Katarzyna Witek

Przestępczość komputerowa : aspekty prawne

Edukacja - Technika - Informatyka nr 2(24), 39-47

2018

© Wydawnictwo UR 2018 „Edukacja – Technika – Informatyka” nr 2/24/2018
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2018.2.4

KATARZYNA WITEK

Przestępczość komputerowa – aspekty prawne

Legal Aspects of Cybercrime

Magister, Uniwersytet Rzeszowski, Wydział Socjologiczno-Historyczny, Instytut Filozofii, Polska

Streszczenie

Autorka omawia wybrane aspekty prawne przestępczości komputerowej. W pierwszej części artykułu poruszono kwestie związane z definiowaniem przestępczości komputerowej. Kolejne zagadnienie dotyczą rodzaju przestępstw możliwych do popełnienia z wykorzystaniem komputera z uwzględnieniem klasyfikacji przestępstw komputerowych na gruncie polskiego prawa karnego. Autorka wykorzystuje dwie prawno-porównawcze metody badawcze, tj. historyczno-opisową oraz formalno-dogmatyczną.

Słowa kluczowe: przestępczość komputerowa, cyberprzestępczość, Kodeks karny, rodzaje przestępstw komputerowych, kryminologia

Abstract

The author discusses selected legal aspects related to computer crime. In the first part of the article, the author discusses issues related to the definition of computer crime. Another issue concerns the type of crimes that can be committed using a computer, classifying computer crime sunder Polish criminal law. In the article, the author uses two comparative research methods, i.e. historical-descriptive method and formal-dogmatic method.

Keywords: computer crime, cybercrime, The Criminal Code, cybercrime classifications, criminology

Wstęp. Kwestie terminologiczne

Istnieje wiele definicji przestępczości komputerowej. Odstąpiłam jednak w artykule od deskryptywnego i wtórnego zaprezentowania wszystkich pojęć związanych z cyberprzestrzenią oraz wyliczania proponowanych definicji na rzecz przybliżenia trudności terminologicznych, które pojawiają się w aspekcie prawnym poruszanej problematyki.

Wraz z coraz częstszym wykorzystywaniem nowych technologii w celach sprzecznych z prawem pojawiła się potrzeba nazwania czynów polegających na naruszeniu dóbr prawnych z użyciem komputera. W literaturze zaczęły pojawiać się takie pojęcia, jak *przestępstwa związane z wykorzystaniem komputer* czy po

prostu *przestępstwa komputerowe* (Siwicki, 2013, s. 9), jednak nie są one wystarczająco precyzyjne i winno się je rozpatrywać raczej w kategorii haseł niż oznaczeń konkretnego działania przestępczego (Jakubski, 1996, s. 34).

Pierwotnie termin *przestępczość komputerowa* był definiowany dwojako. W pierwszym ujęciu to komputer był przedmiotem lub środowiskiem zamachu, a mianem *przestępstwa komputerowego* określano działanie z użyciem komputera mające na celu naruszenie dowolnego dobra prawnego podlegającego ochronie karnej. Drugie rozumienie było determinowane posiadaniem przez sprawcę wyspecjalizowanych umiejętności oraz szczególnej wiedzy z zakresu informatyki, co miało stanowić element konieczny do popełnienia przestępstwa (Siwicki, 2013, s. 10).

Próba stworzenia kompleksowej definicji przestępstw popełnianych z użyciem komputera okazała się wyjątkowo skomplikowana, szczególnie że ich identyfikacja w poszczególnych kodyfikacjach karnych znacznie się od siebie różniła. „W szerokim rozumieniu, przestępczość ta obejmuje wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszeniu 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" (Jakubski, 1996, s. 34). Oznacza to, że mianem przestępstwa komputerowego określamy zarówno czyny, w których komputer pełnił funkcję narzędzia do dokonania przestępstwa, jak i te skierowane przeciwko systemom przetwarzania danych (Jakubski, 1996, s. 34).

Definicji *przestępstw komputerowych* możemy również szukać na polu karnoprocesowym, gdzie będzie ona ściśle związana z faktem, że w systemie komputerowym mogą znajdować się dowody na działalność przestępczą. W takim ujęciu za przestępstwa komputerowe uznaje się wszystkie czyny zabronione przez prawo karne, których ściganie stwarza potrzebę uzyskania przez ograny wymiaru sprawiedliwości dostępu do informacji przetwarzanych w systemach informatycznych. Tak rozumiane pojęcie obejmuje przypadki, w których system komputerowy stanowi zarówno narzędzie, jak i przedmiot zamachu (Adamski, 2000, s. 34).

