KPP

MONOGRAFIE

Wybrane aspekty przestępczości w cyberprzestrzeni

Studium prawnokarne i kryminologiczne

mgr Iga A. Jaroszewska

Olsztyn 2017

Redakcja naukowa:
mgr Iga A. Jaroszewska

Recenzenci:
dr hab. Krystyna Szczechowicz, prof. UWM
dr Piotr Rychlik

Projekt okładki:
dr Agata Opalska

Korekta autorska.

Kortowski Przegląd Prawniczy Monografie (KPP Monografie)

ISBN: 978-83-949079-6-9

SPIS TREŚCI

WYKAZ SKRÓTÓW

ADL	- The Anti-Defamation League
ARPA	- Agencja Zaawansowanych Projektów Badawczych
ARPANET	- Advanced Research Projects Agency Network
art.	- artykuł
BSA	- Business Software Alliance
CCDCoE	- NATO Cooperative Cyber Defence Centre of Excellence
CERT	- Computer Emergency Response Team
EKPC	- Europejska Konwencja Praw Człowieka
Europol	- Europejski Urząd Policji
GCA	- Global Cybersecurity Agenda
ICT	- Information and Communication Technology
ISP	- Internet Service Provider
IT	- Information technology
ITU	- Międzynarodowy Związek Telekomunikacyjny
KGB	- Komitet Bezpieczeństwa Państwowego przy Radzie Ministrów ZSRR
k.k.	- Kodeks karny
NASK	- Naukowa i Akademicka Sieć Komputerowa
NATO	- Organizacja Traktatu Północnoatlantyckiego
NGO	- Non-governmental organizations
OECD	- Organizacja Współpracy Gospodarczej i Rozwoju
ONZ	- Organizacja Narodów Zjednoczonych
PICS	- Platform for Internet Content Selection
RP	- Rzeczpospolita Polska
TCP/IP	- Transmission Control Protocol/Internet Protocol
TFUE	- Traktat o Funkcjonowaniu Unii Europejskiej
UE	- Unia Europejska
URL	- Uniform Resource Locator
USA	- Stany Zjednoczone Ameryki
WSIS	- World Summit on the Information Society
WWW	- World Wide Web

WSTĘP

Rozwój cyberprzestrzeni to nie tylko nowe możliwości, ale także liczne wyzwania dla krajowych i międzynarodowych ustawodawców. Internet to nośnik o charakterze międzynarodowym, dla którego tradycyjne normy sprawowania jurysdykcji są niewystarczające. Choć początkowo miał on służyć przede wszystkim celom badawczym i edukacyjnym, w wyniku czego cechował go brak zabezpieczeń, to wciąż rosnąca popularność sieci komputerowych oraz wzrost liczby użytkowników zwróciły uwagę na kwestię jego bezpieczeństwa. Nowe środowisko wpłynęło nie tylko na kształt istniejących stosunków prawnych, ale przede wszystkim przyczyniło się do powstania nowych form przestępczości, które zaczęto określać mianem cyberprzestępstw. Stosowanie zwyczajowych rozwiązań prawnych do cyberprzestrzeni okazało się niemożliwe, a granice, w których dotychczas działały organy państwowe są niewystarczająco szerokie - nadużycia komputerowe stanowią zagrożenie nie tylko dla bezpieczeństwa krajowego, a dla całych społeczności.

Ze względu na transgraniczny charakter zjawiska, bezpieczeństwo cyfrowe stało się przedmiotem zainteresowania wszystkich członków społeczeństwa informacyjnego. Cyberprzestępczość uznano za jeden z najpoważniejszych problemów, z którym obecnie muszą się zmierzyć organy ścigania. Choć określenie skali zjawiska jest niezwykle trudne, nie ulega wątpliwości, że wykorzystywanie zdobyczy technologicznych do celów sprzecznych z prawem jest coraz bardziej powszechne.

W Polsce pierwsze próby dostosowywania obowiązujących norm prawnych do wymogów zwalczania cyberprzestępczości zostały podjęte w połowie lat 90-tych. Obecnie, z uwagi na ratyfikację Konwencji Rady Europy o cyberprzestępczości, należałoby zwrócić uwagę na zgodność rodzimego porządku prawnego z nowymi wymogami. Sformułowane zostały wytyczne dotyczące karalności oraz zasady odpowiedzialności osób prawnych, a ponadto określono zasady jurysdykcji i przesłanki ekstradycji sprawców. Pełną zgodność polskiego Kodeksu karnego z postanowieniami Konwencji miała zapewnić ustawa z dnia 4 kwietnia 2014 roku o zmianie ustawy - Kodeks kamy oraz niektórych innych ustaw.

ROZDZIAŁ I
ZAGADNIENIA WPROWADZAJĄCE

Nowe możliwości, jakie niesie za sobą rozwój szeroko rozumianej cyberprzestrzeni, to także nowe pytania i wyzwania zarówno dla krajowych, jak i międzynarodowych ustawodawców. Wynika to bezpośrednio ze specyfiki zjawiska, z którym mamy do czynienia, transgranicznego charakteru sieci globalnej, dla której tradycyjne normy sprawowania jurysdykcji okazały się niewystarczające. Internet to nośnik międzynarodowy, który nie może pozostać poza regulacją prawną. Działania podejmowane w sieci mają wpływ na świat pozawirtualny, a nawet mogą stwarzać dla niego realne zagrożenie. Ponadto, brak granic państwowych i rozległość sieci komputerowych, znacznie utrudniają nakładanie jakichkolwiek ograniczeń przez prawodawstwa narodowe[1].

1.1. INTERNET - EWOLUCJA I CHARAKTERYSTYKA

W świadomości wielu osób pojęcie Internetu jest równoznaczne z jego najpowszechniejszym zastosowaniem, czyli stronami WWW. Rozumowanie to jest niepełne, a sam Internet to zdecydowanie więcej niżeli tylko „protokół http, który stanowi podstawę funkcjonowania ogólnoświatowego katalogu stron WWW”[2]. To ogólnoświatowa sieć komputerowa, „globalny system wymiany danych, funkcjonujący w oparciu o wzajemnie połączone sieci lokalne, rozmieszczone w wielu fizycznych lokalizacjach, umożliwiających jednoczesną, wielopłaszczyznową interakcję użytkowników z całego świata”[3]. Zamienne stosowanie tych określeń najprawdopodobniej wynika z głównej funkcji Internetu, jaką jest wyszukiwanie informacji, które są magazynowane przede wszystkim w postaci stron WWW.

Zimna wojna to okres rywalizacji nie tylko politycznej, czy ideologicznej, ale przede wszystkim militarnej i technologicznej. Wówczas rząd Stanów Zjednoczonych, stojący na czele bloku zachodniego, powołał ARPA *(Advanced Research Projects Agency*) - agencję rządową działającą w strukturach Departamentu Obrony, która miała na celu tworzenie nowych projektów z zakresu technologii wojskowej. W stosunkowo krótkim czasie utworzono pierwsze badawcze centra komputerowe, a agencja została podstawowym fundatorem badań nad systemami komputerowymi na terenie USA. Rozpoczęto budowę pierwszej zdecentralizowanej sieci połączonych komputerów - nowego systemu łączności umożliwiającego podtrzymanie

[1] J.Kulesza, *Międzynarodowe Prawo Internetu*, Ars boni et aequi, Poznań 2010, s. 55-65.
[2] Ibidem, s. 56.
[3] Ibidem, s. 57.

ciągłości dowodzenia nawet podczas ataku nuklearnego. Unikatowa sieć otrzymała nazwę ARPANET (*Advanced Research Projects Agency Network*) i jest uważana za pramatkę współczesnego Internetu. Kolejnym krokiem była próba połączenia różnych sieci ARPANET, w efekcie umożliwiająca im swobodny przesył danych. Stało się to możliwe dzięki stworzonemu w latach 70. protokole transmisji danych TCP/IP (*Transmission Control Protocol/Internet Protocol*), późniejszej podstawie struktury Internetu[4].

