem decydującym jest tutaj pokonanie przez sprawcę zabezpieczeń chroniących zgromadzone dane lub system komputerowy. W największym uproszczeniu możemy powiedzieć, że sprawca ponosi odpowiedzialność karną za zapoznanie się z treścią informacji zgromadzonej na komputerze (np. danymi ekonomicznymi czy zawartością skrzynki pocztowej), jeżeli uzyskał dostęp na skutek złamania istniejących zabezpieczeń. Ofiarą takiego przestępstwa może być praktycznie każdy użytkownik czy instytucja. Ściganie sprawcy takiego czynu następuje na wiosek pokrzywdzonego. Warto tu podkreślić, że jeśli uzyskanie dostępu do zgromadzonej w systemie komputerowym informacji nie wymagało pokonania żadnych zabezpieczeń, to popełnienie czynu zabronionego nie występuje. Trudności z ukaraniem sprawców takich czynów wynikają często z problemu udowodnienia faktu zapoznania się z treścią nielegalnie pozyskanej informacji, np. samo ściągnięcie plików nie oznacza jeszcze, że sprawca zapoznał się z ich zawartością, a tym samym uzyskał informację.

Zgodnie z art. 267 § 2 k.k. karze podlega każdy, *kto w celu uzyskania informacji, do której nie jest uprawiony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.* O tej metodzie cybernetycznego ataku wspomniałem już wcześniej. Ustawodawca nie wskazał konkretnych urządzeń, których wykorzystanie jest karalne. Oznacza to, że przepis ten obejmuje także komputer wyposażony w odpowiednie oprogramowanie. Z reguły sprawcystosują te urządzenia w celu zdobycia poufnych informacji umożliwiających dalsze przestępstwa, np. zdobycie danych dotyczących kart kredytowych.

Niszczenie informacji jest czynem, którego skutki mogą być bardzo dotkliwe dla bibliotek. Każde naruszenie integralności komputerowego zapisu informacji może uniemożliwić lub ograniczyć osobom uprawnionym możliwości zapoznania się z treścią informacji. Usunięcie lub zmodyfikowanie choćby 10% rekordów bibliotecznych byłoby dla biblioteki i jej użytkowników sytuacją bardzo kłopotliwą i uciążliwą. Sprawca takiego czynu podlega karze od trzech miesięcy do pięciu lat pozbawienia wolności i może być także zobowiązany do naprawienia szkody w części lub całości (choć w praktyce trudno mi wyobrazić sobie cyberprzestępcę, który na zapleczu bibliotecznym odtwarza rekordy). Na podstawie tego przepisu mogą być karane także osoby, które rozpowszechniają wirusy komputerowe. W Polsce samo pisanie wirusów nie jest karalne, a jedynie ich rozpowszechnianie. Chodzi tutaj oczywiście wyłącznie o działania umyślne, zatem przypadkowe zarażenie bibliotecznego komputera wirusem nie podlega karze.

Ostatnią grupą przestępstw przeciwko ochronie informacji są czyny określane mianem sabotażu komputerowego, który może polegać na:

- zniszczeniu, uszkodzeniu, usunięciu lub zmianie zapisu informacji,
- zakłócaniu lub uniemożliwianiu automatycznego gromadzenia lub przekazywania informacji,
- zniszczeniu lub uszkodzeniu urządzenia służącego automatycznemu przetwarzaniu, gromadzeniu i przesyłaniu informacji,
- zniszczeniu albo wymianie nośnika informacji.

Przepis ten dotyczy głównie danych gromadzonych przez organy administracji rządowej lub samorządowej oraz istotnych dla obronności kraju. W praktyce jest on bardzo często związany z szantażem komputerowym – odstąpienie od wywołania istotnych uszkodzeń sytemu informatycznego związane jest z określoną gratyfikacją finansową dla sprawcy. Nie obejmuje on czynów popełnionych nieumyślnie.

W rozdziale XXXV *Kodeksu karnego* wymienione są przestępstwa przeciwko mieniu. Do grupy czynów zabronionych, których sprawcy działają w celu osiągnięcia korzyści majątkowych zaliczono:

- kradzież programu komputerowego,
- kradzież karty bankomatowej,
- oszustwo telekomunikacyjne,
- oszustwo komputerowe,
- paserstwo programu komputerowego.