Nieustający rozwój nowoczesnych technologii miał wpływ nie tylko na samo zjawisko przestępczości, ale także na stosowaną terminologię – określenie *przestępstwo komputerowe* stało się w dzisiejszych czasach zbyt ogólne. Ze względu na obecność komputerów w nieomal wszystkich dziedzinach naszego życia definiowanie tego zjawiska jedynie poprzez komputer jako narzędzie zamachu stało się zatem mało przejrzyste. Badacze zajmujący się omawianą problematyką, próbując określić istotę definiowanych przestępstw, coraz częściej odwołują się do technologii informacyjnych oraz telekomunikacyjnych, podkreślając w ten sposób związek tej formy przestępczości z sektorem ICT (*Informa-*

tion and Communication Technology). Jednak wielu z nich określa zakres znaczeniowy tych pojęć raczej w sposób intuicyjny, co znacznie utrudnia posługiwanie się nimi. Dlatego też zarówno w mowie potocznej, jak i tekstach naukowych znacznie częściej używa się określenia *cyberprzestrzeń* (Siwicki, 2013, s. 12–14).

Termin *cyberprzestępczość* jest rzadko stosowany w ustawodawstwie karnym ze względu na liczne wątpliwości terminologiczne. Trudno jest ustalić jednoznaczny zakres znaczeniowy tego pojęcia, ponieważ przestępczość ta ewoluuje wraz z postępem technologicznym. Stworzenie definicji przestępczości jest jednak wyjątkowo istotne nie tylko z punktu widzenia praktyki ścigania karnego czy kryminologii (Siwicki, 2013, s. 15), ale przed wszystkim dlatego, że będzie bezpośrednio oddziaływało na skuteczność międzynarodowego systemu do walki z przestępczością komputerową (Kulesza, 2010, s. 149).

Podjęto bardzo wiele prób zdefiniowania pojęcia *cyberprzestępczości*, a znaczący wkład w unifikację stosowanej terminologii miały inicjatywy legislacyjne podnoszone na forum takich organizacji, jak: Rada Europy, Organizacja Narodów Zjednoczonych czy Organizacja Współpracy Gospodarczej i Rozwoju (Siwicki, 2013, s. 17).

Na szczególną uwagę na gruncie prawa międzynarodowego zasługuje definicja wypracowana podczas X Kongresu ONZ w sprawie Zapobiegania Przestępczości i Traktowania Przestępców (Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders), wprowadzająca podział na:

– cyberprzestępstwo w sensie wąskim (przestępstwo komputerowe), obejmujące wszelkie nielegalne działania skierowane przeciwko bezpieczeństwu systemów komputerowych i elektronicznie przetwarzanych przez te systemy danych, wykonywane z wykorzystaniem operacji elektronicznych,

– cyberprzestępstwo w sensie szerokim (przestępstwo dotyczące komputerów) obejmujące wszelkie nielegalne działania, popełnione przy użyciu lub skierowane przeciwko systemom, czy sieciom komputerowym, włączając w to m.in. nielegalne posiadanie oraz udostępnianie lub rozpowszechnianie informacji za pomocą komputera bądź sieci (Siwicki, 2013, s. 17).

W komunikacie Komisji Europejskiej z 7 lutego 2013 r. stwierdzono, że pojęcie *cyberprzestępczości* „odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego". Zatem grupa czynów określana tym mianem to posługiwanie się sieciami telekomunikacyjnymi z zamiarem naruszenia jakiegokolwiek dobra chronionego przez prawo karne, co w praktyce można ograniczyć do trzech rodzajów zamachów. Pierwsza grupa obejmuje przestępstwa pospolite, najczęściej zagrażające bezpieczeństwu przetwarzanej informacji (np. oszustwo czy fałszerstwo dokumentów), które zostały popełnione z wykorzystaniem technologii

