Bezpieczeństwo w sieci jako problem pedagogiczny

Mgr Agata Jakieła

Ur. 18 kwietnia 1987 w Krośnie. Absolwentka II Liceum Ogólnokształcącego im. Konstytucji 3 Maja w Krośnie. Magister prawa na Wydziale Prawa i Nauk o Gospodarce oraz IV roku socjologii na Wydziale Zamiejscowym Nauk o Społeczeństwie KUL w Stalowej Woli, wolontariusz Akademickiego Biura Porad Prawnych, Prezes Stalowowolskiego Koła Naukowego Studentów Prawa Viribus Unitis. Zainteresowania: prawo cywilne, prawo konstytucyjne.

1. SŁOWO WSTĘPNE

Społeczeństwo informacyjne to domena XXI wieku, to droga ciągłego rozwoju nowoczesnych technologii i patentów, wyścig wielkich koncernów w poszukiwaniu nowych rozwiązań. Do urzeczywistnienia tych dążeń społeczeństwo posłużyło się Internetem, dzięki któremu granice ludzkiego komunikowania uległy zatarciu, a bariery przestrzenne i czasowe zostały obalone, tworząc zjawisko określane dzisiaj jako globalna wioska. Internet stwarza możliwości usług bankowych, transakcji handlowych, sieci komunikacyjnych co wiąże się z przetwarzaniem ogromnej ilości informacji, która niewątpliwie stanowi najważniejszy zasób gospodarczy, kulturowy i naukowy. Sieć internetowa stała się dzisiaj nieodłącznym elementem sprawnie funkcjonującego społeczeństwa informacyjnego.

Sługa Boży Jan Paweł II w orędziu na XXXVI Światowy Dzień Środków Masowego Przekazu porównał Internet do rzymskiego forum, które było miejscem otwartym dla szerokiego ogółu obywateli (…) w którym toczyło się życie społeczne, gdzie na światło dzienne wychodziły najlepsze i najgorsze strony natury ludzkiej. Forum było zatłoczoną i tętniącą życiem przestrzenią w środku miasta, miejscem, które odzwierciedlało kulturę otaczającego środowiska, a jednocześnie tworzyło własną kulturę. W nie mniejszym stopniu dotyczy to również cyberprzestrzeni, która jest niejako nowym horyzontem, (…) który kryje niebezpieczeństwa i obietnice[1]. Tak pojmowany Internet stanowił będzie źródło wiedzy i informacji, „tętniącą życiem przestrzenią", która przyczyni się do rozwoju duchowego i materialnego społeczeństwa. Jan Paweł II obok obietnic, które mają bardzo pozytywny wydźwięk wspomina o niebezpieczeństwach i zagrożeniach, mogących przybrać różne formy, doprowadzając do realizacji znamion czynu zabronionego – do przestępstwa. Dlatego też, bezpieczeństwo w sieci jest dzisiaj, tak istotne. Ma ono charakter podmiotowy. Stanowi także podstawową potrzebę grup społecznych i państw. Obejmuje zaspokojenie takich potrzeb jak: istnienie, przetrwanie, całość, tożsamość (identyczność), niezależność, spo-

[1] Jan Paweł II, *Internet: Nowe forum głoszenia ewangelii, Orędzie Jana Pawła II na XXXVI Światowy Dzień Środków Masowego Przekazu*, Watykan 2002, http://www.opoka.org.pl/biblioteka/W/WP/jan_pawel_ii/przemowienia/internet_aut_12052002.html (29.03.2011 r.)

kój, posiadanie i pewność rozwoju. Brak bezpieczeństwa powoduje niepokój i poczucie zagrożenia[2].

