Wojciech Lis
Lublin

Słowa kluczowe: swoboda komunikowania się, rzeczywistość sieciowa, ochrona informacji, przestępczość internetowa

Key words: mitigation of communication, network reality, information protection, Internet crime

BEZPIECZEŃSTWO W CYBERPRZESTRZENI W UJĘCIU PRAWNOKARNYM – WYBRANE ZAGADNIENIA

Współczesny sposób komunikowania się i przekazywania informacji pod każdym względem uległ zasadniczej zmianie z uwagi na możliwości, jakie daje globalna sieć. Internet nie tylko umożliwia komunikowanie się na odległość w czasie rzeczywistym, lecz także dostęp do wszelkiego rodzaju w zasadzie niczym nielimitowanych informacji. Co więcej, wyzwala aktywność jego użytkowników, pozwala angażować się w różnego rodzaju inicjatywy, wypowiadać na każdy temat, wpływać na procesy decyzyjne państw i rządów. W kontekście dynamicznego rozwoju Internetu tradycyjne środki masowego przekazu zeszły na dalszy plan. Pojawienie się Internetu otworzyło nowe, nieznane wcześniej możliwości dla nauki, gospodarki, kultury, polityki. Zalety Internetu są niewątpliwe. Niestety, korzystanie z niego nie jest wolne od niebezpieczeństw; może on wyrządzić także wiele szkód jego użytkownikom. Nie należy bowiem zapominać, że dokonana pod wpływem Internetu rewolucja informatyczna jest nie tylko ogromną szansą, lecz także ogromnym zagrożeniem, którego skalę chyba nie w pełni sobie uświadamiamy. Internet, jako nowa płaszczyzna spotykania się ludzi, jest ogromnie popularny ze względu na swoją funkcjonalność, natomiast niewielką wagę przywiązuje się do bezpiecznego korzystania z możliwości, jakie stwarza; wydaje się, że aspekty bezpieczeństwa jakby nie do końca są dostrzegane. Tymczasem rozpiętość przestępstw popełnianych za pośrednictwem Internetu jest bardzo szeroka i niezwykle zróżnicowana. Zwalczaniu przestępstw popełnianych za pośrednictwem Internetu oraz zamachów na systemy komputerowe i sieci informatyczne służy kryminalizacja niektórych zachowań. Wiele z nich zostało przeniesionych do cyberprze-

strzeni bezpośrednio z codziennego życia, inne są ściśle związane ze specyfiką Internetu. Te najbardziej niebezpieczne zostały stypizowane w ustawie Kodeksu karnego z 6 czerwca 1997 r.[1], który wyznacza granice swobodnego poruszania się w cyberprzestrzeni. Przepisy karne, które znajdują zastosowanie w odniesieniu do przypadków łamania prawa przez użytkowników Internetu, zawarte są także w wielu innych ustawach, w tym przede wszystkim w ustawie z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[2], określającej zasady odpowiedzialności karnej z tytułu naruszenia praw autorskich.

Należy zauważyć, że na gruncie normatywnym brak jest jednej powszechnie uznanej definicji przestępczości internetowej, która nieodzownie wiąże się z wykorzystaniem komputera. Najbardziej odpowiednia, w kontekście podjętych rozważań, wydaje mi się ta, która obejmuje wszelkie zachowania przestępne mające związek z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak również na bezpośrednim godzeniu w przetwarzaną informację, jej nośnik oraz obieg w komputerze, a także w cały system połączeń komputerowych, a wreszcie i w sam komputer. Będą to więc czyny popełniane z użyciem elektronicznych systemów przetwarzania danych, jak również skierowane przeciwko takiemu systemowi[3].

Analiza wszystkich tak rozumianych przestępstw, ujętych w Kodeksie karnym, przekracza możliwości niniejszego artykułu, który ma charakter poglądowy, a jego celem jest uświadomienie skali zagrożeń związanych z użytkowaniem Internetu. Niemniej jednak można wskazać grupę przestępstw, które pojawiają się najczęściej, zagrażając nie tylko bezpieczeństwu użytkowników Internetu, ale także i państwu.

Przestępstwo nielegalnego pozyskania informacji, o którym mowa w art. 267 § 1 kk, sprowadza się do uzyskania, bez uprawnienia, dostępu do informacji dla sprawcy nieprzeznaczonej, w wyniku otwarcia zamkniętego pisma, podłączenia się do sieci telekomunikacyjnej lub przełamania albo ominięcia elektronicznych, magnetycznych, informatycznych lub innych szczególnych jej zabezpieczeń. Karalne jest także uzyskanie, bez uprawnienia, dostępu do całości lub części systemu informatycznego; zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem w celu uzyskania informacji, do której sprawca nie jest uprawniony, a także ujawnienie innej osobie informacji uzyskanej w jeden z wyżej określonych sposobów.

Dobrem chronionym przez postanowienia tego przepisu jest zabezpieczenie informacji przed dostępem do nich osób nieuprawnionych, prawo do dysponowania informacją z wyłączeniem innych osób, a także bezpieczeństwo jej przekazywania, w konsekwencji prywatność korespondencji.

---

[1] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r. Nr 88 poz. 553 z późn. zm.

[2] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, tekst jedn. Dz.U. z 2006 r. Nr 90 poz. 631 z późn. zm.

[3] K. J. Jakubski, *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo" 1996, nr 12, s. 34.

Przełamanie albo omijanie elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń chroniących informację, które ma umożliwić sprawcy dostęp do takiej informacji, określane jest jako **hacking.** Oznacza on działanie polegające na usunięciu szczególnych konstrukcji, swoistych osłon w postaci kodów i haseł, które służą uniemożliwieniu dostępu do zgromadzonej i przetwarzanej informacji, za pośrednictwem Internetu, zapewniającego połączenia pomiędzy komputerami, bez konieczności fizycznego kontaktu z takimi urządzeniami. Działania mające znamiona hackingu same w sobie są przestępstwem, jednakże bardzo często stanowią część większej akcji przestępnej, której celem jest popełnienie także innych czynów zabronionych.