komputerowej. Drugi rodzaj stanowi publikacja w mediach elektronicznych treści zakazanych przez prawo – są to tzw. przestępstwa zawiązane z treścią informacji (np. materiały nawołujące do nienawiści rasowej bądź związane z seksualnym wykorzystywaniem dzieci). Ostatnią grupę tworzą przestępstwa polegające na wykorzystaniu sieci łączności elektronicznej w celu naruszenia dóbr chronionych przez prawo karne (np. ataki przeciwko systemom informatycznym oraz hackerstwo). Naruszenia te są szczególnie niebezpieczne, ponieważ mogą być skierowane przeciwko najważniejszym infrastrukturom krytycznym, a w konsekwencji okazać się dramatyczne w skutkach dla całego społeczeństwa (Bębas, Plis, Bednarek, 2012, s. 149).

Powyższa typologia nie jest wynikiem jednoznacznych kryteriów podziału. Przestępstwa te wyodrębniono na podstawie narzędzia użytego do ich popełnienia, a nie przedmiotu ochrony. Wspólną cechą tej kategorii czynów zabronionych jest powołanie się na sposób działania sprawcy – szeroko rozumianego prezentowania w sieciach elektronicznych informacji zakazanych przez prawo (Siwicki, 2013, s. 20), a także fakt, że mogą być popełnione na masową skalę, niezależnie od odległości dzielącej miejsce popełnienia przestępstwa od miejsca, w którym mają wystąpić skutki (Bębas i in., 2012, s. 149).

Podsumowując, *cyberprzestępczość* należy rozumieć jako przestępczość mającą miejsce w cyberprzestrzeni – przestrzeni przechowywania, przetwarzania oraz obrotu informacji tworzonej przez systemy elektroniczne, a przede wszystkim internet. W wąskim rozumieniu obejmuje jedynie takie zamachy, których zrealizowanie nie będzie możliwe poza cyberprzestrzenią, podczas gdy w szerokim ujęciu będzie to ogół zachowań przestępczych dokonanych z wykorzystaniem urządzeń teleinformatycznych (Kosiński, 2015, s. 88). Komputer może być zarówno celem przestępstwa, kluczowym elementem lub po prostu narzędziem koniecznym do jego popełniania. Niezależnie od zastosowania, użycie komputera umożliwia działanie z dużej odległości, często bez świadomości, gdzie faktycznie jest zlokalizowane urządzenie. Sprawca nie musi znajdować się w miejscu popełnienia przestępstwa, a dowody jego działania często mieszczą się w geograficznie odległej przestrzeni (Kulesza, 2010, s. 152–153).

Pojęcia *cyberprzestępstwa* nie wolno jednak utożsamiać z przestępstwami internetowymi, „w przypadku których usługi sieciowe (możliwości oferowane przez Internet) umożliwiły lub co najmniej ułatwiły sprawcy realizację zamierzonego czynu przestępnego albo jego poszczególnych stadiów" (Sowa, 2002, s. 62). O przestępczości internetowej możemy mówić jedynie wtedy, gdy bez wykorzystania sieci do popełnienia określonego czynu by nie doszło bądź jego dokonanie byłoby znacznie bardziej utrudnione.

Warto również zauważyć, że w przeszłości cyberprzestępczość była głównie kojarzona z osobami indywidualnymi. Dziś można jednak zaobserwować tendencję do współpracy organizacji przestępczych ze specjalistami z branży IT

z zamiarem popełnienia przestępstwa, często mającego na celu zdobycie funduszy na sfinansowania dalszych nielegalnych działań. Organizacje takie skupiają osoby z całego świata, co umożliwia popełnienie przestępstw na niespotykaną dotąd skalę. Przenoszą one swoją działalność do internetu, co znacznie ułatwia kierowanie grupą przestępczą oraz umożliwia zwiększenie zysków w stosunkowo krótkim czasie. Same przestępstwa nie zawsze są nowe – kradzież, oszustwa, nielegalny hazard, sprzedaż fałszywych leków – i ewoluują wraz z możliwościami, jakie daje internet, stając się coraz bardziej powszechne i szkodliwe.