Rozwój ARPANET i stopniowe konstytuowanie się sieci lokalnych to dopiero początek rozkwitu nowej przestrzeni społecznej, jaką powoli stawał się Internet. Na początku lat 90. zasadniczo wzrosło użycie komputerów osobistych, a firmy telekomunikacyjne zaczęły przejawiać zainteresowanie usługami sieciowymi[5]. Wzrost znaczenia sieci był związany z rozszerzaniem jej zasięgu, dlatego też nie stawiano żadnych przeszkód przed dołączającymi się sieciami. Nadzór amerykańskiego Departamentu Obrony skończył się w momencie, gdy udział cywilnych użytkowników zaczął stwarzać realne niebezpieczeństwo dla tajności projektu[6]. Komercjalizacja Internetu stała się faktem.

„W „Małej Encyklopedii PWN" z 1995 roku nie ma jeszcze hasła „Internet". Słowo to zaczęło trafiać na łamy codziennych gazet w drugiej połowie lat 90."[7]. Choć przyłączenie Polski do Internetu ogłoszono 12 września 1991 roku[8], musiało minąć trochę czasu zanim zaczęto dostrzegać możliwości, jakie niosło za sobą „nowe medium". Przed wyborami parlamentarnymi w 1997 roku Komisja Wyborcza zakazała publikacji wyników sondaży przed dniem głosowania także w Internecie, co świadczyło o wzroście jego znaczenia. Kolejnym krokiem była publikacja listu gończego przez częstochowską policję[9]. Internet stał się wszechobecny, zaczął oddziaływać na życie i obyczaje coraz większej liczby osób, a tempa jego rozwoju nie da się porównać do żadnych dotychczasowych przeobrażeń.

Początkowo Internet miał służyć przede wszystkim celom badawczym i edukacyjnym. Charakteryzował go brak zabezpieczeń i łatwy dostęp do wszelakich informacji, także tych tajnych. Nie sprawowano kontroli nad obrotem danymi. Już w 1996 roku Pierre Delvy pisał w swoim raporcie „Deuxieme Deluqe", przygotowanym na zlecenie Komisji Kultury Rady Europy, że „zgrupowanie ludzi o różnych horyzontach w jednej otwartej i interaktywnej tkance jest sytuacją niespotykaną i obiecującą (...), (lecz) także źródłem nowych problemów"[10]. Wciąż

[4] J. Hofmolk, *Internet jako nowe dobro wspólne*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2009, s. 66-70.
[5] Ibidem, s. 74-5.
[6] Ibidem, s. 109.
[7] T. Bienias, *Internet*, Wydawnictwo Znak, Kraków 1998, s. 8.
[8] Ibidem, s. 20.
[9] Ibidem, s. 10.
[10] P. Delvy, *Deuxieme Deluqe* [on-line], „Magazyn Sztuki" 1997, nr 13, dostęp: 3.02.2015,

rosnąca popularność sieci komputerowych i nieustający wzrost liczby użytkowników zwróciły uwagę na bardzo istotne kwestie, jakimi są bezpieczeństwo i zaufanie. Współcześni internauci wywodzą się z różnych grup społecznych, a ich kompetencje i motywacje znacznie różnią się od tych, które charakteryzowały pierwszych odbiorców Internetu[11]. Delvy słusznie zauważył, że tylko i wyłącznie od nas zależy, jak wykorzystamy nowe technologie, i że to na nas ciąży zbiorowa odpowiedzialność[12].

1.2. NOWA FORMACJA SPOŁECZNO-GOSPODARCZA – POWSTANIE SPOŁECZEŃSTWA INFORMACYJNEGO

Wraz z rozwojem techniki można było zaobserwować przekształcanie się społeczeństwa z uprzemysłowionego, którego głównym celem była konsumpcja dóbr, w społeczeństwo informacyjne, kładące szczególny nacisk na rozwój każdej należącej do niego jednostki[13].

Sam termin „społeczeństwo informacyjne" pochodzi z Japonii. Jako pierwszy użył go w 1963 roku etnolog T. Umesao w artykule dotyczącym ewolucyjnej teorii społeczeństwa opartego na przemysłach informacyjnych, a spopularyzowane zostało już pięć lat później przez teoretyka mediów K. Koyama. Japończycy doskonale rozumieli, że chodzi o coś więcej, niż tylko popularność technik komputerowych. Y. Masuda opracował strategię rozwoju wszystkich stref życia społecznego w oparciu o najnowsze technologie oraz ich industrialne zastosowanie[14]. Do Europy pojęcie to dotarło w 1978 roku za pośrednictwem pary socjologów - Simona Nory i Alaina Minca, w sprawozdaniu przedłożonym prezydentowi Francji. Jednak dyskusję na ten temat zapoczątkował dopiero opublikowany w 1994 roku raport ówczesnego komisarza Unii Europejskiej M. Bangemann'a pt. „Europa a społeczeństwo globalnej informacji - zalecenia dla Rady Europejskiej *(Europe and the Global Information Society: Recommendations to the European Council)*[15] "[16]. Był to początek budowy społeczeństwa informacyjnego.

Choć wszyscy wyrażają zgodę na traktowanie społeczeństwa informacyjnego jako

http://magazynsztuki.eu/old/n_technologia/dmgi%20potop.htm.

[11] J. Hofmolk, *Internet jako nowe dobro wspólne,* op. cit., s. 112-13.

[12] P. Delvy, *Deuxieme Deluqe,* op. cit.

[13] A. Szewczyk (red.). *Dylematy cywilizacji informatycznej,* Polskie Wydawnictwo Ekonomiczne, Warszawa 2004, s. 11-12.

[14] T. Goban-Klas, *Społeczeństwo informacyjne i jego teoretycy* [w:] J. Lubacz (red.), *W drodze do społeczeństwa informacyjnego,* Drukarnia Oficyny Wydawniczej Politechniki Warszawskiej, Warszawa 1999, s. 29-30.

[15] Report on Europe and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council, Bulletin of the European Union, Supplement No. 2/94.

[16] A. Kisiel, *Społeczeństwo Informacyjne – wybrane przykłady szans i zagrożeń, „*Polskie Stowarzyszenie Zarządzania Wiedzą, Seria: Studia i Materiały" 2011, nr 51, s. 117-18.

nowej formacji społeczno-gospodarczej, nie osiągnięto consensusu w kwestii wspólnej nazwy nowej epoki, a także jej definicji. Niezależnie jednak od konkretnych definicji, ich niezmiennym elementem jest akcentowanie roli informacji, jako podstawowego składnika budowy tego społeczeństwa.