W literaturze przedmiotu wskazuje się, że do typowych metod, jakimi posługują się hakerzy w celu uzyskania nieuprawnionego dostępu do systemu komputerowego, należą:

1) koń trojański – program komputerowy pozornie użyteczny, w rzeczywistości realizujący nieznane i niepożądane dla ofiary ataku funkcje, sprowadzające się do umożliwienia hackerowi dostępu do systemu komputerowego;
2) backdoor – program komputerowy umożliwiający dostęp do systemu komputerowego z ominięciem istniejących zabezpieczeń „tylnymi drzwiami". Hacker samodzielnie instaluje taki program po dokonaniu penetracji systemu komputerowego, aby ułatwić sobie ewentualny powrót, bądź korzysta z programów zainstalowanych samodzielnie przez autorów oprogramowania na wypadek konieczności uzyskania dostępu do systemu komputerowego, jeżeli w wyniku awarii zostałyby zamknięte bądź znacznie utrudnione pozostałe drogi dostępu;
3) exploit – program komputerowy, który wykorzystuje błędy w zabezpieczeniach systemu operacyjnego lub innego oprogramowania. Niedoskonałości w oprogramowaniu nie stanowią rzadkości, a wykorzystujący je hakerzy uzyskują dzięki temu nieuprawniony dostęp do atakowanych systemów komputerowych;
4) spoofing – działania polegające na uzyskaniu nieuprawnionego dostępu do systemu komputerowego na skutek „podawania się" za inny komputer. Ta metoda polega na fałszowaniu podstawowych usług oraz protokołów sieciowych, tak aby ofiara ataku nie rozpoznała atakującego;
5) sniffing – działanie polegające na podsłuchiwaniu transmisji danych za pomocą specjalnych programów – snifferów, które przechwytują przesyłane dane.

Nie zawsze celem działania sprawcy jest pozyskanie informacji zgromadzonej i przechowywanej w systemie informatycznym, bardzo często jest nim także **nielegalne uzyskanie programu komputerowego**, o którym mowa w art. 278 § 2 kk, które polega na uzyskaniu bez zgody osoby uprawnionej cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej. Nielegalne uzyskanie programu komputerowego oznacza każde zachowanie prowadzące do wejścia w posiadanie cudzego programu komputerowego, bez zgody osoby uprawnionej. Czynność sprawcza polegająca na uzyskaniu programu komputerowego ma szersze znaczenie niż zabór i nie musi prowadzić do pozbawienia pokrzywdzonego możliwości dysponowania takim programem. Nielegalne uzyskanie programu komputerowe-

go może, ale nie musi, polegać na kradzieży materialnego nośnika z jego zapisem. Obejmuje ono wszelką formę przejęcia takiego programu bez zgody jego dysponenta w taki sposób, który umożliwia wykorzystywanie tego programu przez osobę nieuprawnioną, a więc zarówno zabór nośnika z zapisanym na nim programem, jak i skopiowanie samego programu bez dokonania zaboru jego nośnika[4]. Tym samym jego dotychczasowy dysponent wcale nie musi zostać pozbawiony władzy nad programem komputerowym.

Przedmiotem ochrony są prawa majątkowe twórcy i prawnego użytkownika do programu komputerowego, a jako przedmiot uboczny – prawa osobiste twórcy programu komputerowego.

Typowym przestępstwem popełnianym za pośrednictwem Internetu jest **oszustwo**, które polega na doprowadzeniu innej osoby do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, w celu osiągnięcia korzyści majątkowej (art. 286 § 1 kk). Przedmiotem ochrony jest mienie w szerokim rozumieniu tego pojęcia, obejmujące zarówno własność, jak i prawa majątkowe, którymi pokrzywdzony rozporządza. Najczęściej za pośrednictwem Internetu są dokonywane oszustwa w ramach aukcji internetowych.

> Mechanizm oszustw na aukcjach internetowych jest zazwyczaj podobny i polega ogólnie na niewywiązywaniu się ze zobowiązań powstałych w związku z zawarciem umowy za pośrednictwem serwisu aukcyjnego. Część internetowej transakcji przebiega na pierwszy rzut oka legalnie – wystawienie na sprzedaż określonego towaru, przeprowadzenie licytacji w ramach serwisu aukcyjnego, dokonanie płatności przez zwycięzcę aukcji. Jednakże dalszy przebieg transakcji następujący po zakończeniu etapu dokonywania płatności niczym już nie przypomina zgodnej z prawem transakcji elektronicznej. Pieniądze są bowiem przez oszusta pobierane, lecz wylicytowany towar nigdy nie dociera do klienta – odbiorca nie otrzymuje nabytego towaru bądź uzyskuje w jego zamian zupełnie bezwartościowy przedmiot[5] [który nie był przedmiotem aukcji internetowej – W. L.].

Oszustwo komputerowe tym różni się od oszustwa zwykłego, że nie wymaga podejmowania przez sprawcę oszukańczych działań zmierzających do niekorzystnego rozporządzenia przez pokrzywdzonego własnym lub cudzym mieniem. Czynność sprawcza polega na wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienianiu, usuwaniu albo wprowadzaniu nowego zapisu danych informatycznych, bez upoważnienia, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody (art. 287 § 1 kk). Oszustwo komputerowe zostaje popełnione z chwilą zrealizowania chociażby jedne-

[4] Por.: Wyrok Sądu Apelacyjnego w Krakowie z dnia 8 lipca 2009 r., II AKa 98/09, „Krakowskie Zeszyty Sądowe" 2009, nr 7–8, poz. 58.

[5] A. Drzazga, *Przestępczość internetowa*, w: *Wpływ Internetu na ewolucję państwa i prawa*, red. R. Grabowski, Rzeszów 2008, s. 216.

go ze wskazanych zachowań, bez względu na jego wynik. Warunkiem przestępności jest, by sprawca działał bez upoważnienia, czyli nie posiadając formalnego umocowania do zachowania się w sposób określony w przepisie.

Przedmiotem ochrony są prawa majątkowe stwierdzone w danych informatycznych oraz same zapisy tych danych. Strona przedmiotowa została ujęta w dwie odmiany: w pierwszej sprawca wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji, przekazywanie danych informatycznych, w drugiej zmienia, usuwa albo wprowadza nowy zapis danych informatycznych. Pierwsza odmiana stanowi ingerencję w funkcje wykonywane przez system informatyczny, druga – w zapisane dane informatyczne[6].