Ustawodawstwo karne niektórych państw uznaje cyberprzestępstwo za odrębny rodzaj działania niezgodnego z prawem, lecz na gruncie prawa polskiego jest ono jedynie określane jako czyn zabroniony popełniony w obszarze cyberprzestrzeni i nie stanowi osobnej kategorii czynów karalnych. Regulacje dotyczące tej grupy przestępstw można zatem odnaleźć w kilku aktach normatywnych, w tym m.in. w Kodeksie karnym, przede wszystkim w rozdziale XXXIII Przestępstwa przeciwko ochronie informacji, w ustawie o ochronie danych osobowych czy ustawie o prawie autorskim i prawach pokrewnych.

Gwarantem efektywnego ścigania cyberprzestępczości jest stosowanie spójnych regulacji – bezprawnego zachowania, które miało miejsce w cyberprzestrzeni nie należy traktować jak wyjątkowej formy postępowania, niemieszczącej się w zakresie obowiązującego prawa. Jednak pewne cechy internetu, wyróżniające go spośród dotychczas znanych technologii, uzasadniają potrzebę opracowania nowych, adekwatnych regulacji czy też modyfikacji powszechnie stosowanych norm proceduralnych. Kluczową kwestią jest podjęcie działań w celu ochrony infrastruktury komputerowej, odpowiedzialnej za właściwe funkcjonowanie sieci globalnej. Najważniejszy jest jednak wzgląd na różnorodność tradycji i potrzeb społecznych oraz jurysdykcję krajową, jednocześnie pamiętając, że internet weryfikuje obowiązujące granice państwowe (Kulesza, 2010, s. 154–155).

Rodzaje przestępstw komputerowych

Jednym z głównych podziałów przestępczości komputerowej, obowiązującym w środowisku międzynarodowym, jest klasyfikacja Komitetu Ekspertów Rady Europy z 1989 r., który w oparciu o zalecenie nr R(89)9 Komitetu Ministrów Rady Europy utworzył raport przedstawiający minimalny i fakultatywny podział przestępstw, które powinny być regulowane przez ustawodawstwa krajów członkowskich. Podział ten jako pierwszy obligował wszystkie państwa członkowskie, zawierał on:

- oszustwa komputerowe,
- fałszerstwa komputerowe,
- nieuprawnione uzyskanie dostępu do systemu komputerowego,
- sabotaż komputerowy,
- bezprawne powielanie półprzewodników,
- zniszczenie programów albo danych komputerowych,

– piractwo komputerowe (*cybersquatting*),
– podsłuch komputerowy.

Lista fakultatywna zawierała takie czyny, jak:
– modyfikacja danych lub programów komputerowych,
– szpiegostwo komputerowe,
– korzystanie z komputera czy programu komputerowego bez odpowiedniego zezwolenia (Hołyst, 2007, s. 335).

Projekt Konwencji Rady Europy o Cyberbezpieczeństwie następująco definiuje *oszustwo komputerowe*: „wprowadzenie, zmiana, usunięcie lub zablokowanie danych komputerowych albo inna ingerencja w proces przetwarzania danych, w zamiarze przysporzenia sobie lub innej osobie nienależnej korzyści majątkowej". Definicja ta ma wiele cech wspólnych z ujęciem istoty oszustwa komputerowego w zaleceniu Rady Europy z 1989 r. także pod tym względem, że konstytuuje typ przestępstwa skutkowego. O dokonaniu oszustwa komputerowego, wg projektu konwencji, decyduje wywołanie skutku w postaci utraty własności przez osobę pokrzywdzoną przestępstwem. Jest to ujęcie węższe aniżeli to, które przyjął polski ustawodawca w art. 287 k.k., który przewiduje typ przestępstwa określany mianem *oszustwa komputerowego*. Istota tego czynu polega bowiem „na usiłowaniu uzyskania korzyści majątkowej lub spowodowania szkody przez manipulowanie zapisem na komputerowym nośniku informacji albo innym oddziaływaniu na automatyczne przetwarzanie informacji" (Adamski, 2001, s. 47–48).

Oszustwa komputerowe są uznawane za przestępstwa trudne do ścigania. Proces ujawniania, wykrywania, dowodzenia czy zapobiegania wymaga współdziałania organów ścigania i poszkodowanego przestępstwem komputerowym, który nie zawsze jest zainteresowany ujawnieniem słabości własnego systemu z uwagi np. na obawę utraty zaufania klientów.