Część tych czynów jest powszechnie utożsamiana z pojęciem piractwa komputerowego. Zjawisko nielegalnego kopiowania programów komputerowych ma niestety wciąż charakter masowy. Przepisy dotyczące zwalczania tego procederu zawarte są także w *Ustawie o prawie autorskim i prawach pokrewnych*. Zapisy art. 278 § 2 k.k. mają większe znaczenie dla zwalczania nielegalnego kopiowania, gdyż przewidują karę pozbawienia wolności od trzech miesięcy do lat pięciu. Ściganie sprawcy z mocy tego paragrafu nastąpi zarówno wtedy, gdy sprawca przywłaszczy sobie nośnik z programem (np. dyskietkę), jak i cały komputer, na którym program był zainstalowany. Najistotniejszymi przesłankami są w tym przypadku chęć osiągnięcia korzyści majątkowej i uzyskanie programu komputerowego bez zgody osoby uprawnionej. W praktyce najczęściej sprawca jedynie kopiuje program, pozostawiając w dyspozycji poszkodowanego jego nośnik. Piractwo komputerowe wciąż stanowi bardzo istotny problem ze względu na przyzwolenie społeczne i małą świadomość prawną użytkowników. Środowisko bibliotekarskie nie akceptuje takich zachowań i zwalcza piractwo komputerowe.

Osobno ustawodawca uregulował kwestie związane z przywłaszczeniem karty bankomatowej. Jedną z wielu korzyści rozwoju sieci informatycznych stało się upowszechnienie kart magnetycznych umożliwiających pobieranie pieniędzy z automatów bankomatowych. Niestety w szybkim czasie stały się one celem cyberprzestępców. Choć banki niechętnie udzielają informacji na temat poniesionych w ten sposób strat, to jednak są to niewątpliwie kwoty znaczące. Skopiowanie lub kradzież karty bankomatowej jest przestępstwem niezależnie od tego czy przy jej wykorzystaniu zostały osiągnięte korzyści majątkowe, czy nie. Chroniona jest więc sama karta i zakodowane na niej informacje, a nie tylko środki finansowe, z których za jej pomocą możemy korzystać.

Jak wspomniano powyżej, cyberprzestrzeń obejmuje także sieci telekomunikacyjne. Mimo że ustawodawca osobno uregulował kwestie oszustw komputerowych i telekomunikacyjnych, to jednak najczęściej przestępstwa na szkodę operatorów telefonicznych są dokonywane przy wykorzystywaniu komputerów. Początkowo włamania do sieci telekomunikacyjnych określano mianem *phreaking*. Z czasem jednak zaczęto używać określenia *boxing* (nazwa ta nawiązywała do popularnej metody oszukiwania operatorów). Straty, które przez to przestępstwo ponoszą firmy telekomunikacyjne sięgają setek milionów dolarów rocznie[17].

O oszustwie komputerowym mówimy, gdy sprawca w celu osiągnięcia korzyści majątkowej lub wyrządzenia szkody innej osobie, bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie, przesyłanie informacji lub zmienia, usuwa czy wprowadza nowy zapis na komputerowym nośniku informacji. Pojęcie oszustwa komputerowego wiąże się najczęściej z manipulowaniem danymi lub programem w celu osiągnięcia korzyści majątkowych. Przykładem takiego oszustwa może być wspomniana już metoda *salami* lub zmiana danych dotyczących stanu konta bankowego. Przestępstwa tego typu mogą dotyczyć zarówno dużych firm (np. podwójna księgowość), jak i spraw drobniejszych. Oszustwem komputerowym byłoby bez wątpienia dokonanie zmian na koncie bibliotecznym czytelnika bez zgody biblioteki.

Przesłanką do wprowadzenia przez ustawodawcę pojęcia *paserstwa programu komputerowego* był fakt, że program komputerowy nie będąc rzeczą nie podlegał wcześniejszym regulacjom dotyczącym paserstwa. Przechowywanie, ukrywanie lub pośredniczenie w zbyciu programu komputerowego pozyskanego za pomocą czynu zabronionego jest karalne.