Powszechną formą oszustwa komputerowego jest **phishing**, polegający na wyłudzeniu cennych danych osobowych, najczęściej w postaci numeru karty kredytowej, kodów, haseł, danych dotyczących konta lub innych informacji, które mają charakter poufny. Do wyłudzenia takich danych dochodzi na skutek wprowadzenia ofiary w błąd za pośrednictwem stworzonych przez oszusta wiadomości elektronicznych bądź witryn WWW. Technika phishingu opiera się na rozsyłaniu licznych wiadomości e-mail, rzekomo pochodzących ze sprawdzonych witryn internetowych, informujących o konieczności zweryfikowania określonych danych dotyczących adresata, zwłaszcza numeru karty kredytowej, numeru konta, loginu czy hasła. Po skorzystaniu ze znajdującego się w treści wiadomości odnośnika, udostępnionego rzekomo dla wygody odbiorcy informacji, adresat zostaje automatycznie przekierowany do fałszywej, spreparowanej przez oszusta strony internetowej. Odnośnik taki może występować w postaci hiperłącza o dowolnym brzmieniu bądź link przybiera postać rzeczywistego adresu WWW, który został jednak skojarzony z serwerem profesjonalnie przygotowanej fałszywej strony internetowej. Fałszywa strona internetowa, na którą przekierowany zostaje adresat wiadomości e-mail, stanowi narzędzie służące do przechwytywania wpisywanych na niej poufnych informacji. Bardziej zaawansowane i trudniejsze do wykrycia są metody polegające na zafałszowaniu systemu tłumaczącego nazwy domenowe na numery IP i w konsekwencji przekierowaniu użytkownika na stronę oszustów internetowych. Zdobycie takich informacji pozwala oszustom na kradzież tożsamości ofiary, którą następnie posługują się w celu zdobycia korzyści majątkowych (dokonywanie zakupów w imieniu ofiary czy wyprowadzenie pieniędzy z jej rachunku bankowego). Kradzież tożsamości pozwala oszustom w stosunkowo krótkim czasie osiągnąć bardzo duże korzyści majątkowe, ponieważ ofiara ataku z reguły nie jest świadoma tego, że ktoś inny w sposób bezprawny podszywa się pod nią, posługując się jej personaliami.

Kodeks karny nie zawiera bezpośredniego odniesienia do kradzieży tożsamości, ale zawiera przepisy, które pozwalają ścigać sprawców kradzieży danych osobowych. Poza wspominanym już art. 267 kk, zakazującym nielegalnego pozyskiwania informacji, należy wskazać art. 268 kk, który kryminalizuje zachowania polegają-

[6] Zob.: A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 116.

ce na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu istotnej informacji albo udaremnianiu lub znacznemu utrudnianiu w inny sposób osobie uprawnionej zapoznanie się z nią. Przestępstwo **niszczenia informacji**, o którym mowa, chroni integralność, kompletność i poprawność informacji. W celu ograniczenia zakresu kryminalizacji tego rodzaju zachowań prawodawca podkreśla, że przestępstwo musi dotyczyć „istotnej informacji". Odpowiedzialność sprawcy zostaje zaostrzona, jeżeli dopuszcza się on wskazanych wyżej działań wobec zapisu na informatycznym nośniku danych lub wyrządzając znaczną szkodę majątkową.

Przestępstwo **naruszenia integralności danych**, o którym mowa w art. 268a kk, chroni bezpieczeństwo elektronicznie przetwarzanej informacji i systemów komputerowych, na które składa się integralność (nienaruszalność zapisu informacji w postaci danych informatycznych), prawidłowość funkcjonowania programów komputerowych, a także dostępność informacji w postaci danych informatycznych (możliwość korzystania z nich przez osoby uprawnione)[7].

Czynność sprawcza polega na niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu do danych informatycznych albo w istotnym stopniu zakłócaniu bądź uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych, nie będąc do tego uprawnionym. Dla bytu analizowanego przestępstwa bez znaczenia jest rodzaj informacji oraz charakter związanych z nią dóbr i interesów. Wykorzystuje się do tego programy komputerowe, które niszczą, uszkadzają, usuwają, zmieniają lub utrudniają dostęp do danych informatycznych albo w istotnym stopniu zakłócają lub uniemożliwiają automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych. W wyniku tych działań powstają dane nieautentyczne, które mogą zostać uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne[8].

Bezpieczeństwo danych i systemów komputerowych jest zagrożone także przez nielegalną ingerencję w jego prawidłowe funkcjonowanie, co jest szczególnie niebezpieczne, kiedy dotyczy danych informatycznych o wyjątkowym znaczeniu ze względu na ich potencjał informacyjny. W związku z tym prawodawca kryminalizuje przestępstwo **sabotażu komputerowego**, obejmujące działania polegające na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, bądź zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych (art. 269 § 1 kk). Zabronione jest także niszczenie albo wymienianie informatycznych nośników danych lub niszczenie albo uszkadzanie urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych o szczególnym znaczeniu dla obronności kraju,

---

[7] Zob.: A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001, s. 28–29.

[8] Zob.: R. A. Stefański, *Prawo karne materialne, część szczególna*, Warszawa 2009, s. 489.

bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego (art. 269 § 2 kk). „Najczęstszym sposobem dokonania tego czynu jest zainfekowanie systemu komputerowego programem odpowiednio przygotowanym w celu złamania zabezpieczeń chroniących dostęp do komputera, a następnie zatarcie śladów przez wprowadzenie do komputera wirusa, bomby logicznej lub robaka komputerowego”[9].

Dobrem chronionym są bezpieczeństwo elektronicznie przetwarzanej informacji i systemów komputerowych w postaci ich integralności, ale także (a może nawet przede wszystkim) obronność kraju, bezpieczeństwo w komunikacji, funkcjonowanie administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego[10].

Przestępstwo **zakłócania pracy systemu komputerowego**, o którym mowa w art. 269a kk, polega na zakłóceniu pracy systemu komputerowego lub sieci teleinformatycznej przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych. Przy czym zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej musi być istotne.

Dobrem chronionym w tym przypadku jest bezpieczeństwo elektronicznie przetwarzanej informacji, systemów komputerowych i sieci teleinformatycznych.