Jesteśmy istotami społecznymi, a informacja istnieje od momentu, w którym nauczyliśmy się komunikować i przybiera coraz to doskonalsze formy. Powstanie nowej formacji społeczno-gospodarczej jest ściśle związane z rozwojem technologicznym, który w znacznym stopniu ułatwił dostęp do informacji oraz ich rozprzestrzenianie się - Internet służy nie tylko do wyszukiwania informacji, ale także ich umieszczania, czy przekazywania innym.

Kluczowym elementem społeczeństwa informacyjnego jest powiązanie komputerów ze środkami łączności, co intensyfikuje efektywność pracy, zarówno intelektualnej, jak i kontrolowanej przez nią produkcji i dostawy towarów. Można je zatem zdefiniować, jako „społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz przetwarzanie informacji jest podstawą tworzenia dochodu narodowego i dostarcza źródła utrzymania większości społeczeństwa”[17]. To nowy rodzaj społeczeństwa, rozwijający się w krajach zaawansowanych technologicznie, gdzie rozporządzanie informacją, jej jakość oraz szybkość wymiany są podstawowymi czynnikami konkurencyjności w usługach oraz przemyśle, a stopień rozwoju obliguje do korzystania z nowoczesnych technik magazynowania, przekazywania, przetwarzania i użytkowania informacji[18].

Im bardziej strategiczna jest rola informacji oraz procesów z nią związanych w życiu społecznym, tym bardziej zasadne jest posługiwanie się pojęciem społeczeństwa informacyjnego w nawiązaniu do konkretnej wspólnoty[19].

1.3. CYBERPRZESTRZEŃ

Żyjemy w czasach, w których dla wielu osób miarą statusu społecznego jest liczba znajomych na portalu społecznościowym, a cena, którą potencjalny nabywca jest w stanie zapłacić za wirtualny przedmiot, dostępny jedynie w sieciowej grze komputerowej, może przekraczać nawet kilka tysięcy złotych. Znakiem czasów stało się przetwarzanie możliwie jak największej ilości danych o pojedynczych osobach w rozmaitych systemach

[17] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania* [on-line], Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 53, dostęp: 21.02.2015, http ://informacj acyfrowa. wsb. edu.pl/pdfs/SpoleczenstwoInformacyjne .pdf.

[18] Ministerstwo Gospodarki - ePolska. Plan działania na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 - 2006, s. 67.

[19] L. Porębski, *Elektroniczne oblicze polityki: demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Uczelniane Wydawnictwo Naukowo-Dydaktyczne AGH, Kraków 2001, s. 13.

teleinformatycznych. Internet jest zdecydowanie najczęściej wykorzystywanym i najszybszym źródłem pozyskiwania informacji, a przy tym obszarem świadczenia wielu usług. Tak powstała „cyberprzestrzeń" - nowe miejsce ludzkiej aktywności[20].

Pojęcie „cyberprzestrzeń" pojawiło się po raz pierwszy już w połowie lat 80. w opowiadaniu „Burning Chrome" Williama Gibsona, a następnie zostało spopularyzowane przez jego debiutancką powieść „Neuromancer". Amerykański pisarz, uważany za prekursora cyberpunku, użył tego pojęcia do scharakteryzowania wirtualnej rzeczywistości, w której toczyły się losy jego bohaterów[21]. „Oznaczał on świat numerycznych sieci traktowanych jako pole bitwy, na którym ścierają się światowe koncerny. Stawka, o jaką walczą, to nowa granica gospodarcza i kulturowa"[22]. Biorąc pod uwagę fakt, że w tamtym czasie trudno było przewidzieć masowy rozwój sieci komputerowej, wizja autora okazała się zaskakująco trafna.

Choć trudno mówić o istnieniu jednej, powszechnie obwiązującej definicji cyberprzestrzeni, ta sformułowana przez Pierre'a Delvy we wcześniej wspomnianym raporcie wydaje się być ponadczasowa: „(cyberprzestrzeń) jest to przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie"[23].

W Polsce cyberprzestrzeń po raz pierwszy została zdefiniowana w założeniach do Rządowego Programu Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2009-2011[24], jako „przestrzeń komunikacyjna tworzona przez systemy powiązań internetowych". W kolejnym Rządowym Programie Ochrony, na lata 2011-2016[25], uległa ona rozbudowaniu i za cyberprzestrzeń uznano „cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne" „wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami".

Przedstawione powyżej rozumienie cyberprzestrzeni stało się częścią języka prawnego wraz z nowelizacją ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych RP[26]. Zgodnie z ustawową definicją, cyberprzestrzeń należy rozumieć, jako

---

[20] J.Wasilewski, *Zarys definicyjny cyberprzestrzeni* [w:] „Przegląd Bezpieczeństwa Wewnętrznego"2013, nr 9, s. 225-6 [on-line], dostęp: 18.03.2015, http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa/987,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-9-5-2013.html.

[21] M.Nowak, *Cybernetyczne przestępstwa - definicje i przepisy prawne* [on-line], „Biuletyn EBIB" 2010, nr 4, dostęp: 3.02.2015, http://www.ebib.pl/2010/113/a.php?nowak.

[22] P.Delvy, *Deuxieme Deluqe*, op. cit.

[23] P.Delvy, *Deuxieme Deluqe*, op. cit.

[24] Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia [on-line], Warszawa 2009, dostęp: 29.04.2015, https://www.msz.gov.pl/resource/93e1e4c7-e129-41c7-8365-39dbad8b1c54:JCR.

[25] Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 [on-line], dostęp: 29.04.2015, http://bip.msw.gov.pl/bip/programy/19057,Rzadowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.

[26] Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 [on-line], dostęp: 29.04.2015, http://bip.msw.gov.pl/bip/programy/19057,Rzadowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.

„przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne”[27], „wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami” [28]. Określenie wprowadzone do polskiego prawa, podobnie, jak definicja proponowana przez CCDCoE *{NATO Cooperative Cyber Defence Centre of Excellence),* uwzględnia zarówno techniczny, jak i ludzki składnik cyberprzestrzeni.

Choć tę samą definicję powtórzono w Polityce Ochrony Bezpieczeństwa Rzeczypospolitej Polskiej 2013[29], wydaje się być ona niewystarczająco precyzyjna. Przede wszystkim brakuje wyraźnego rozróżnienia błędnie utożsamianych ze sobą pojęć „informacja” i „dane”, a także określenia, czym właściwie są systemy informatyczne. Ponadto, słownikowe znaczenie zastosowanych w definicji terminów (np. przestrzeń, powiązania, relacje) jest stosunkowo trudne do interpretacji w kontekście pojęcia cyberprzestrzeni. Brak jest też jakiejkolwiek wzmianki o zasobach informacyjnych cyberprzestrzeni, a to właśnie ich bezpieczeństwo było celem stworzenia Polityki. Co ciekawe, w Polityce Ochrony Bezpieczeństwa Rzeczypospolitej Polskiej, rozdzielono przestrzeń przetwarzania informacji na tę odbywającą się na terytorium kraju i poza nim, czyli w miejscach, w których funkcjonują przedstawiciele Rzeczypospolitej Polskiej, jakby zapominając, że główną cechą protokołów wykorzystywanych przez systemy informatyczne jest ich oderwanie od fizycznej lokalizacji[30].