Sabotaż komputerowy, inaczej ataki, których celem jest „spowodowanie zakłóceń w funkcjonowaniu systemów komputerowych lub całkowite zablokowanie ich działania" (Płoszyński, 2012, s. 46), stanowi obecnie jedną z bardziej rozpowszechnionych, także w polskim internecie kategorii zamachów na bezpieczeństwo elektroniczne przetwarzanej informacji. Zamachy te są wymierzone w dostępność informacji, czyli atrybut decydujący o zaufaniu do techniki komputerowej, a ich szkodliwość jest wprost proporcjonalna do stopnia zależności danej organizacji lub instytucji od technologii informatycznej.

Kodeks kamy z 1997 r. przewiduje następujące rodzaje przestępstw komputerowych:

1. Przestępstwa przeciwko ochronie informacji. Należą do nich: hacking komputerowy (art. 267 § 1 k.k.), podsłuch komputerowy –nieuprawnione przechwycenie informacji (art. 267 § 2 k.k.), bezprawne niszczenie informacji (art. 268 § 2 k.k.) oraz sabotaż komputerowy (art. 269 § 1 i 2 k.k.).

2. Przestępstwa przeciwko mieniu. Wymienić tu można: nielegalne uzyskanie programu komputerowego (art. 278 § 2 k.k.), paserstwo programu komputerowego (art. 293 § 1 k.k.), oszustwo komputerowe (art. 287 § 1 k.k.), oszustwo telekomunikacyjne (art. 285 § 1 k.k.) oraz kradzież karty bankomatowej (art. 278 § 5 k.k.).

3. Przestępstwa przeciwko bezpieczeństwu powszechnemu. Na uwagę zasługują następujące stany faktyczne: sprowadzenie niebezpieczeństwa dla życia i zdrowia wielu osób albo mienia w znacznych rozmiarach (art. 165 § 1 ust. 4 k.k.), nieumyślne zakłócenie automatycznego przetwarzania informacji związane ze sprowadzaniem niebezpieczeństwa powszechnego (art. 165 § 2 k.k.) oraz zamach terrorystyczny na statek morski lub powietrzny (art. 167 § 1 i 2 k.k.).

4. Przestępstwa przeciwko Rzeczypospolitej Polskiej: szpiegostwo albo wywiad komputerowy (art. 130 § 2 i 3 k.k.).

5. Przestępstwa przeciwko wiarygodności dokumentów: fałszerstwo dokumentów (art. 270 § 1 k.k.). Sprzęt komputerowy, oprogramowanie (skaner, drukarka) może służyć do fałszowania pewnych części dokumentu, takich jak podpis, data, lub do wykonania jego nielegalnych kopii.

Wymienić należy także formy piractwa komputerowego wg ustawy z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2002 r., nr 80, poz. 904 ze zm.):

– przywłaszczenie autorstwa lub wprowadzenie w błąd co do autorstwa całości lub części utworu (art. 115 ust. 1),

– rozpowszechnianie cudzego utworu (programu) bez podania nazwiska lub pseudonimu twórcy (art. 115 ust. 2),

– rozpowszechnianie bez upoważnienia albo wbrew jego warunkom cudzego programu (art. 116 ust. 1),

– utrwalanie lub zwielokrotnianie bez uprawnienia lub wbrew jego warunkom cudzego programu (art. 117 ust. 1),

– paserstwo przedmiotu będącego nośnikiem programu (art. 118),

– uniemożliwienie lub utrudnienie wykonywania prawa do kontroli korzystania z programu (art. 119).

W zakres przestępczości komputerowej wchodzi także m.in. nielegalne kopiowanie układów scalonych, zabronione przez ustawę z 30 marca 2002 r. – Prawo własności przemysłowej (t.j. Dz.U. z 2003 r., nr 119, poz. 1117). Ustawa ta przez topografię układu scalonego rozumie rozwiązanie polegające na przestrzennym, wyrażonym w dowolny sposób, rozplanowaniu elementów, z których co najmniej jeden jest elementem aktywnym, oraz wszystkich lub części połączeń układu scalonego.