Do zakłócania systemów komputerowych, niszczenia lub uszkadzania zawartych w nich danych dochodzi głównie za pomocą specjalnie w tym celu tworzonych programów oraz sieci zainfekowanych komputerów, które stanowią narzędzie przestępstwa z art. 269b kk, kryminalizującego **bezprawne wykorzystanie programów i danych**. Przestępstwo to polega na wytwarzaniu, pozyskiwaniu, zbywaniu lub udostępnianiu innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej (art. 269b § 1 kk).

Przepis przewiduje penalizację czynności, które stanowią swoiste przygotowanie do popełnienia wymienionych w nim typów przestępstw. Urządzenia lub programy, kody, hasła czy inne dane umożliwiające dostęp do informacji, przystosowane do popełnienia tych przestępstw, to typowe narzędzia hackerskie[11].

Przedmiotem ochrony są informacje i dane informatyczne przechowywane w systemie komputerowym lub sieci teleinformatycznej.

---

[9] *Ibidem*, s. 490.

[10] Zob.: P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2000, nr 1, s. 94.

[11] Zob.: A. Adamski, *Przestępczość w cyberprzestrzeni*, s. 34–35.

Poza grupą przestępstw przeciwko informacji, Internet, niestety, służy także do szerzenia zakazanych przez prawo treści. Jednym z nich jest **publiczne nawoływanie do popełnienia czynu zabronionego**. Zgodnie z art. 255 kk

> § 1. Kto publicznie nawołuje do popełnienia występku lub przestępstwa skarbowego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Kto publicznie nawołuje do popełnienia zbrodni, podlega karze pozbawienia wolności do lat 3. § 3. Kto publicznie pochwala popełnienie przestępstwa, podlega grzywnie do 180 stawek dziennych, karze ograniczenia wolności albo pozbawienia wolności do roku.

Przedmiotem ochrony, objętym postanowieniami tych przepisów, jest porządek publiczny; „nawoływanie do przestępstwa czy pochwalanie go stanowi zagrożenie dla funkcjonowania państwa i może prowadzić do anarchii życia publicznego”[12]. Czynność nawoływania do popełnienia wymienionych w art. 255 § 1 i 2 kk czynów zabronionych sprowadza się do oddziaływania na psychikę innych, bliżej nieokreślonych osób poprzez wzywanie ich lub zachęcanie w różny sposób do popełnienia przestępstwa[13]. Z kolei pochwalanie wiąże się z wyrażaniem dodatniej oceny (aprobaty, uznania) dla przestępstwa, które ma zostać popełnione, lub też dla przestępstwa już popełnionego. Chodzi zatem o wyrażanie aprobaty dla zachowań, które na płaszczyźnie polskiego prawa karnego odpowiadają znamionom typu czynu zabronionego[14]. Terminy „nawołuje” i „pochwala” zawierają w sobie intencjonalność działania; sprawca w wypadku nawoływania ma zamiar wywołania u adresatów swojego apelu decyzji popełnienia przestępstwa, a w wypadku pochwalania ma zamiar wytworzenia przyjaznego, przychylnego stosunku wobec sprawcy, aprobaty dla czynu przestępnego[15]. Przy czym karalne jest tylko takie nawoływanie i pochwalanie, które zostało podjęte publicznie, czyli wówczas, kiedy sprawca zwraca się do bliżej nieoznaczonego kręgu osób.

Innym czynem zabronionym wykorzystującym Internet do szerzenia zakazanych przez prawo treści jest **publiczne znieważanie ludności**, stypizowane w art. 257 kk, zgodnie z którym „Kto publicznie znieważa grupę ludności albo poszczególną osobę z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości lub z takich powodów narusza nietykalność cielesną innej osoby, podlega karze pozbawienia wolności do lat 3”. Kryminalizując tego rodzaju zachowania, prawodawca chroni porządek publiczny zagrożony przez zachowania mające podłoże dyskryminacyjne, mogące prowadzić do konfliktów i podziałów społecznych, a także – ubocznie – godność jednostki lub grupy lud-

---

[12] Z. Ćwiąkalski, *Komentarz do art. 255*, w: *Kodeks karny. Część szczególna. Komentarz*, t. 2, red. A. Zoll, Kraków 2008, s. 1169.

[13] Por.: Wyrok Sądu Najwyższego z dnia 17 marca 1999 r., IV KKN 464/98, „Prokuratura i Prawo” 1999, nr 10, poz. 7.

[14] Zob.: K. Wiak, *Komentarz do art. 255*, w: *Kodeks karny. Komentarz*, s. 1104.

[15] Zob.: R. A. Stefański, *Prawo karne materialne*, s. 441.

ności oraz nietykalność cielesną człowieka[16]. Sprawca realizuje ustawowe znamiona przestępstwa wtedy, kiedy powodem jego czynu jest przynależność narodowa, etniczna, rasowa, wyznaniowa albo bezwyznaniowość pokrzywdzonego. Poza tym zachowanie sprawcy musi mieć charakter publiczny, czyli powinno zostać zrealizowane w taki sposób, aby było w stanie dotrzeć do wiadomości szerokiego, bliżej nieokreślonego kręgu osób, co zapewnia przekaz poprzez Internet.

Przestępstwo **obrazy uczuć religijnych innych osób**, o którym mowa w art. 196 kk, realizowane jest poprzez znieważanie publicznie przedmiotu czci religijnej lub miejsca przeznaczonego do publicznego wykonywania obrzędów religijnych. Przedmiot czci religijnej należy rozumieć szeroko, obejmując jego zakresem pojęciowym wszystko, do czego odnosi się cześć religijna w ramach danego wyznania, wszystko czemu ta cześć i kult są w ramach danej religii oddawane, a więc także do podmiotów kultu, czyli osób czczonych w ramach danej religii. Zachowanie sprawcy jest ukierunkowane na wywołanie u pokrzywdzonego odczucia obrazy jego uczuć religijnych, które są kształtowane treścią danej religii czy też stosunkiem określonego wyznania do danego przedmiotu, objętego przez daną religię konkretnym znaczeniem, uznanym za przedmiot kultu, godnym najwyższego szacunku[17].

Przez obrazę uczuć religijnych rozumie się takie zachowania, które odbierane są subiektywnie przez członków danej wspólnoty religijnej jako poniżające lub obelżywe dla przedmiotu tych uczuć, w szczególności przedmiotu czci religijnej lub miejsc sprawowania aktów religijnych. Subiektywne odczucie członków danej wspólnoty religijnej to jednak za mało, w związku z tym obraza musi być oceniana także obiektywnie. W tym sensie przypisanie danemu zachowaniu charakteru znieważenia powinno być dokonywane z uwzględnieniem społecznych norm kulturowo-obyczajowych i powszechnie przyjętych kryteriów oceny[18].