Rosenne pisząc o nieuchwytności, nieokreśloności i oderwaniu od naturalnych cech[31], podkreśla jak bardzo specyficznym środowiskiem jest cyberprzestrzeń - często rządząca się własnymi prawami oraz posiadająca cechy właściwe tylko sobie. Z tej przyczyny, korzystanie z sieci wymaga należytego przygotowania użytkownika, którym to w przypadku obustronnego oddziaływaniu cyberprzestrzeni i sfery prawnej staje się państwo, a konkretnie jego organy prawotwórcze.

Ze względu na coraz większą rolę, jaką odgrywają systemy teleinformatyczne, zarówno w życiu społeczeństwa, jaki i w infrastrukturze państwowej, cyberprzestrzeń stała się przedmiotem zainteresowań współczesnej doktryny prawnej. Należało zbadać nowe, cyfrowe środowisko, które wpłynęło nie tylko na kształt zawierania umów cywilnoprawnych, czy dokonywanie czynności administracyjnych, ale przede wszystkim przyczyniło się do powstania

[27] Art. 2 ust. 1b Ustawy o stanie wojennym, op. cit.
[28] Ibidem.
[29] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej [on-line], dostęp: 29.04.2015, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html.
[30] J. Kosiński, *Pradygmaty cyberprzstępczości,* Difin SA, Warszawa 2015, s. 34.
[31] S. Rosenne, *The perplexities of modern international law, General Course on Public International Law,* RCADI 2003, s. 349.

nowych form przestępczości. Wiele z dotychczas znanych czynności prawnych uległo zmianie w cyberprzestrzeni, a jeszcze więcej powstało zupełnie nowych[32].

1.3.1. PRÓBY MIĘDZYNARODOWEJ REGULACJI INTERNETU

Okazało się, że zastosowanie zwyczajowych rozwiązań prawnych do cyberprzestrzeni jest niemożliwe, a praktyki krajowe, w kwestii rozstrzygania sporów, czy chociażby samego administrowania siecią, w znaczny sposób się od siebie różnią[33].

Granice, w jakich zazwyczaj działały organy państwowe, okazały się być niewystarczająco szerokie i elastyczne - niemożliwym było zastosowanie wobec podmiotów działających w cyberprzestrzeni tych samych podstaw prawnych jak w przypadku podmiotów, które działają jedynie w świecie rzeczywistym. Ponadto, niektóre obszary bezpośrednio powiązane ze specyfiką Internetu, wymagają wskazania nowych, indywidualnych rozwiązań - ponadgranicznych, odrębnych od zasady terytorialności[34].

Podejmowane dotąd próby regulacji prawnej cyberprzestrzeni mają jedynie fragmentaryczny charakter i ograniczają się do dostosowania obowiązujących zasad prawa miejscowego oraz prawa międzynarodowego do aktywności podejmowanej w Internecie[35].

Jednak problem z określeniem zakresu kompetencji poszczególnych państw w cyberprzestrzeni zyskał w ostatnim czasie kolejny, międzynarodowy przejaw - cyberatak, czyli atak na strategiczne zasoby informatyczne państw z użyciem Internetu. Zjawisko to zapoczątkował atak rosyjskich hakerów na Estonię w 2007 roku[36], a w maju 2014 roku Stany Zjednoczone, jako pierwsze w historii, pozwały inny kraj w związku z cyberszpiegostwem. Departament Sprawiedliwości USA postawił w stan oskarżenia pięciu członków chińskiej armii pod zarzutem włamania się do komputerów i kradzieży cennych tajemnic handlowych dotyczących wiodących producentów stali, elektrowni jądrowej oraz branży solarnej.

Sprawa ta otwiera drogę do większej liczby aktów oskarżenia i pokazuje, że państwa poważnie traktują sprawę odpowiedzialności obcych rządów za przestępstwa popełnione w cyberprzestrzeni.

---

[32] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni* op. cit., s. 227.
[33] J. Kulesza, *Międzynarodowe Prawo Internetu,* op. cit., s. 289.
[34] Ibidem, s. 349 – 351.
[35] Ibidem, s. 305.
[36] Ibidem, s. 350.
[37]

ROZDZIAŁ II
CYBERPRZESTĘPCZOŚĆ – PROBLEMATYKA TERMINOLOGICZNA

Na początku lat 90. XX wieku dostęp do Internetu posiadało jedynie 3 miliony osób, z czego ponad 70% stanowili obywatele Stanów Zjednoczonych, a 15% pochodziło z Europy Zachodniej. Pozostali użytkownicy to mieszkańcy Kanady, Australii, Japonii, Republiki Korei oraz Izraela. W tamtym czasie, poza wymienionymi państwami, dostęp do Internetu był praktycznie niemożliwy[37]. Tym bardziej trudno uwierzyć, że w 2012 roku na świecie było już prawie 2,5 miliarda użytkowników Internetu, 5 miliardów telefonów komórkowych oraz ponad 600 milionów stron internetowych, a liczba dziennie wysyłanych wiadomości e-mail przekraczała 2 miliardy[38].

Postęp technologiczny końca dwudziestego wieku w znacznym stopniu przyczynił się do powstania dotychczas nieznanych zjawisk patologicznych, które ze względu na swoją szkodliwość społeczną, zostały uznane za przestępstwa, bądź wykroczenia. Jednym z takich zjawisk[39] są nadużycia komputerowe, stanowiące zagrożenie nie tylko dla bezpieczeństwa krajowego, lecz także całych społeczności[40].

2.1. PRZESTĘPSTWA KOMPUTEROWE

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 komputera", czy po prostu „przestępstwa komputerowe"[41], jednak nie były one wystarczająco precyzyjne i winno się je rozpatrywać raczej w kategorii haseł, niż oznaczeń konkretnego działania przestępczego[42].

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

[37] Worldmapper, *Internet Users 1990, Map No.335* [on-line], dostęp: 10.04.2015, http://www.worldmapper.org/display.php?selected=335.
[38] PINGDOM, *Internet 2012 in numbers* [on-line], dostęp: 10.04.2015, http://royal.pingdom.com/2013/0l/16/internet-2012-in-numbers/.
[39] K. J. Jakubski, *Przestępczość komputerowa – zarys problematyki, „*Prokuratura i prawo" 1996, nr 12, s. 34.
[40] M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 9.
[41] Ibidem.
[42] K. J. Jakubski, *Przestępczość komputerowa - zarys problematyki,* op. cit. s. 34.

szczególnej wiedzy z zakresu informatyki, co miało stanowić element konieczny do popełnienia przestępstwa[43].

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"[44]. Oznacza to, że mianem przestępstwa komputerowego określamy zarówno czyny, w których komputer pełnił rolę narzędzia do dokonania przestępstwa, jak i te skierowane przeciwko systemom przetwarzania danych[45].

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 zarówno przypadki, w których system komputerowy stanowi narzędzie, jak i przedmiot zamachu[46].

Nieustający rozwój nowoczesnych technologii miał wpływ nie tylko na same 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 (*Information 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"[47].

---

[43] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 10.
[44] K. J. Jakubski, *Przestępczość komputerowa - zarys problematyki,* op. cit. s. 34.
[45] Ibidem, s. 34.
[46] A. Adamski, *Prawo karne komputerowe*, op. cit., s. 34.
[47] M.Siwicki, *Cyberprzestępczość,* op. cit., s. 12-14.