2. INTERNET – NARZĘDZIE PRZESTĘPSTWA

Dopóki Internet był wyłączną domeną uczonych, a potem także relatywnie nielicznych amatorów sieciowej komunikacji, dopóki był całkowicie oderwany od jakiejkolwiek działalności komercyjnej – był on obszarem w którym prawo nie było potrzebne[3]. Diametralna zmiana nastąpiła, gdy w Internecie pojawiła się działalność komercyjna. Gdy mowa o pieniądzach – kończą się żarty, znika wyrozumiałość dla ludzkich słabostek albo poszanowanie dla czyjeś odmienności. W sprawach biznesowych przesyłana informacja musi być pewna, bezpieczna, nienaruszalna i niezaprzeczalna[4]. Gdy tych cech brakuje tworzą się idealne warunki do rozwoju przestępczości internetowej. Mimo licznych systemów zabezpieczeń sieci komputerowych przed interwencją osób z zewnątrz oraz środków represyjnych dla sprawców internetowych przestępstw, ich liczba ciągle rośnie. Wykorzystanie Internetu jako narzędzia przestępstwa jest niezwykle niebezpieczne, z uwagi na dużą liczbę potencjalnych ofiar, których może ono dotyczyć. Identyfikacja internetowych przestępców jest utrudniona, ponieważ nie pozostawiają oni po sobie typowych fizycznych śladów obecności np. w postaci odcisków palców, próbek DNA czy innego rodzaju dowodów. Dlatego też cyberprzestrzeń stwarza możliwość zachowania anonimowości, co w konsekwencji prowadzi do poważnych utrudnień w odnalezieniu przestępcy. Nie można jednak mówić, o pełnej i nieograniczonej anonimowości, ponieważ jej istnienie wykluczyłoby niemal całkowicie możliwość wykrycia sprawców, a tym samym utwierdziłoby ich w poczuciu bezkarności a społeczeństwo o niemocy organów ścigania. Spora liczba komputerowych przestępców, pozostawia po sobie ślad w postaci numeru IP, który pozwala na identyfikację miejsca popełnienia przestępstwa, co jednak nie wskazuje bezpośrednio na jego sprawcę.

Przestępstwem komputerowym jest zachowanie przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające na naruszeniu uprawnień do programu komputerowego godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze, cały system połączeń komputerowych a także w sam komputer[5]. Do głównych przestępstw komputerowych, które wskazuje Kodeks karny[6] należy zaliczyć oszustwo komputerowe z art. 287 KK, fałszerstwo komputerowe z art. 270 KK, utrudnianie lub uniemożliwianie dostępu do informacji w tym *hacking* czyli bezprawne uzyskanie informacji określone w art. 267 § 1 KK., dalej szpiegostwo komputerowe 130 § 3 KK, przestępstwa karne skarbowe, piractwo komputerowe 278 § 2 KK. Doktryna i nauka prawa podzieliła te przestępstwa na przestępstwa komputerowe przeciwko ochronie informacji, przestępstwa komputerowe przeciwko wiarygodności dokumentów, obrotowi gospodarczemu i pieniężnemu oraz przestępstwa komputerowe przeciwko mieniu. Artykuł skupia uwagę przede wszystkim na ostatniej grupie przestępstw a mianowicie przestępstw komputerowych przeciwko mieniu, w kon-

[2] B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, Prokuratura i Prawo 2011, nr 1, s. 11.

[3] R. Tadeusiewicz, *Społeczność Internetu*, Warszawa 2002, s. 68.

[4] Tamże, s. 69.

[5] K. Baniuk, *Wielka encyklopedia prawa*, Białystok-Warszawa 2000, s. 475.

[6] Ustawa z dnia 6 czerwca 1997 r., Kodeks Karny, Dz. U. 1997, nr 553, poz. 88, ze zm.

tekście zagadnień *de lege lata* oraz postulatów na płaszczyźnie *de lege ferenda*.

3. KRADZIEŻ PROGRAMU KOMPUTEROWEGO

Prawo własności oraz inne prawa majątkowe, muszą być należycie chronione nie tylko przez przepisy prawa cywilnego, ale również w głównej mierze przez przepisy prawa karnego. Art. 278 § 2 wskazuje na kradzież programu komputerowego, która polega na uzyskaniu bez zgody uprawnionej cudzego programu komputerowego, w celu osiągnięcia korzyści majątkowej. Obejmuje zarówno zabór nośnika, jak i skopiowanie programu na inny nośnik[7]. Od kradzieży rzeczy ruchomej różni się przedmiotem czynności wykonawczej, określeniem czynności sprawczej, ale także tym że sprawca zawsze działa w celu osiągnięcia korzyści majątkowej[8]. Przepis ten, chroni własność, posiadanie lub inne prawa rzeczowe albo obligacyjne do programu komputerowego. Przedmiotem ochrony są prawa majątkowe twórcy i prawnego użytkownika programu, a jako przedmiot uboczny prawa autorskie twórcy.