Przedmiotem ochrony są uczucia religijne osób wierzących, czyli pewien stosunek określonej grupy (przede wszystkim emocjonalny) do wyznawanej przez siebie religii przejawiający się także w prawie do ochrony szacunku wobec wyznawanych przez nią wartości oraz miejsc i przedmiotów otaczanych czcią i poważaniem. Uczucia religijne, ze względu na ich charakter, podlegają szczególnej ochronie prawa. Bezpośrednio powiązane są bowiem z wolnością sumienia i wyznania, stanowią wartość konstytucyjną[19]. Warunkiem karalności jest znieważenie publiczne; znamię publiczności zostanie spełnione, jeżeli sprawca posłużył się środkami umożliwiającymi mu dotarcie do większego, bliżej nieokreślonego kręgu osób.

Szczególnie dotkliwe są wszelkiego rodzaju publiczne pomówienia, dokonane za pośrednictwem Internetu, których celem jest zniesławienie lub znieważenie ofiary ata-

---

[16] Zob.: K. Wiak, *Komentarz do art. 257*, w: *Kodeks karny. Komentarz*, s. 1112.

[17] Zob.: O. Górniok, *Komentarz do art. 196*, w: *Kodeks karny*, t. 2, *Komentarz do artykułów 117–363*, red. O. Górniok i in., Gdańsk 2005, s. 198–199.

[18] Por.: Wyrok Sądu Najwyższego z dnia 17 lutego 1993 r., III KRN 24/92, „Wokanda" 1993, nr 10, s. 8.

[19] Por.: Orzeczenie Trybunału Konstytucyjnego z dnia 7 czerwca 1994 r., K 17/93, „Orzecznictwo Trybunału Konstytucyjnego" 1994, nr 1, poz. 11.

ku. **Przestępstwo zniesławienia**, zgodnie z art. 212 § 1 kk, polega na pomawianiu innej osoby, grupy osób, instytucji, osoby prawnej lub jednostki organizacyjnej niemającej osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności. Postacią kwalifikowaną przestępstwa zniesławienia jest posłużenie się przez sprawcę środkami masowego komunikowania. W grę wchodzą wszelkie ogólnodostępne środki, za pomocą których współcześnie odbywa się wymiana myśli i przekazywanie informacji, wśród nich mieści się także Internet.

Należy podkreślić, że przepis art. 212 kk mówi nie o poniżeniu w ogóle, lecz „o poniżeniu w opinii publicznej", co oznacza, że chodzi tu nie tyle o urazę osobistych uczuć osoby pokrzywdzonej, ale o to, jak osoba pomówiona będzie postrzegana przez szeroki, bliżej nieokreślony krąg osób. Karalne jest więc takie pomówienie, które może prowadzić do upokorzenia danej osoby w opinii innych osób, spowodować, że inne osoby będą uważać pokrzywdzonego za osobę poniżoną. W konsekwencji, jeżeli pomówienie wywołuje wyłącznie skutki w sferze osobistej danej osoby i nie wystawia na szwank jej publicznej reputacji, wówczas nie można mówić o zniesławieniu[20].

Przedmiotem ochrony jest tu cześć w znaczeniu zewnętrznym (przedmiotowym). O takim charakterze czci świadczy fakt, że karalnością objęte jest tylko takie pomówienie, które może poniżyć w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności.

Bardzo często w parze ze zniesławieniem idzie **znieważenie**, o którym mowa w art. 216 § 1 kk, zgodnie z którym „Kto znieważa inną osobę w jej obecności albo choćby pod jej nieobecność, lecz publicznie lub w zamiarze, aby zniewaga do osoby tej dotarła, podlega grzywnie albo karze ograniczenia wolności". Kwalifikowaną formę znieważenia stanowi znieważanie innej osoby za pomocą środków masowego komunikowania. Sprawca takiego znieważenia podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 216 § 2).

W przypadku znieważenia przedmiotem ochrony jest cześć w znaczeniu wewnętrznym (podmiotowym), oznaczająca poczucie własnej godności osobistej, wewnętrzne przekonanie o własnej osobie. Chroniona jest godność każdej osoby fizycznej, bez względu na jej płeć, wiek, status społeczny czy pochodzenie[21]. Nawet osoby dotknięte chorobą psychiczną czy upośledzeniem umysłowym nie tracą wartości, jaka nierozerwalnie związana jest z faktem bycia człowiekiem, w związku z tym i one mogą zostać znieważone[22]. W doktrynie zdecydowanie dominuje pogląd, że zniewaga może zostać popełniona jedynie przez działanie, co w przypadku posługiwania się Internetem nie budzi wątpliwości.

---

[20] Por.: Postanowienie Sądu Najwyższego z dnia 14 października 2010 r., II KK 105/10, LEX nr 621198.

[21] Zob.: A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 486.

[22] Zob.: W. Kulesza, *Zniesławienie i zniewaga. Ochrona czci i godności osobistej człowieka w polskim prawie karnym – zagadnienia podstawowe*, Warszawa 1984, s. 170.

Internet jest także wykorzystywany do **propagowania ustroju faszystowskiego** lub innego totalitarnego ustroju państwa bądź nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość, które to zachowania są kryminalizowane przez art. 256 § 1 kk. Podobne co do istoty jest przestępstwo, o którym mowa w art. 256 § 2 kk, które ma charakter wieloodmianowy; czynność sprawcza polega na produkowaniu, utrwalaniu, sprowadzaniu, nabywaniu, przechowywaniu, posiadaniu, prezentowaniu, przewożeniu lub przesyłaniu druków, nagrań lub innych przedmiotów, zawierających inkryminowane treści w celu ich rozpowszechniania, albo będących nośnikiem symboliki faszystowskiej, komunistycznej lub innej totalitarnej (art. 256 § 2 kk).

Dobrem chronionym są wartości konstytucyjne określające ustrój państwa, w szczególności zasada demokratycznego państwa prawnego oraz prawo do równego korzystania z wolności i praw przez wszystkie osoby, niezależnie od dzielących je różnic. Dodatkowym przedmiotem ochrony jest wolność grup narodowościowych, etnicznych, rasowych, wyznaniowych albo bezwyznaniowych.