2.2. POJĘCIE CYBERPRZESTĘPCZOŚCI

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[48], ale przed wszystkim będzie bezpośrednio oddziaływało na skuteczność międzynarodowego systemu do walki z przestępczością komputerową[49].

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[50].

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:

a) 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, oraz
b) 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[51].

W Komunikacie Komisji Europejskiej[52] z 7 lutego 2013 roku stwierdzono, że pojęcie cyberprzestępczości „odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe

[48] Ibidem, s. 15.
[49] J. Kulesza, *Międzynarodowe Prawo Internetu,* op. cit., s. 149.
[50] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 17.
[51] Ibidem, s. 17.
[52] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee Of The Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, (JOIN/2013/0001).

narzędzie przestępcze lub są głównym celem działania przestępczego”[53]. Zatem grupa czynów określana tym mianem polega na posługiwaniu 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[54].

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[55], a także fakt, że mogą być popełnione na masową skalę, niezależnie od odległości dzielącej miejsce popełnienia przestępstwa od miejsca, w którym mają wystąpić skutki[56].

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[57]. Komputer może być zarówno celem przestępstwa, kluczowym elementem, czy po prostu narzędziem koniecznym do jego popełniania. Niezależnie od zastosowania, użycie komputera umożliwia działanie z dużej

[53] Ibidem, s. 3.
[54] S. Bębas, J. Plis, J. Bednarek (red.), *Patologie w cyberświecie*, Wyższa Szkoła Handlowa, Radom 2012, s. 149.
[55] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 20.
[56] M. Gruchoła, *Polityka Unii Europejskiej w zakresie cyberprzestępczości* [w:] S. Bębas, J. Plis, J. Bednarek (red.), *Patologie w cyberświecie*, op. cit., s. 149.
[57] J. Kosiński, *Pradygmaty cyberprzestępczości*, op. cit., s. 88.

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[58].

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"[59]. 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 - ewoluują wraz z możliwościami jakie daje Internet, stając się coraz bardziej powszechne i szkodliwe[60].

Ustawodawstwo karne niektórych państw uznaje cyberprzestępstwa za odrębny rodzaj działania niezgodnego z prawem, lecz na gruncie prawa polskiego jest ono jedynie określane jako czyn zabroniony popełniony w obszarze cyberprzestrzeni[61] 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[62], a przede wszystkim rozdziale XXXIII „Przestępstwa przeciwko ochronie informacji", w ustawie o ochronie danych osobowych[63], czy ustawie o prawie autorskim i prawach pokrewnych[64].

Gwarantem efektywnego ścigania cyberprzetępczości jest stosowanie spójnych regulacji - bezprawnego zachowania, które miało miejsce w cyberprzestrzeni nie należy

[58] J. Kulesza, *Międzynarodowe Prawo Internetu,* op. cit., s. 152-3.
[59] M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo 2002" nr 4, s. 62.
[60] Interpol, *Cybercrime* [on-line], dostęp: 17.04.2015, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[61] Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej, s. 5.
[62] Ustawa z dnia 6 czerwca 1997 r. - Kodeks kamy (Dz.U. 1997 nr 88, poz. 553).
[63] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133, poz. 883).
[64] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24, poz. 83) [dalej: pr. aut].

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[65]

2.3. HISTORIA KONTROLI NADUŻYĆ W CYBERPRZESTRZENI

Trudno dokładnie określić kiedy po raz pierwszy wykorzystano komputery do celów niezgodnych z prawem, jednak najwcześniejsze doniesienia pochodzą z prasy amerykańskiej lat 60., a dotyczyły one naruszenia integralności danych, sabotażu oraz szpiegostwa. Na tym etapie, ze względu na niewielką dostępność komputerów, popełnianie przestępstwa ograniczały się do fizycznych uszkodzeń, czy włamań do systemów informatycznych w celu prowadzenia rozmów telefonicznych na cudzy koszt. Jednak, jak słusznie zauważa Adamski, każdy przełom technologiczny, niosący za sobą nowe wynalazki, narusza utrwalony kształt stosunków społecznych, tym samym stwarzając wyzwania dla prawodawców[66].

W latach 70. technologia komputerowa stała się tańsza, co przełożyło się na wzrost liczby komputerów. Systemy komputerowe zaczęły przenikać do różnorodnych dziedzin życia, co sprzyjało rozwojowi nowych form przestępczości. Nielegalne użycie komputera, manipulowanie danymi, czy zamachy na skomputeryzowane depozyty pieniężne, skłoniły państwa do próby stworzenia ustawodawstwa mającego na celu przeciwdziałanie cyberprzestępczości. Starano się dostosować dotychczasowe regulacje tak, aby móc powstrzymać nowe zjawisko. Pierwszą reformą ustawodawczą, będącą bezpośrednim następstwem komputeryzacji, było wprowadzenie przepisów służących ochronie danych osobowych[67].

Mimo coraz częstszego wykorzystania komputerów do celów sprzecznych z prawem, wciąż nie zdawano sobie sprawy, jak poważnym zagrożeniem jest cyberprzestępczość. Dopiero dwa głośne incydenty z końca lat 80-tych uzmysłowiły opinii publicznej realność zagrożeń jakie niesie za sobą komputeryzacja. Pierwszym z nich był paraliż sieci ARPANET w 1988

[65] J. Kulesza, *Międzynarodowe Prawo Internetu,* op. cit., s. 154-5.
[66] A. Adamski, *Prawo karne komputerowe*, Wydawnictwo C.H. Beck, Warszawa 2000, s. 1.
[67] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 22.

roku, wywołany przez robaka komputerowego autorstwa Roberta T. Morrisa. Sytuacja nie tylko miała zakończenie w sądzie, ale była też bezpośrednią przyczyną utworzenia zespołu szybkiego reagowania na incydenty zagrażające bezpieczeństwu sieci - CERT. Druga, wyjątkowo sensacyjna jak na tamte czasy była sprawa „hackerów z Hanoweru" - grupy młodych Niemców przeszukujących brytyjskie i amerykańskie komputery wojskowe w celu sprzedaży pozyskanych informacji KGB. Efektem ich działania było międzynarodowe śledztwo zakończone aresztowaniem podejrzanych przez Bundeskriminalamt[68]. Efektem tych zdarzeń była reglamentacja prawna nadużyć dokonywanych z użyciem elektronicznych systemów przetwarzania danych oraz zamachów skierowanych przeciwko nim[69].

Lata 80. to także pierwsze przypadki tzw. piractwa komputerowego, a w efekcie kolejna tendencja legislacyjna mająca na celu wzmocnienie ochrony własności intelektualnej. Wiele państw zdecydowało się na zamianę dotychczas chroniącej prawa autorskie odpowiedzialności cywilnoprawnej na odpowiedzialność karną[70].