Przestępstwa przeciwko bezpieczeństwu powszechnemu stanowią osobną kategorię czynów

zabronionych. Do takich przestępstw komputerowych zaliczamy sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób, zamach terrorystyczny na statek morski lub powietrzny oraz nieumyślne zakłócenie automatycznego przetwarzania informacji prowadzące do zaistnienia niebezpieczeństwa powszechnego. Przepisy te w nieznacznym stopniu dotyczą bibliotek i ich pracowników. Mają one chronić głównie systemy informatyczne najważniejszych instytucji życia publicznego (szpitale, stacje kolejowe, lotniska, obiekty wojskowe itp.).

Bezpośrednio bibliotek mogą dotyczyć *przestępstwa przeciwko wiarygodności dokumentów*. Zgodnie z art. 270 § 1 k.k. fałszerstwo dokumentów, zarówno w całości, jak i częściach, zagrożone jest karą grzywny, ograniczenia wolności lub pozbawienia wolności od trzech miesięcy do pięciu lat. Biblioteki, tak jak wszystkie inne instytucje, mogą paść ofiarą tego typu przestępstw. Postęp techniczny powoduje, że możliwość kopiowania i fałszowania dokumentów jest bardzo duża. Tym samym zagrożenie, że na podstawie sfałszowanego dokumentu biblioteka udostępni sprawcy cenne materiały lub dokona zakupu kradzionej książki jest niestety realne. Zabezpieczenie się przed takimi zdarzeniami jest często trudne, gdyż biblioteki nie dysponują kosztownym sprzętem umożliwiającym wiarygodną weryfikację przedkładanych dokumentów. Wydaje się, że obecnie najlepszym zabezpieczeniem jest zdrowy rozsądek i uważne weryfikowanie podejrzanych okazji handlowych.

Internet od lat stanowi narzędzie pośredniczące w dokonywaniu i innych przestępstw. Jako główny kanał informacyjny, w większości państw rozwiniętych, wykorzystywany jest także do wielu celów przez świat przestępczy. Nie sposób wymienić wszystkich możliwości wykorzystania sieci do celów przestępczych, dlatego wspomnę tylko o dwóch. Pierwsza z nich dotyczy bibliotek bezpośrednio, druga dotyczy nas w stopniu pośrednim. Wraz z rozwojem Internetu rozwinął się także handel elektroniczny. Objął on sektor księgarski, w którym duża liczba książek jest kupowana przez biblioteki on-line. Udział procentowy nabywanych w ten sposób zbiorów bibliotecznych będzie stale rósł. Wpływa na to zarówno wygoda kupowania, jak i niższe koszty utrzymania księgarni (co przekłada się na ceny książek). Biblioteki będą z upływem lat częściej uczestniczyły w różnego rodzaju aukcjach internetowych w celu pozyskania cennych zbiorów niedostępnych już na rynku księgarskim. Z takimi metodami pozyskiwania zasobów wiążą się określone niebezpieczeństwa. Najwięcej zgłoszonych przestępstw internetowych dotyczy właśnie aukcji internetowych oraz zakupów on-line. Dlatego warto uważnie weryfikować sprzedawców, zanim narazimy się na utratę naszych skromnych zasobów finansowych. W dynamicznie zmieniającym się cybernetycznym świecie nie jest to zadanie łatwe, ale zawsze warto sprawdzić opinię o sprzedawcy, choćby kierując zapytanie do innych bibliotek.

Osobną kwestią jest rozpowszechnianie pornografii. Zagadnienie to dotyczy bibliotek pośrednio, gdyż oferują one jedynie dostęp do potencjalnego narzędzia przestępstwa, jakim może stać się stojący w czytelni komputerowej sprzęt elektroniczny. Internet bardzo szybko stał się miejscem aktywności środowisk związanych z produkcją i dystrybucją pornografii. Udostępnianie tego typu treści *za pośrednictwem sieci komputerowych w ciągu ostatnich kilku lat stało się powszechnym zjawiskiem. W Internecie można odnaleźć setki witryn internetowych oferujących zdjęcia, filmy a także pornograficzne przekazy na żywo za pośrednictwem kamer internetowych*[18]. Zgodnie z *Kodeksem karnym* (art. 202 § 1 i § 2), *kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jednocześnie, kto małoletniemu poniżej lat 15 prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.* Nośnik, za pośrednictwem którego prezentowane są takie treści, nie ma tutaj znaczenia. Oczywiście sam fakt udostępnienia przez bibliotekę komputera podłączonego do sieci nie jest karalny. Wyszukanie takich treści w Internecie wymaga od użytkownika podjęcia określonych działań, np. wpisanie adresu strony lub słowa kluczowego w wyszukiwarce. Czy więc bibliotekarze powinni reagować widząc na ekranie monitora zakazane treści? Moim zdaniem tak, z dwóch powodów. Po pierwsze skoro widzą te treści, to oznacza z reguły, że mogą być one widoczne także przez osoby, które sobie tego nie życzą, czyli innych użytkowników biblioteki. Drugim powodem są kwestie moralne, biblioteka nie wydaje się być miejscem stosownym do zapoznawania się z takimi treściami.