Przez program komputerowy rozumieć należy zakodowany na odpowiednim nośniku informacji zapis składający się na utwór przedstawiający wartość materialną[9]. Przestępstwo to jest przestępstwem powszechnym, w którym sprawcą może być każda osoba spełniająca warunki do bycia podmiotem w rozumieniu prawa karnego, a więc posiadająca zdolność do zawinienia (osoba, która popełniając czyn miała ukończone 17 lat). Wskazując na znamiona określające czynność sprawczą tego przestępstwa, należy skupić się pojęciu „uzyskanie" [bez gody osoby uprawnionej cudzego program], Oznacza ono wszelką formę przejęcia programu komputerowego bez zgody jego dysponenta, w taki sposób, który możliwa wykorzystanie tego programu przez osobę nieuprawnioną. W tym znaczeniu uzyskanie programu komputerowego oznacza przejęcie nośnika informacji, na którym zakodowany jest program, jak i wszelkie formy nielegalnego kopiowania programów komputerowych bez zgody ich dysponenta, przy jednoczesnym zachowaniu pierwotnej wersji informacji kodującej program we władaniu i dyspozycji osoby uprawnionej[10].

Uzyskanie programu komputerowego następuje w sposób identyczny, jak w przypadku kradzieży rzeczy, wbrew woli osoby która jest jej właścicielem. W przypadku, gdy sprawca przy sporządzaniu kopii programu komputerowego, łamie specjalistyczne zabezpieczania, zainstalowane na nośniku informacji, na którym zapisany jest dany program, ponosił będzie odpowiedzialność za przestępstwo określone w art. 279 § 1 KK tj. Kradzież z włamaniem. Kradzież programu komputerowego jest przestępstwem materialnym. Skutek określany jako znamię przestępstwa z art. 278 § 2 występuje w momencie objęcia przez sprawcę w posiadanie nośnika informacji z zakodowanym programem komputerowym. Do jego nastąpienia nie jest konieczne jakiekolwiek następcze działanie sprawy w stosunku do tego programu, zwłaszcza zaś jego uruchomienie przy pomocy odpowiedniego urządzenia lub wykorzystywanie[11].

[7] A. Grześkowiak, *Prawo karne*, Warszawa 2007, s. 371.

[8] M. Budyń – Kulik, P. Kozłowska – Kalisz, M. Kulik, M. Mozgawa, *Kodeks karny*, Praktyczny komentarz, Warszawa 2010, s. 574.

[9] M. Dąbrowska – Kardas, P. Kardas [w:] A. Zoll, *Kodeks Karny, Część szczególna, komentarz*, t. III, Zakamycze 2006, s. 31.

[10] M. Dąbrowska – Kardas, P. Kardas, op. cit., s. 64

[11] Tamże, s. 66.

Sprawca działając w zamiarze bezpośrednim, musi być w pełni świadomy i wyrażać chęć uzyskania programu komputerowego bez zgody osoby uprawnionej, dodatkowo czyniąc to w przekonaniu, że chce przy tym osiągnąć korzyść majątkową. Jeżeli chociażby jeden z elementów znamion strony przedmiotowej nie jest objęty świadomością sprawcy, nie są spełnione podmiotowe warunki odpowiedzialności za kradzież programu komputerowego, bowiem w takim przypadku sprawca nie tyle chce popełnić opisane w tym typie przestępnym zachowanie, co jedynie na jego wypełnienie się godzi[12]. Stanowisko to jest zgodne z linią orzeczniczą SN. Ustawodawca mając na uwadze rangę przestępstwa, ochronę własności, praw autorskich, jak również bezpieczeństwo w sieci komputerowej, dostosował granice zagrożenia karą oraz środki karne za popełnienie przestępstwa z art. 278 § 2, które jest zagrożone karą pozbawienia wolności od 3 miesięcy do 5 lat. Sąd na podstawie art. 58 § 3 może wymierzyć grzywnę lub karę pozbawienia wolności, przy jednoczesnym orzeczeniu środka karnego. Możliwość zamiany przewidzianej za to przestępstwo kary pozbawienia wolności na grzywnę albo karę ograniczenia wolności nie odnosi się do sprawcy występku umyślnego, uprzednio skazanego na karę pozbawienia wolności na czas nie krótszy niż 6 miesięcy bez warunkowego zawieszenia jej wykonania[13]. W przypadku skazania sąd orzeka przepadek przedmiotów pochodzących z przestępstwa, chyba, że podlegają one zwrotowi pokrzywdzonemu lub innemu podmiotowi (art. 44 KK)[14].