We wcześniejszych latach kwestia konsekwencji jakie towarzyszą powszechnej komputeryzacji nie skupiała szczególnej uwagi organizacji rządowych ani międzynarodowych[71]. Wprowadzenie stron WWW zaowocowało nie tylko wzrostem liczby użytkowników Internetu, ale również zwróciło uwagę na problem przeciwdziałania treściom, które były przedmiotem ograniczeń prawnych tylko na gruncie niektórych ustawodawstw. Należało dostosować przepisy prawa karnego procesowego do potrzeb ścigania cyberprzestępców oraz ustalić ramy odpowiedzialności za propagowanie nielegalnych i szkodliwych treści z wykorzystaniem Internetu[72]. W tym okresie rządy różnych krajów po raz pierwszy równocześnie zdały sobie sprawę z zagrożenia dla globalnego porządku prawnego[73], a nadużycia komputerowe zostały uznane za jeden z rodzajów przestępczości transgranicznej [74] oraz stały się tematem badań nad przestępczością zorganizowaną[75].

W Polsce pierwsze próby dostosowywania obowiązujących norm prawnych do wymogów zwalczania cyberprzestępczości zostały podjęte w połowie lat 90., jednak prawo karne wciąż poddawane jest nowelizacjom[76].

Ponad czterdziestoletni okres rozkwitu technologii komputerowych pokazał, że

---

[68] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 2-3.
[69] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 23.
[70] Ibidem, s. 23.
[71] K. J. Jakubski, *Przestępczość komputerowa - zarys problematyki,* op. cit., s. 34.
[72] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 25.
[73] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 3.
[74] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 25.
[75] K. J. Jakubski, *Przestępczość komputerowa - zarys problematyki,* op. cit., s. 34.
[76] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 25.

korzystanie z najnowszych osiągnięć techniki oraz wolności informacji wymaga wyznaczenia jasno określonych granic[77]. Międzynarodowy charakter przestępczości oraz nieustający wzrost strat przez nią powodowanych, są jedynymi z głównych przyczyn zmiany podejścia do problemu przestępczości komputerowej[78]

2.4. WYBRANE INICJATYWY MIĘDZYNARODOWE W ZAKRESIE PRZECIWDZIAŁANIA CYBERPRZESTĘPCZOŚCI

„Szacuje się, że codziennie na całym świecie ponad milion osób pada ofiarą cyberprzestępczości. Koszt związany z cyberprzestępczością może wynosić łącznie 388 miliardów dolarów w skali globalnej”[79].

Bezpieczeństwo cyfrowe powoli staje się podstawową materią dla wszystkich członków społeczeństwa informacyjnego. W momencie, kiedy tak ogromna część życia codziennego uzależniona jest od komputerów, niezbędne staje się zapewnienie ich bezpieczeństwa[80]. Inicjatywy międzynarodowe odnoszące się do kwestii bezpieczeństwa w cyberprzestrzeni obejmują zarówno działania opiewające na skalę światową, jak i te podejmowane na poziomie krajowym, czy regionalnym.

2.4.1. UNIA EUROPEJSKA

Jednym ze strategicznych celów utworzenia Unii Europejskiej było umożliwienie wolnego przepływu osób, towarów oraz usług w obrębie jej obszaru. Swobodny ruch osób zapewnia Układ z Schengen[81], a obrót towarów i usług jest zagwarantowany przez utworzenie na terytorium Unii Jednolitego Rynku Europejskiego[82]. Jednak zniesienie kontroli paszportowych zapoczątkowało dyskusję nad koniecznością wzmocnienia granic zewnętrznych UE oraz potrzebą podjęcia dodatkowych działań w celu zapewnienia bezpieczeństwa obywateli[83].

Systemy informatyczne są podstawowym elementem relacji politycznych, społecznych

---

[77] A. Adamski, *Prawo karne komputerowe*, op. cit., s. 4.
[78] K. J. Jakubski, *Przestępczość komputerowa - zarys problematyki*, op. cit., s. 34.
[79] Komisja Europejska – Komunikat Prasowy: Unijne centrum ds. walki z cyberprzestępczością będzie zwalczać przestępstwa internetowe i chronić e-konsumentów [on-line], dostęp: 5.05.2015, http://europa.eu/rapid/press-release_IP-12-317_pl.htm.
[80] J. Kulesza, *Międzynarodowe Prawo Internetu,* op. cit., s. 154.
[81] Podstawowym akt prawny w sprawie stopniowego znoszenia kontroli na wspólnych granicach, który został podpisany w 1985 r.
[82] Jednolity Rynek Europejski (ang. Single European Market) - zintegrowany rynek, którego granice wyznaczają granice zewnętrzne Unii Europejskiej (tzw. rynek wewnętrzny UE). Program jego utworzenia zawarty był w Białej Księdze z 1985 r. Podstawową przesłanką jego utworzenia było umożliwienie swobodnego przepływu dóbr, kapitału, usług i siły roboczej wewnętrznych krajów UE.
[83] A. Suchorzewska, *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzmem,* Wolters Kluwer Polska, Warszawa 2010, s. 109-10.

oraz gospodarczych na ternie Unii Europejskiej, a zależność społeczeństwa od technologii cyfrowych jest niezmiernie wysoka i stale rośnie. Ich prawidłowe funkcjonowanie i bezpieczeństwo są niezbędne do pozyskania zaufania konsumentów oraz utrzymania poprawnego funkcjonowania gospodarki internetowej, co z kolei przekłada się na kondycję rynków wewnętrznych, wzrost gospodarczy oraz odsetek bezrobocia. Zapewnianie należytego poziomu ochrony systemów informatycznych winno się odbywać w zakresie skutecznych i kompleksowych środków prewencyjnych, jakie współtowarzyszą działaniom wobec cyberprzestępczości podnoszonym w obszarze prawa karnego[84].

W ciągu ostatniej dekady Unia Europejska opracowała kilka instrumentów prawnych mających na celu przeciwdziałanie cyberprzestępczości. Mimo że, rozwiązania te są wiążące jedynie dla państw członkowskich, niektóre kraje spoza UE decydują się na wykorzystanie standardów unijnych jako punktu odniesienia do lokalnych dyskusji na temat harmonizacji przepisów prawnych w tej materii[85].

Choć aktywność Unii Europejskiej na płaszczyźnie bezpieczeństwa cybernetycznego datowana jest już na rok 1997, kiedy to Parlament wraz z Radą UE wydały dyrektywę w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym[86], kompetencje Unii w zakresie prawa karnego były bardzo mocno ograniczone, a wydawane dyrektywy rzadko odwoływały się do prawnokarnych środków ochrony.

Sytuacja ulegała zmianie wraz z wejściem w życie Traktatu z Lizbony[87] - prawo karne stało się osobną dziedziną współpracy. Artykuły 82-86 TFUE[88] *(Traktat o Funkcjonowaniu Unii Europejskiej*) upoważniają Unię Europejską do ujednolicenia przepisów prawa karnego. Szczególną uwagę zwrócono na potrzebę przeciwdziałania przestępczości o charakterze transgranicznym oraz konieczność współpracy w zakresie ich zwalczania, m.in. poprzez wypracowanie wspólnych definicji, a także ustanowienie norm minimalnych odnoszących się do określania przestępstw oraz kar w danej dziedzinie[89].

Na szczególną uwagę zasługuje art. 83 TFUE dotyczący uprawnień Parlamentu

---

[84] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.
[85] M. Gercke, *Understanding cybercrime: phenomena, challenges and legał response,* op. cit., s. 128.
[86] Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (97/66/WE).
[87] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r., Dz.U. 2009 nr 203, poz. 1569.
[88] Traktat o funkcjonowaniu Unii Europejskiej, Dz.Urz. UE 2012, C 326/47.
[89] M. Gercke, *Understanding cybercrime: phenomena, challenges and legał response,* op. cit., s. 128-9.