Bardzo istotnym aktem normatywnym regulującym kwestie związane z przestępstwami w cyberprzestrzeni jest wspomniana już *Ustawa o prawie autorskim i prawach pokrewnych*. Program komputerowy jest przedmiotem prawa autorskiego tak, jak każdy inny utwór w rozumieniu tej ustawy. Ochroną objęte są wszystkie programy spełniające przesłanki ustawy, czyli *będące przejawem działalności twórczej o indywidualnym charakterze i ustalone w dowolnej postaci.* Przeznaczenie programu komputerowego oraz jego wartość nie mają znaczenia, ustawodawca zapewnił twórcom tych utworów ochronę taką jak utworom literackim. Co więcej, uwzględniając ich specyficzny charakter i łatwość kopiowania dokonał kilku zapisów zwiększających ich ochronę przed piractwem komputerowym. Zakładając, że zasady ochrony praw autorskich utworów literackich są bibliotekarzom dobrze znane, wspomnę tylko o jednej istotnej różnicy dotyczącej programów komputerowych. Chodzi tutaj o ograniczenia w zakresie tzw. dozwolonego użytku. W przypadku rozpowszechnionego utworu literackiego możemy bez narażenia się na konsekwencje prawne korzystać z niego na użytek własny, a nawet udostępnić członkom najbliżej rodziny. Jednak z takiego użytkowania wyłączone są programy komputerowe, w ich przypadku dozwolony użytek osobisty nie jest możliwy.

Dlatego dość ostrożnie należy podchodzić do udostępniania użytkownikom płyt zawierających programy

komputerowe. Choć w razie wykonania kopii, naruszenie praw autorskich następuje z winy użytkownika i biblioteka nie ponosi za to odpowiedzialności, to jednak zalecam w tym zakresie daleką ostrożność. Jeżeli kopia będzie wykonana na sprzęcie bibliotecznym, może nam grozić nawet jego utrata! Wykonywanie wszelkich kopii programów komputerowych jest możliwe wyłącznie wtedy, gdy jest to niezbędne dla zapewnienia ich prawidłowego funkcjonowania (ale nawet wówczas nie wolno bez zgody twórcy korzystać jednocześnie z programu i kopii). Piractwo komputerowe polega w uproszczeniu na kopiowaniu, rozpowszechnianiu lub pośredniczeniu w zbyciu kopii programów komputerowych. Chcę także zaznaczyć, że błędnym jest często spotykane przekonanie, że korzystanie z zagranicznych serwerów uniemożliwia ściganie sprawcy przez organy polskiego wymiaru sprawiedliwości.

Zakończenie

Zagrożenie dla bibliotek ze strony przestępców działających w cyberprzestrzeni jest realne. O ile kradzież rekordów bibliograficznych z katalogu bibliotecznego nie leży raczej w zakresie ich zainteresowań, o tyle zgromadzone w systemach bibliotecznych dane osobowe czytelników mogą stać się celem przestępczej działalności. Dlatego należyte zabezpieczenie baz danych, zgodnie z obowiązującymi w tym zakresie przepisami prawnymi, jest obowiązkiem bibliotekarzy. Mimo problemów finansowych polskich bibliotek należy wygospodarować w budżetach odpowiednie środki w celu ochrony baz danych tak, by zagrożenia przedstawione w tym artykule nie stały się przyczyną ich kłopotów.