Raport przygotowany na zlecenie Unii Europejskiej podaje internet jako przykład świadczący o umiejętnościach oszustów w zakresie stosowania osią-

gnięć nauki i techniki, dzięki którym powstają nowoczesne formy międzynarodowych oszust komputerowych. Zalicza się do nich:

– występowanie pod cudzym nazwiskiem,

– kradzież informacji (stanowiącej tajemnicę bankową) z elektronicznych środków przekazu,

– oszustwa związane z bankowością (np. uzyskiwanie drogą elektroniczną informacji identyfikujących właścicieli kont i ich salda),

– oszustwa związane z elektronicznym hazardem (loterią),

– piramidy finansowe w poczcie elektronicznej (organizacje reklamujące się jako firmy inwestycyjne, a w rzeczywistości korzystające z tzw. mechanizmów piramidy finansowej, której działanie opiera się na wpłaceniu osobom, które wcześniej przystąpiły do przedsięwzięcia, zysków z wpłat dokonanych przez nowych uczestników).

Przepisy karne dotyczące przestępczości komputerowej zawarte są także w innych ustawach. Wskazać należy tutaj następujące akty: 1) ustawę z 1994 r. o prawie autorskim i prawach pokrewnych, 2) ustawę z 1997 r. o ochronie danych osobowych, 3) ustawę z 2001 r. o podpisie elektronicznym,4) ustawę z 2002 r. o świadczeniu usług drogą elektroniczną, 5) ustawę z 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Hołyst, 2007, s. 336–337).

Podsumowanie

Rozwój nowoczesnych technologii, które już na dobre zagościły w naszym codziennym życiu, wpłynął także na sferę związaną z przestępstwami komputerowymi. Przestępczość komputerowa staje się coraz bardziej powszechna. Wynika to z ogólnego niezrozumienia wagi problemu i istoty zabezpieczeń oraz z braku świadomości tego, w jaki sposób należy radzić sobie z nowo powstającymi zagrożeniami w internecie. Wzrost komercjalizacji cyberprzestrzeni, różnice w polityce internetowej różnych krajów, odmienność przepisów i praktyk w zakresie zwalczania i zapobiegania przestępstwom komputerowym pociągają za sobą trudności w egzekwowaniu prawa na poziomie międzynarodowym. Ataki w cyberprzestrzeni powodują, że odpowiedzialność organów ścigania i instytucji zajmujących się bezpieczeństwem kraju zaczyna się zacierać, wywołując tym samym konieczność wypracowania nowszych form współpracy. Rosnący poziom zagrożenia wynikającego z coraz częstszego wykorzystywania komputerów i sieci do przestępstw komputerowych wyraźnie stawia nowe wyzwania dla krajowych organów ścigania oraz organizacji międzynarodowych. Błędne jest jednak mniemanie, że te problemy da się przezwyciężyć. Tylko proces edukacji i koordynacji działań zarówno na poziomie krajowym, jak i międzynarodowym oraz regularny przegląd i aktualizacja przepisów sprawią, że egzekwowanie prawa w jakimś stopniu będzie nadążało za zmianami technologicznymi. Tylko

przez przyjęcie strategicznego podejścia do zarządzania zmianą w zakresie stosowania prawa będziemy mogli czerpać korzyści z życia w dobie nowoczesnych technologii, nie narażając się niepotrzebnie na działania cyberprzestępców.

Literatura

Adamski, A. (2000). *Prawo karne komputerowe*. Warszawa: C.H. Beck.

Adamski, A. (2001). *Przestępczość w cyberprzestrzeni*. *Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*. Toruń: TNOiK.

Bębas, S., Plis, J., Bednarek, J. (red.) (2012). *Patologie w cyberświecie*. Radom: WSH.

Hołyst, B. (2007). *Kryminalistyka*. Warszawa: LexisNexis.

Jakubski, K.J. (1996). Przestępczość komputerowa – zarys problematyki. *Prokuratura i Prawo, 12*, 34–50.

Kosiński, J. (2015). *Paradygmaty cyberprzestępczość*. Warszawa: Difin.

Kulesza, J. (2010). *Międzynarodowe prawo internetu*. Poznań: Ars boni et aequi.

Płoszyński, Z. (2012). Przestępczość internetowa. *Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa, 3*, 31–56.

Siwicki, M. (2013). *Cyberprzestępczość*. Warszawa: C.H. Beck.

Sowa, M. (2002). Odpowiedzialność karna sprawców przestępstw internetowych. *Prokuratura i Prawo, 4*, 62–79.