Europejskiego i Rady w zakresie ustanawiania norm minimalnych odnoszących się do „do określania przestępstw oraz kar w dziedzinach szczególnie poważnej przestępczości wymiarze transgranicznym". Przyjęte brzmienie art. 83 tworzy kolejny etap w rozwoju stopnia i sposobów współdziałania wymiarów sprawiedliwości w zakresie prawa karnego. Udzielenie szerszych uprawnień instytucjom Unii jest następnym krokiem w zakresie wspólnego zwalczania przestępczości o ponadnarodowym wymiarze. Jednak akapit drugi ust. 1 art. 83 wyraźnie ogranicza te uprawnienia do przestępstw o najpoważniejszym ciężarze gatunkowym, a w stosunku pozostałych czynów zabronionych, Rada może posłużyć się jedynie aktem prawnym w formie decyzji. W celu sprecyzowania kompetencji, jakie otrzymały Parlament Europejski i Rada, następujące dziedziny przestępczości zostały wymienione, a jedną z nich jest właśnie przestępczość komputerowa[90].

Pomimo zasadniczych zmian w strukturze UE, rozwiązania, które zostały przyjęte w przeszłości pozostają prawomocne. Na podstawie art. 9[91] Protokołu w sprawie postanowień przejściowych, akty prawne ustanowione przed wejściem w życie Traktatu z Lizbony zostają utrzymane do czasu ich uchylenia, unieważnienia lub zmiany w zastosowaniu traktatów.

Inicjatywy podjęte przez Unię Europejską (a wcześniej Wspólnotę Europejską) w celu zwalczania i przeciwdziałania cyberprzestępczości są tak liczne, że niemożliwe byłoby ich omówienie w niniejszej pracy. Można natomiast stwierdzić, że przyjęte rozwiązania ukazują zaangażowanie organów unijnych w walkę z przestępczością internetową. Przyjęte dokumenty zawierają nie tylko uregulowania normatywne, ale określają również obligatoryjne przesłanki jurysdykcji[92].

Jednak niemożliwe byłoby pominięcie Dyrektywy Parlamentu Europejskiego i Rady z dnia 12 sierpnia 2013 roku dotyczącej ataków na systemy informatyczne. Ustanawia ona minimalne normy odnoszące się do określania przestępstw oraz kar w obszarze ataków na te systemy. Ponadto, ma ułatwić zapobieganie takim przestępstwom i udoskonalić współpracę między organami sądowymi oraz innymi właściwymi organami[93].

Omawiana dyrektywa zobowiązuje państwa członkowskie do podjęcia niezbędnych środków zmierzających do karania jako przestępstwo, umyślnego oraz bezprawnego uzyskiwania dostępu do całości lub części systemu informatycznego, gdy zostało ono dokonane

[90] G. Gruew, Kompetencja instytucji Unii Europejskiej do ustanawiania i kształtowania norm prawa karnego, „Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza" 2012, nr 1, s. 107-113. materialnego
[91] Protocol (No 36) on transitional provisions (EUR-Lex, nr 12008M/PRO/36).
[92] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 37-44.
[93] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

z naruszeniem środków bezpieczeństwa, przynajmniej w przypadkach, które nie są sytuacjami mniejszej wagi[94].

Karze podlegać ma także doprowadzenie w sposób umyślny oraz bezprawny do poważnego utrudnienia lub zakłócenia w funkcjonowaniu systemu informatycznego poprzez wprowadzenie, przekazanie, uszkodzenie, usunięcie, pogorszenie, zmianę lub eliminację danych komputerowych, czy też uczynienie ich niedostępnymi co najmniej w wypadkach, które nie są sytuacjami mniejszej wagi[95].

Z kolei art. 5 omawianej dyrektywny zobowiązuje państwa do zagwarantowania karalności umyślnego i bezprawnego pogarszania, zmieniania lub eliminowania danych komputerowych w systemach informatycznych, a także czynienia ich niedostępnymi, przynajmniej w przypadkach, które nie są sytuacjami mniejszej wagi.

Ostatnią czynności, której karalność ma zagwarantować niniejsza dyrektywa jest umyślna produkcja, sprzedaż, dostarczanie w celu użycia, dowóz, rozpowszechnianie lub też udostępnianie w jakikolwiek inny sposób jednego z wymienionych narzędzi, jeśli ono zostało dokonane bezprawnie oraz umyślnie z zamiarem popełnienia któregoś z przestępstw, wymienionych w art. 3-6, przynajmniej w wypadkach, które nie są sytuacjami mniejszej wagi:

a. programu komputerowego, stworzonego lub przystosowanego przede wszystkim w celu popełniania przestępstw, które zostały zawarte art. 3-6,
b. hasła, kodu dostępu, bądź też podobnych danych, które umożliwiają dostęp do całości albo części systemu informatycznego[96].

Zatem podstawowym celem tego dokumentu jest „zagwarantowanie, by ataki na systemy informatyczne były karane we wszystkich państwach członkowskich skutecznymi, proporcjonalnymi i odstraszającymi sankcjami karnymi”[97], a jego osiągnięcie ma zapewnić współpraca między organami ścigania a organami sądowymi na ternie całej Unii, mająca kluczowe znaczenie dla skutecznej walki ze zjawiskiem cyberprzestępczości.

Warto również zwrócić uwagę na utworzone w ramach Europolu, Europejskie Centrum ds. Walki z Cyberprzestępczością, którego główną misją jest zwalczanie nielegalnych działań podejmowanych przez zorganizowane grupy przestępcze. Centrum ma za zadanie wspierać,

[94] Art. 3 Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne.
[95] Art. 4 Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne.
[96] Art. 6 Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne.
[97] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

a w razie potrzeby koordynować operacje oraz dochodzenia prowadzone przez organy państw członkowskich w takich obszarach, jak: walka z wykorzystywaniem seksualnym dzieci, przestępstwami technologicznie zaawansowanymi, czy oszustwem płatniczym. Dyrektor Centrum, Troels Örting, podsumowując pierwszy rok działalności, stwierdził, że dotychczasowe rezultaty są bardzo zadowalające"[98].

Jednak w przygotowanym przez Business Software Alliance[99] (BSA) i opublikowanym 3 marca 2015 roku raporcie - „European CyberSecurity Dashboard", będącym pierwszym tego rodzaju badaniem odpowiednich rozwiązań politycznych w państwach członkowskich, zwrócono uwagę na znaczące braki w cyberbezpieczeństwie Unii Europejskiej, wynikające przede wszystkim z różnic w polityce, prawie oraz możliwościach poszczególnych państw członkowskich[100].

Z danych zaprezentowanych w raporcie wynika, że większość państw ma świadomość zagrożeń wynikających z istnienia oraz nieustającego rozwoju systemów teleinformatycznych, ponadto uznaje działania na rzecz bezpieczeństwa cybernetycznego za jeden z głównych celów narodowych[101].