Przypisy

[1] Opowiadanie *Burning Chrome* opublikowało w 1982 r. amerykańskie czasopismo *„Omni”* a pojęcie *cyberprzestrzeń* spopularyzowała debiutancka powieść Wiliama Gibsona *Neuromance* opublikowana w 1984 r.

[2] DELVY, P. Drugi Potop. *Magazyn Sztuki* 1997 nr 13 [on-line]. [Dostęp 12 kwietnia 2010]. Dostępny w World Wide Web: **http://dsw.muzeum.koszalin.pl/magazynsztuki/archiwum/nr_13/perre_delvy_2potop.htm**.

[3] PODRECKI, P. i in. *Prawo Internetu*. Warszawa: Wydawnictwo Prawnicze Lexis Nexis, 2007, s. 20.

[4] Dz. U. z 2007 r. Nr 128, poz.1402.

[5] Dz. U. z 1994 r. Nr 24, poz. 83.

[6] JAKUBSKI, K. Przestępczość komputerowa – zarys problematyki. *Prokuratura i Prawo* 1996 nr 12, s. 34.

[7] SOWA, M. Odpowiedzialność karna sprawców przestępstw internetowych. *Prokuratura i Prawo* 2002 nr 4, s. 62.

[8] *Wymiana doświadczeń w zakresie przestępczości…* [on-line]. Warszawa: Komenda Główna Policji, 2008 [Dostęp 16 kwietnia 2010]. Dostępny w World Wide Web: **http://www.katowice.szkolapolicji.gov.pl /pdf/Karty_platnicze.pdf**.

[9] PŁAZA, A. Przestępstwa komputerowe. Skrót pracy magisterskiej na blogu VaGli. W: *VaGla.pl* [on-line]. [Dostęp 12 kwietnia 2010]. Dostępny w World Wide Web: **http://prawo.vagla.pl/skrypts/przestepstwa.htm**.

[10] Informatyka kryminalistyczna. Fragment książki: GRUZA, E., GOC, M., MOSZCZYŃSKI, J. Kryminalistyka – czyli rzecz o metodach śledczych. W: *Klub kryminalny* [on-line]. Warszawa: WaiP, 2008 [Dostęp 12 kwietnia 2010]. Dostępny w World Wide Web: **http://www.klubkryminalny.pl/index.php/informatyka-kryminalistyczna/**.

[11] DENNING, D. E. *Wojna informacyjna i bezpieczeństwo informacji.* Warszawa: Wydawnictwa Naukowo-Techniczne, 2002, s. 294.

[12] PŁAZA, A. dz. cyt., s. 9-10.

[13] HARĘŻA, A. *Przyczynek do zagadnienia węszenia w sieciach – jako formy przestępstwa komputerowego* [on-line]. [Dostęp 17 kwietnia 2010], Dostępny W World Wide Web: **http://www.skn-bpk.prawo.uni.wroc.pl /.../art1_Weszenie_w_sieciach_AH.doc**.

[14] *i-slownik.pl Słownik Slangu Komputerowego* [on-line]. [Dostęp 17 kwietnia 2010]. Dostępny w World Wide Web: **http://www.i-slownik.pl/1,1366,spoofing.html**.

[15] Dz. U. z 1997 r. Nr 88, poz. 553.

[16] GOLATA, R. *Internet – aspekty prawne*. Warszawa: Difin, 2003, s.105.

[17] PŁAZA, A. dz. cyt., s. 30.

[18] GIENAS, K. Pornografia w Internecie - zarys problematyki. *Nowe Media* [on-line]. [Dostęp 17 kwietnia 2010]. Dostępny na World Wide Web: **http://www.nowemedia.org.pl/nuke/modules.php?name=Content& pa=showpage&pid=31**.

Cybernetyczne przestępstwa - definicje i przepisy prawne / Mariusz Nowak // W: Biuletyn EBIB [Dokument elektroniczny] / red. naczelny Bożena Bednarek-Michalska - Nr 4/2010 (113) maj. - Czasopismo elektroniczne. - [Warszawa] : Stowarzyszenie Bibliotekarzy Polskich KWE, 2010. - Tryb dostępu: http://www.ebib.info/2010/113/a.php?nowak. - Tyt. z pierwszego ekranu. - ISSN 1507-7187