Niestety takie zagrożenie karą skutecznie nie zwalcza plagi nielegalnego oprogramowania, które jest zjawiskiem powszechnym w wielu krajach Europejskich. Jak wynika z badań przeprowadzonych w 2007 roku przez Bussines Softwere Alliance[15], co piąty przedstawiciel małego i średniego przedsiębiorstwa nie dostrzega żadnego zagrożenia z nielegalnego oprogramowania. W Polsce 64 % szefów ankietowanych firm nie ma całkowitej pewności czy używane oprogramowanie jest całkowicie legalne, nie zdając sobie sprawy, jakie ryzyko niesie używanie nielegalnego oprogramowanie tak na płaszczyźnie prawno – finansowej jak również dla samego systemu operacyjnego. Należy w tym momencie wskazać najczęstsze zagrożenia, jakie stwarza używanie nielegalnego oprogramowania ściągniętego od nieznanego dostawcy, należą do nich przede wszystkim możliwość utraty, wycieku danych, samoczynne instalowanie wirusów, trojanów oraz programów szpiegujących, bardzo istotne z punku widzenia prawa naruszenie prawa autorskiego, co w konsekwencji doprowadzi do postępowania karnego. Według tego samego badania w Polsce stopa piractwa wynosi ok. 58 % (dla porównania średnia w Europie waha się w okolicach 38%). Te dane wskazują na bardzo dużą tolerancję Polaków dla tego typu przestępstwa. Dodatkowo na podstawie tych danych można stwierdzić brak skuteczności organów ścigania, jak również niedociągnięcia ustawodawcze, które nie przyczyniają się do walki z tą przestępczością. Daje to podstawy ku temu, by twierdzić, że problem zachowania bezpieczeństwa w sie-

[12] Por. Wyrok SN z dnia 22 listopada 1973 r., III KR 278/73, OSNPG 1974, nr 7, poz. 81.

[13] M. Dąbrowska – Kardas, P. Kardas, op. cit., s. 60.

[14] Z. Ćwiąkalski, P. Kardes, J. Majewski, J. Raglewski, M. Szewczyk, K. Wróbel, A. Zoll, *Kodeks karny, cześć ogólna, Komentarz, wyd. II*, s. 709.

[15] Wszelkie dane dotyczące badania zaczerpnięte ze strony: http://www.egospodarka.pl/21748,Firmy-i-nielegalneprogramowanie,1,39,1.html (29.03.2011 r.)

ci to jedno a kodeksowe przepisy to drugie. Ponadto jednostkowe, mające charakter incydentalny interwencje organów ścigania, stanowią chwilowy hamulec przeciwko rozprzestrzenianiu się nielegalnego oprogramowania. Stałe monitorowanie przedsiębiorców, jak również osób fizycznych w znacznym stopniu obniżyłoby skalę tego przestępstwa a tym samym zaowocowałoby zwiększeniem bezpieczeństwa w sieci oraz poszanowania prawa autorskiego.

4. OSZUSTWO KOMPUTEROWE

Kolejnym bardzo ważnym przestępstwem komputerowym przeciwko mieniu jest oszustwo komputerowe z art. 287 KK, które polega na wykonaniu, bez upoważnienia, przynajmniej jednej z czynności polegających na: wpływaniu na wpływaniu na automatycznie przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, zmianie, usuwaniu lub wprowadzeniu nowego zapisu danych informatycznych[16]. Jest to czyn zagrożony karą pozbawienia wolności do 3 miesięcy do 5 lat. W sprawach mniejszej wagi sąd może wymierzyć karę grzywny, ograniczenia wolności lub pozbawienia wolności do roku. Czynem zabronionym jest tutaj wpływanie na komputerowe zapisy informacji. Jest to przestępstwo kierunkowe wymagające dla swej realizacji zabarwienia woli celem, motywem lub pobudką, w przypadku tego przestępstwa celem będzie osiągniecie korzyści materialnej rozumianej zgodnie z art. 115 § KK. Przykładem takiego przestępstwa będzie włamanie się w systemu operacyjnego banku X i wydanie określonych dyspozycji wykonania przelewu na rachunek sprawcy. Jest to przestępstwo powszechne, według regulacji kodeksowej sprawcą może być każdy, każdy kto posiądzie umiejętności i według żargonu komputerowego stanie się *cracerem* - to osoba, zajmuje się łamaniem zabezpieczeń komputerowych w sposób niezgodny z prawem. Krakera nie można utożsamiać z hakerem.