Czynność sprawcza polega na propagowaniu bądź nawoływaniu, a więc wymaga od sprawcy podjęcia określonego działania.

> Propagowanie, w rozumieniu art. 256 kk, oznacza każde zachowanie polegające na prezentowaniu faszystowskiego lub innego totalitarnego ustroju państwa, w zamiarze przekonania do niego. [...] Propagowanie może, ale nie musi być połączone z pochwalaniem. Można bowiem coś publicznie pochwalać bez zamiaru propagowania, jak i propagować nie pochwalając tego, co się propaguje[23].

Z kolei nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość, oznacza sianie nienawiści, czyli silnej niechęci, wrogości do innej osoby czy grupy osób. Nawoływanie do nienawiści z powodów wymienionych w art. 256 kk sprowadza się do tego typu wypowiedzi, które wzbudzają uczucia silnej niechęci, złości, braku akceptacji, wręcz wrogości do poszczególnych osób lub całych grup społecznych czy wyznaniowych, bądź też z uwagi na formę wypowiedzi podtrzymują i nasilają takie negatywne nastawienie i tym samym podkreślają uprzywilejowanie, wyższość określonego narodu, grupy etnicznej, rasy lub wyznania[24].

Zjawiskiem powszechnie występującym w Internecie jest pornografia we wszystkich jej odmianach. Prawodawca w art. 202 § 1 kk zabrania publicznego prezentowania treści pornograficznych w sposób narzucający ich odbiór osobie, która tego sobie nie życzy. Karalne jest także produkowanie, utrwalanie lub sprowadzanie, przechowywanie bądź posiadanie w celu rozpowszechniania albo rozpowszechnia-

---

[23] Uchwała Sądu Najwyższego z dnia 28 marca 2002 r., I KZP 5/02, „Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa" 2002, nr 5–6, poz. 32.

[24] Zob.: R. A. Stefański, *Prawo karne materialne*, s. 443–444.

nie lub publiczne prezentowanie treści pornograficznych z udziałem małoletniego albo związanych z prezentowaniem przemocy lub posługiwaniem się zwierzęciem (§ 3). Przedmiotem kolejnych form przestępstwa pornografii jest utrwalanie treści pornograficznych z udziałem małoletniego poniżej lat 15 (§ 4); przechowywanie, posiadanie lub uzyskiwanie dostępu do treści pornograficznych z jego udziałem (§ 4a) oraz produkowanie, rozpowszechnianie, prezentowanie, przechowywanie lub posiadanie treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej (§ 4b), a także uczestniczenie w prezentacji treści pornograficznych z udziałem małoletniego w celu zaspokojenia seksualnego (§ 4c).

Pomimo dość rozbudowanego charakteru przepisu kryminalizującego pornografię, jej zdefiniowanie sprawia poważne trudności. Podkreśla się wręcz, że sformułowanie opisowej definicji pornografii, która pozwalałaby na prostą subsumpcję określonego stanu faktycznego i nie wymagałaby wartościowania treści o charakterze erotycznym, jest niemożliwe. W dużym uproszczeniu można jednak przyjąć, że pornografia oznacza przedstawienie ludzkich zachowań seksualnych i nagości w taki sposób, aby wywołać u odbiorcy pobudzenie seksualne[25], co wiąże się z istotą pornografii, do której zalicza się wytwarzanie oraz obrót materiałami przedstawiającymi inne osoby w trakcie czynności seksualnych lub osoby obnażone, czyli pozbawione okrycia intymnych części swojego ciała[26].

Szczególna ochrona dzieci (małoletnich poniżej 15 lat) przed zjawiskiem pornografii ma na celu chronić ich obyczajność w dziedzinie seksualnej, zwłaszcza chronić je przed destrukcyjnym wpływem pornografii na ich rozwój psychofizyczny.

W celu zwiększenia ochrony dzieci przed wykorzystywaniem seksualnym prawodawca wprowadził w art. 200a kk dodatkowe dwa typy przestępstw. Istotą czynności sprawczej pierwszego z nich jest nawiązanie kontaktu z małoletnim poniżej 15 lat za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej i tym samym zmierzanie – za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej – do spotkania z nim w celu popełnienia przestępstwa zgwałcenia (art. 197 § 3 pkt 2 kk) lub obcowania płciowego z małoletnim poniżej 15 lat (art. 200 kk) albo w celu produkowania lub utrwalania treści pornograficznych. Drugi typ polega na składaniu propozycji obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu albo utrwalaniu treści pornograficznych małoletniemu poniżej 15 lat za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej i zmierzaniu do jej realizacji.

Wprowadzenie w błąd może polegać zarówno na działaniu, jak i zaniechaniu (np. przemilczeniu pewnych informacji). Wyzyskanie błędu opiera się na zaniechaniu działań zmierzających do wyprowadzenia jakiejś osoby z błędnego przekonania

[25] *Ibidem*, s. 265.

[26] S. Hypś, *Komentarz do art. 202*, w: *Kodeks karny. Komentarz*, s. 919.

dotyczącego rzeczywistego stanu rzeczy[27]. Wyzyskanie niezdolności do należytego pojmowania sytuacji wymaga od sprawcy podjęcia aktywnych działań zmierzających do wykorzystania okoliczności, w jakich małoletni w chwili czynu się znajdował, konsekwencji których, z uwagi na młody wiek i niewystarczający stopień rozwoju psychofizycznego, nie był w stanie ani przewidzieć, ani sobie uświadomić. Groźba bezprawna oznacza z kolei groźbę karalną, o której mowa w art. 190 kk[28], jak i groźbę spowodowania postępowania karnego lub rozgłoszenia wiadomości uwłaczającej czci zagrożonego lub jego osoby najbliższej (art. 115 § 12 kk).

Czynność sprawcza, o której mowa w art. 200a § 2 kk, została określona jako składanie propozycji – przedstawienie oferty dotyczącej obcowania płciowego, poddania się bądź wykonania innej czynności seksualnej lub wzięcie udziału w produkowaniu albo utrwalaniu treści pornograficznych – małoletniemu poniżej 15 lat i zmierzanie do jej realizacji. Oczywiście dla bytu tego przestępstwa nie jest konieczne, aby doszło do realizacji jednego z tych celów. Przy czym dla przestępności takiego działania owa propozycja koniecznie musi być złożona za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej.