Dr Andrzej Kmiecik, badający działalność grup hakerskich i krakerskich w USA określił hakera jako miłośnika komputerów, posiadającego zaawansowane umiejętności programowania, znajdujący luki w systemach, ciągle zdobywający nową wiedzę i dzielący się nią z innymi, nigdy nie niszczący celowo danych[17]. Kraker posiada podobne umiejętności, jednak celowo przyczynia się do powstawania problemów w komputerze, do którego się włamał, kierując się złymi pobudkami. Dlatego w kontekście oszustwa komputerowego sprawcą będzie kraker.

Sprawca oszustwa komputerowego może działać w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, będzie to wiązało się ściśle z pobudkami danego sprawcy oraz jego zamiarem. Zaś szkoda majątkowa rozpatrywana będzie w kontekście uszczerbku, ale i również utraconych korzyści. Praktyka wykazała, że na tą czynność sprawczą składają się różnego rodzaju manipulacje komputerowe podłączenie się do systemu przesyłania informacji i przy tym modyfikacja jej treści, uszkodzenie serwera, który służy do przesyłu zakodowanych informacji jak np. w przypadku poczty elektronicznej.

Jednym z najbardziej wyrafinowanych działań, które stanowią ogromne zagrożenia dla bezpieczeństwa w sieci, który może zagrażać mieniu jest tzw. *phishing*[18], który polega na tworzeniu duplikatów stron

[16] A. Grześkowiak, *Prawo karne*, Warszawa 2007, s. 371 – 372.

[17] A. Kmiecik, *Postawy etyczne hakera i krakera*, [w:] M. Sokołowski (red.), *Media i edukacja w globalizującym się świecie*, Olsztyn 2003, s. 461 i n.

[18] http://pl.wikipedia.org/wiki/Phishing (29.03.2011 r.)

www banków i innych urzędów, w celu wydobywania numerów kart bankowych, wiadomości o kontach bankowych itp. Fałszywe strony oraz emaile do złudzenia przypominają oryginalne[19]. Prawne uregulowania dotyczące walki z tego typu działaniami przestępczymi zostały szczegółowo uregulowane w Ustawie z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną[20].

5. PASERSTWO KOMPUTEROWE

Paserstwo komputerowe, to przestępstwo komputerowe, które penalizują zachowania polegające na nabyciu, przyjęciu, pomocy do zbycia lub pomocy do ukrycia programu komputerowego uzyskanego za pomocą czynu zabronionego, do których stosuje się regulacje dotyczące paserstwa.

W przypadku wykrycia przestępstwa komputerowego naruszającego bezpieczeństwo w sieciach komputerowych, podstawą każdego postępowania w sprawie są przepisy Kodeksu postępowania karnego[21]. W pierwszym etapie następuje stwierdzenie, że bezpieczeństwo sieciowe zostało naruszone, gdzie znaczną rolę odgrywa pokrzywdzony, które powinno się ograniczyć do zawiadomienia organów ścigania, każda inna interwencja może doprowadzić do przypadkowego zatarcia śladów. W kolejnym etapie następuje gromadzenie zabezpieczanie materiałów dowodowych, co w rezultacie doprowadzi do procesu.

6. ZAKOŃCZENIE

Surfując po Internecie mało kto zdaje sobie sprawę z zagrożeń jakie nań czekają. Wielość stypizowanych przestępstw komputerowych wskazuje na ludzką wyobraźnię i zdolności i determinację. Motywem stojącym zwykle za poczynaniami przestępców jest (wspominana przeze mnie) nadzieja zysku. Chęć odniesienia korzyści powoduje, że aby osiągną cel, stosują wszelkie środki – od napadów i włamań, po kradzież informacji i penetrację sieci. Kiedy połączy się motywacja przestępcy i umiejętności zdolnego hakera, powstaje profesjonalny złodziej[22]. Takie osoby, jak już zostało wspomniane potrafią wykradać programy komputerowe, numery kart kredytowych w sposób nielegalny wchodzić w systemy operacyjne danych przedsiębiorstw, banków, czy instytucji. A biorąc pod uwagę wartość aktywów ulokowanych na rachunkach bankowych i numery kart kredytowych, które są udostępniane w sieci, nie dziwi mnogość przestępców oraz niepokój przedstawicieli biznesu sieciowego. Odpowiedzialność za tego typu przestępstwa powinna być w sposób szczególny egzekwowana. Inaczej sieć stanie się śmietnikiem, którego używanie będzie nie do przyjęcia dla zwykłych uczciwych ludzi, natomiast którego nadużywanie będzie domeną różnego kalibru przestępców[23]. Powszechnie jest również wiadome, że każdy, kto kiedykolwiek próbował coś zabezpieczyć (czy to dom, czy sieć komputerową, zdaje sobie sprawę, że ostatecznie bez znaczenia jest to, jak wiele zamków i kamer zastosujesz, czy jak wielu strażników zatrudnisz, bo to użytkowników (społeczności mieszkającej w budyn-

[19] G. Penkowska, *Człowiek i komputer, Zbiór esejów*, Gdańsk 2005, s. 103.