Przestępstwo, o którym mowa, określane jako **child grooming**, jest reakcją na wzmagające się zjawisko wykorzystywania seksualnego dzieci przez osoby dorosłe, możliwe dzięki nawiązywaniu z nimi kontaktu za pomocą Internetu i doprowadzaniu do spotkania z nimi w rzeczywistości. Child grooming wiąże się z zachęcaniem dziecka do udziału w czynności seksualnej w zamian za obietnicę nagrody, z dyskutowaniem na temat intymnych zachowań, z prezentowaniem treści o charakterze pornograficznym w celu przełamania oporu czy zahamowań dotyczących sfery seksualnej.

Przedmiotem ochrony jest nie tylko bezwzględny zakaz podjęcia czynności seksualnych z małoletnim poniżej 15 lat, lecz także zakaz podjęcia działań zmierzających do realizacji takiego celu.

> Ratio legis tego przepisu była zatem konieczność ochrony dobra dziecka zagrożonego przedwczesnym rozbudzeniem seksualnym, wpływającym niekorzystnie na jego rozwój. Ponadto uznaje się, że ze względu na niedojrzałość dziecko do 15 roku życia nie jest w stanie prawidłowo ocenić sytuacji zagrożenia i podjąć świadomej decyzji, dlatego w kontekście integralności seksualnej należy mu zapewnić szczególną ochronę[29].

W ścisłym związku pozostaje z nim przestępstwo z art. 200b kk, wprowadzające karalność publicznego propagowania lub pochwalania zachowań o charakterze pedofilskim.

---

[27] Por.: Wyrok Sądu Najwyższego z dnia 19 lipca 2007 r., V KK 384/06, LEX nr 299205.

[28] Zgodnie z art. 190 kk „§ 1 Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Ściganie następuje na wniosek pokrzywdzonego".

[29] S. Hypś, *Komentarz do art. 200a*, w: *Kodeks karny. Komentarz*, s. 909.

> Pedofilia, której istotą jest patologiczne zaburzenie fizjologiczno-psychiczne wyrażające się w potrzebie zaspokojenia seksualnego z użyciem do tego celu dziecka, prowadzi do naruszenia wielu dóbr, z których za najważniejsze uznaje się zagrożenie prawidłowego rozwoju psychofizycznego dziecka, ale także naruszenie jego godności, demoralizowanie go lub przedmiotowe traktowanie[30].

W tym przypadku przedmiotem ochrony jest obyczajność, na którą składa się społeczno-prawna negatywna ocena zachowań pedofilskich w takim stopniu, że uzasadnione jest już karanie ich publicznego propagowania i pochwalania. Czynność sprawcza polega na publicznym propagowaniu lub pochwalaniu zachowania o charakterze pedofilskim. Dla bytu przestępstwa ważne jest także, żeby odznaczały się one cechą publiczności.

Przedstawienie wszystkich niebezpieczeństw związanych z aktywnością w cyberprzestrzeni nie jest możliwe, ponieważ niemal codziennie pojawiają się nowe sposoby naruszania cudzych dóbr czy interesów przez osoby, dla których taki proceder stał się źródłem osiągania korzyści majątkowych. Globalna sieć jest powszechnie wykorzystywana nie tylko przez przestępców działających indywidualnie, lecz także w sposób zorganizowany. Specyficzne właściwości Internetu, brak kompleksowego ujęcia związanych z nim problemów, brak uregulowań prawnych dotyczących aktywności w cyberprzestrzeni, brak środków oraz metod zwalczania przypadków łamania prawa, bezradność organów ścigania związana z transgranicznością przekazów to tylko niektóre czynniki wpływające na powiększanie się grona cyberprzestępców. W związku z tym nietrudno przewidzieć, że skala zjawiska przestępczości internetowej będzie wzrastać wraz ze zwiększaniem się zasięgu oddziaływania Internetu oraz liczebności jego użytkowników.

> Można też prognozować, że wraz z rozwojem usług świadczonych drogą elektroniczną, rosnącą liczbą komercyjnych zastosowań Internetu, w szczególności ekspansją handlu elektronicznego i wykorzystywania teleinformatyki do potrzeb administracji publicznej (e-government), pojawi się wiele nowych, trudnych dziś do zdefiniowania form przestępczości, której technologicznie zaawansowany charakter stanowić będzie wyzwanie dla prawodawcy, administracji wymiaru sprawiedliwości oraz organów zajmujących się ściganiem przestępstw[31].

Zapewnienie skutecznej ochrony prawnej i poczucia bezpieczeństwa użytkownikom Internetu to niewątpliwie kwestia wprowadzenia właściwych regulacji prawnych i stałego monitorowania procesów, jakie dokonują się w globalnej sieci, po to, aby natychmiast i stanowczo na nie reagować. Jednakże z uwagi na globalny charakter i transgraniczność Internetu oraz dokonujący się stale postęp w zakresie nowoczesnych technologii współczesna walka z cyberprzestępczością wymaga ści-

---

[30] S. Hypś, *Komentarz do art. 200b*, w: *Kodeks karny. Komentarz*, s. 910–911.

[31] A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4, s. 74.

słej współpracy międzynarodowej. Konieczne wydaje się stworzenie pewnego międzynarodowego standardu, zwłaszcza gdy chodzi o kwestie penalizacji najbardziej niebezpiecznych kategorii zachowań. Stworzenie nowoczesnych i kompleksowych regulacji prawnych dotyczących sposobu wykorzystywania nowoczesnych technologii w zakresie gromadzenia, przetwarzania i przesyłania informacji stanowi poważne wyzwanie dla współczesnego prawodawcy.

Nie można przy tym nie zauważyć, że walka z cyberprzestępczością nieuchronnie wiąże się z koniecznością ograniczenia wolności i praw jednostki, co w społeczeństwach obywatelskich musi budzić uzasadniony niepokój. Państwo, przeciwdziałając i walcząc z cyberprzestępczością, siłą rzeczy ingeruje w sferę wolności i praw człowieka. W tym sensie pragnienie bezpieczeństwa i pragnienie wolności w globalnej sieci to wartości, które trudno ze sobą pogodzić. Dążenie do zapewnienia bezpieczeństwa w sieci prowadzi do wprowadzania środków mających je zagwarantować, co jednak nieodzownie wiąże się z ograniczeniem wolności. Z kolei, kiedy brakuje poczucia bezpieczeństwa, jednostki tracą pierwotny impet i pewność siebie, bez których trudno korzystać z przysługującej im wolności. Internet, który przez użytkowników postrzegany jest jako przestrzeń wolna od jakichkolwiek ingerencji, dla ich dobra musi zostać poddany reglamentacji prawnej.