[20] Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną, Dz. U. 2002, nr 144, poz. 1204 ze zm.

[21] Ustawa z dnia 6 czerwca 1997 r., Kodeks postępowania karnego, Dz. U. 1997, nr 87, poz. 555, ze zm.

[22] E. Schetina, K. Green, J. Carlson, *Bezpieczeństwo w sieci, 2002,* s.22

[23] R. Tadusiewicz, op. cit., s. 71.

[24] E. Schetina, K. Green, J. Carlson, op. cit. s. 83.

ku, czy używanej sieci) będzie zależeć jak przydatne okażą się te zabezpieczenia[24]. „Czy książka jest dobra czy zła? Jeśli zatytułowana jest „Mein Kampf", to jest zła, jeśli Biblia, to dobra. Tak samo jest z Internetem: to narzędzie, które w wielu wypadkach zmieniło nasze życie, naszą zdolność dokumentacji, komunikacji itd."[25]. Niestety w innych przypadkach stanowi źródło zła, które prowadzi do przestępstwa.

STRESZCZENIE

Współczesne społeczeństwo informatyczne żyjące w XXI wieku, którego domeną jest Internet, zostało narażone na liczne komputerowe przestępstwa. Kodeks karny typizuje je w kilka grup. Jedną z nich są przestępstwa komputerowe przeciwko mieniu. Stanowią one zagrożenie nie tylko dla internetowego obrotu gospodarczego, ale i również dla prawa własności i innych praw rzeczowych. Dlatego dzisiaj należy kłaść szczególny nacisk na ochronę bezpieczeństwa internetowego, by zapewnić płynność i spokojny rozwój nowoczesnych technologii. Zadaniem ustawodawcy jest stworzenie takiego prawa, które skutecznie zwalczy cyberprzestępczość.

SUMMARY

Modern information society living in the twenty-first century, whose domain is the Internet, is constantly being exposed to a number of computer crimes. Penal Code categorizes such crimes into several groups. One of the crime groups are computer crimes against property. Such crimes pose a danger not only to online business transactions, but also to property rights. That is why we should pay special attention to Internet security protection to ensure smooth and peaceful development of modern technology. The task of the legislator is to create a law that will effectively overcome cybercrimes.

BIBLIOGRAFIA:

Akty prawne:

Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną, Dz. U. 2002, nr 144, poz. 1204 ze zm.

Ustawa z dnia 6 czerwca 1997 r., Kodeks Karny, Dz. U. 1997, nr 553, poz. 88, ze zm/

Ustawa z dnia 6 czerwca 1997 r., Kodeks postępowania karnego, Dz. U. 1997, nr 87, poz. 555, ze zm.

Baniuk K., *Wielka encyklopedia prawa*, Białystok-Warszawa 2000,

Budyń – Kulik M., Kozłowska – Kalisz P., Kulik M., Mozgawa M,, *Kodeks karny*, Praktyczny komentarz, Warszawa 2010,

Grześkowiak A., *Prawo karne*, Warszawa 2007,

Penkowska G., *Człowiek i komputer, Zbiór esejów*, Gdańsk 2005,

Schetina E., Green K., Carlson J., *Bezpieczeństwo w sieci*, 2002,

Sokołowski M., *Media i edukacja w globalizującym się świecie*, Olsztyn 2003,

Tadeusiewicz R., *Społeczność Internetu*, Warszawa 2002,

Zoll A., *Kodeks Karny, Część szczególna, komentarz*, t. III, Zakamycze 2006.

B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, Prokuratura i Prawo 2011, nr 1,

http://pl.wikipedia.org,

http://pl.wikiquote.org,

http://www.egospodarka.pl,

http://www.opoka.org,

Wyrok SN z dnia 22 listopada 1973 r., III KR 278/73, OSNPG 1974, nr 7, poz. 81.

[25] U. Eco w rozmowie z Vicentym Verdu, „El Pais", tłum. „Forum", 24 maja 2010, http://pl.wikiquote.org/wiki/Umberto_Eco (29.03.2011 r.)