Równolegle należy prowadzić działania mające na celu zwiększenie świadomości korzystania z Internetu poprzez propagowanie odpowiedniej wiedzy wśród jego użytkowników. Świadomość istniejących zagrożeń, wyrobienie krytycznego podejścia i wzmocnienie ostrożności wobec otrzymywanych treści pozwoli uniknąć wielu niebezpieczeństw związanych z aktywnością w sieci. Ostatecznie bowiem Internet ma służyć człowiekowi, a nie być kolejnym narzędziem godzącym w jego dobro.

Bibliografia:

Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4.

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001.

Ćwiąkalski Z., *Komentarz do art. 255*, w: *Kodeks karny. Część szczególna. Komentarz*, t. 2, red. A. Zoll, Kraków 2008.

Drzazga A., *Przestępczość internetowa*, w: *Wpływ Internetu na ewolucję państwa i prawa*, red. R. Grabowski, Rzeszów 2008.

Górniok O., *Komentarz do art. 196*, w: *Kodeks karny*, t. 2, *Komentarz do artykułów 117–363*, red. O. Górniok i in., Gdańsk 2005.

Hypś S., *Komentarz do art. 200a*, w: *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2012.

Hypś S., *Komentarz do art. 200b*, w: *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2012.

Hypś S., *Komentarz do art. 202*, w: *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2012.

Jakubski K. J., *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo" 1996, nr 12.
Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.
Kodeks karny. Część szczególna. Komentarz, t. 2, red. A. Zoll, Kraków 2008.
Kodeks karny. Komentarz, red. A. Grześkowiak, K. Wiak, Warszawa 2012.
Kodeks karny, t. 2, *Komentarz do artykułów 117–363*, red. O. Górniok i in., Gdańsk 2005.
Kulesza, *Zniesławienie i zniewaga. Ochrona czci i godności osobistej człowieka w polskim prawie karnym – zagadnienia podstawowe*, Warszawa 1984.
Marek A., *Kodeks karny. Komentarz*, Warszawa 2010.
Orzeczenie Trybunału Konstytucyjnego z dnia 7 czerwca 1994 r., K 17/93, „Orzecznictwo Trybunału Konstytucyjnego" 1994, nr 1, poz. 11.
Postanowienie Sądu Najwyższego z dnia 14 października 2010r., II KK 105/10, LEX nr 621198.
Stefański R. A., *Prawo karne materialne, część szczególna*, Warszawa 2009.
Uchwała Sądu Najwyższego z dnia 28 marca 2002 r., I KZP 5/02, „Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa" 2002, nr 5–6, poz. 32.
Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, tekst jedn. Dz.U. z 2006 r. Nr 90 poz. 631 z późn. zm.
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r., Nr 88 poz. 553 późn. zm.
Wiak K., *Komentarz do art. 255*, w: *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2012.
Wpływ Internetu na ewolucję państwa i prawa, red. R. Grabowski, Rzeszów 2008.
Wyrok Sądu Apelacyjnego w Krakowie z dnia 8 lipca 2009 r., II AKa 98/09, „Krakowskie Zeszyty Sądowe" 2009, nr 7–8, poz. 58.Wyrok Sądu Najwyższego z dnia 19 lipca 2007 r., V KK 384/06, LEX nr 299205.
Wyrok Sądu Najwyższego z dnia 17 lutego 1993 r., III KRN 24/92, „Wokanda" 1993, nr 10, s. 8.
Wyrok Sądu Najwyższego z dnia 17 marca 1999 r., IV KKN 464/98, „Prokuratura i Prawo" 1999, nr 10, poz. 7.

Streszczenie

Współczesny sposób komunikowania się i przekazywania informacji, pod wpływem Internetu, uległ zasadniczej zmianie. W kontekście dynamicznego rozwoju Internetu i nowych technologii tradycyjne środki masowego przekazu zeszły na drugi plan. Internet nie tylko umożliwia komunikowanie się na odległość w czasie rzeczywistym, lecz także dostęp do wszelkiego rodzaju niczym nielimitowanych informacji. Co więcej, wyzwala aktywność użytkowników Internetu, pozwala angażować się w różnego rodzaju inicjatywy, wypowiadać się na każdy temat. Pojawienie się Internetu otworzyło także nowe, nieznane wcześniej możliwości dla nauki, biznesu i kultury. Zalety Internetu są niewątpliwe. Niestety nie jest on wolny od niebezpieczeństw, które mogą wyrządzić wiele szkód czy być źródłem osobistych tragedii jego użytkowników. Rozpiętość przestępstw popełnianych za pośrednictwem Internetu jest szeroka i niezwykle zróżnicowana. Wiele z nich zostało przeniesionych do cyberprzestrzeni bezpośrednio z życia codziennego, inne są ściśle związane ze specyfiką Internetu. Te najbardziej niebezpieczne zostały stypizowane w Kodeksie karnym z 6 czerwca 1997 r.

SAFETY OF CYBERNETIC SPACE FROM THE LEGAL AND CRIMINAL PERSPECTIVE – SELECTED ISSUES

Summary

The contemporary way of communication and information transmission under Internet influence has undergone some changes. In the context of a dynamically developing Internet and new technologies, the traditional means of mass media have receded into the background. Internet does not only facilitate communication over a distance in real time, but also accessibility to all kinds of unrestricted information. Furthermore, it causes the activation of Internet users, enables the involvement in various initiatives, the expression of one's opinion on any subject. The advent of the Internet has also created new, unknown earlier, opportunities for the sciences, business and culture. The merits of the Internet are unquestionable. Unfortunately it is not free from dangers, that can cause a lot of harm or be the cause of personal tragedy to its users. The range of crime perpetrated via the Internet is wide and unusually varied. A lot of it was transferred to the cybernetic space directly from everyday life, others are strictly connected to the specificity of the Internet. The most dangerous were typified in the 6th June 1997 criminal code.