Równocześnie zaznaczono, że istnieją znaczne rozbieżności między przyjętymi politykami cyberbezpieczeństwa, a jednym z najistotniejszych problemów jest niewystarczająca współpraca władz z podmiotami pozarządowymi oraz brak partnerstwa publiczno-prywatnego - ugruntowane ramy dla takiego partnerstwa istnieją tylko w pięciu państwach członkowskich UE (Austrii, Niemczech, Holandii, Hiszpanii i Wielkiej Brytanii). Taka sytuacja pozostawia duży obszar, który mógłby zostać wykorzystany do efektywnej współpracy rządów i sektora prywatnego, będącego właścicielem większości komercyjnej infrastruktury krytycznej w Europie[102].

Mimo że, najlepiej rozwinięte kraje Unii posiadają wewnętrzne systemy zabezpieczające, to wciąż widoczne są istotne braki u pozostałych członków, co decyduje o słabości całej wspólnoty. Przepływ informacji jest procesem nieprzerwanie występującym pomiędzy państwami członkowskimi, w wyniku czego dane podlegające wystarczającej

---

[98] Komisja Europejska - Komunikat Prasowy: Europejskie Centrum ds. Walki z Cyberprzestępczością - pierwszy rok działalności [on-line], dostęp: 5.05.2015, http://europa.eu/rapid/press-release_IP-14- 129_pl.htm.

[99] Założona w 1998 r. i działająca w 60 krajach na świecie organizacja reprezentująca komercyjnych producentów zamkniętego oprogramowania i sprzętu komputerowego. Jej członkami są m.in. Apple, Adobe, Dell, IBM, Intel, Microsoft, Oracle i Symantec.

[100] European CyberSecurity Dashboard and 28 Country Reports Launched - 3 March 2015 [on-line], dostęp: 4.05.2015, http://www.galexia.com/public/about/news/about_news-id300.html.

[101] EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace, s. 1 [on-line], dostęp: 4.05.2015, http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

[102] Ibidem, s. 2.

ochronie w jednym państwie trafiają do systemów słabo chronionych, stając się są narażone na przechwycenie [103]. Choć zagadnienie cyberbezpieczeństwa jest często traktowane jako wyzwanie finansowe, należy je raczej rozpatrywać w kategorii sprawdzaniu z umiejętności zarządzania. Nadanie polityce właściwego toru, stworzenie odpowiednich norm prawnych, umocnienie współpracy pomiędzy zainteresowanymi podmiotami oraz zwiększanie świadomości społecznej wobec cyberzagrożeń stanowią kluczowe kroki, jakie należy podjąć, aby zapewnić bezpieczeństwo wszystkich państw członkowskich[104].

2.4.2. Organizacja Współpracy Gospodarczej i Rozwoju

Organizacja Współpracy Gospodarczej i Rozwoju już w 1983 roku podjęła próby opracowania norm międzynarodowych prawa karnego na płaszczyźnie zapobiegania przestępstwom komputerowym. Dwa lata później opublikowała raport pt. „Przestępstwa związane z komputerem: analiza polityki legislacyjnej w obszarze OECD" *{Computer-related Criminality: Analysis of Legał Policy in the OECD Area*[105]) będący zaczątkiem opracowanej przez Radę Europy Rekomendacji R(89)9 [106]. Zawierał on, poza analizą stanu prawnego obowiązującego w państwach członkowskich OECD, także listę zachowań z użyciem komputera, które powinny podlegać kryminalizacji[107].

W 1990 roku, pod przewodnictwem OECD, powołano pierwszą grupę ekspertów, której zadaniem było sformułowanie zaleceń dotyczących ochrony elektronicznie przetwarzanych informacji. Ponadto, w tym samym roku utworzono drugą grupę, która w oparciu o wcześniejsze ustalenia przygotowała opracowanie pt. „Wytyczne OECD dla bezpieczeństwa systemów informatycznych i sieci: w kierunku kultury bezpieczeństwa" (*OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* [108]). Organizacja Współpracy Gospodarczej i Rozwoju, na podstawie przeglądu stanu prawnego państw członkowskich, przygotowała także liczne postulaty zmian ustawodawczych, a w latach późniejszych opublikowała raporty m.in. na temat wpływu zjawiska *spamu* na państwa

---

[103] P. Borkowski, *Perspektywy cyberbezpieczeństwa Unii Europejskiej* [on-line], Portal Spraw Zagranicznych 2009, dostęp: 4.05.2015, http://www.psz.pl/127-unia-curopcjska/piotr-borkowski- perspektywy-cyber-bezpieczenstwa-unii-europejskiej.

[104] EU Cybersecurity Dashboard, s. 2.

[105] OECD, Computer-related Criminality: Analysis of Legał Policy in the OECD Area, Report DSTI- ICCP 84.22 of 18 April 1986.

[106]RecommendationNo. R (89) 9 Of the Committee of Ministers to Member States on Computer- related crime and finał Report of the European Committee on Crime Problems.

[107] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 44-5.

[108] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [on-line], C(2002)131/FINAL, 29 July 2002, dostęp: 4.05.2015, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C%282002%29131/FINAL&docLanguage=En.

rozwijające się oraz sposobu i zakresu kryminalizacji cyberterroryzmu[109].

Obecnie działania OECD skoncentrowane są przede wszystkim na cyberbezpieczeństwie oraz globalnej promocji przeciwdziałania przestępczości komputerowej. Efektem takiej polityki jest organizacja konferencji, warsztatów, publikacja coraz to nowszych raportów, a także monografii pt. „Wirusy komputerowe i inne złośliwe oprogramowanie. Zagrożenie dla gospodarki opartej na Internecie" (*Computer Viruses and Other Malicious Software: A Threat to the Internet Economy [110]),* zawierającej informacje na temat złośliwego oprogramowania, a także nowe badania dotyczące wpływu bezpieczeństwa cybernetycznego na rozwój ekonomii i sugestie na temat sposobu rozwiązania problemu.

2.4.3. MIĘDZYNARODOWY ZWIĄZEK TELEKOMUNIKACYJNY

Liczne inicjatywy w dążeniu do przeciwdziałania cyberprzestępczości zostały podjęte także przez Międzynarodowy Związek Telekomunikacyjny (*International Telecommunication Union - ITU*), jedną z organizacji wyspecjalizowanych ONZ, ustanowionych w celu ujednolicenia oraz regulacji rynków technologii informacyjnych[111].

Do najistotniejszych należy rola współorganizatora Światowego Szczytu Społeczeństwa Informacyjnego (*World Summit on the Information Society - WSIS),* który miał miejsce w Genewie (2003) oraz w Tunisie (2005). Podczas tych spotkań politycy oraz eksperci z całego świata wymieniali doświadczenia dotyczące rozwoju globalnego społeczeństwa informacyjnego, a także dyskutowali nad potrzebą wypracowania międzynarodowych standardów kryminalizacji cyberprzestępczości. W efekcie przyjęto m.in. Genewski Plan Działania (*Geneva Plan o Action [112]*) oraz Tuniski Program na rzecz Społeczeństwa Informacyjnego (*Tunis Agenda for the Information Society[113]),* mające na celu budowę zaufania i bezpieczeństwa w zakresie korzystania z technologii informacyjno-komunikacyjnych[114].

Sekretarz Generalny ITU powołał także grupę ekspertów składającą się nie tylko z przedstawicieli państw członkowskich, ale także reprezentantów nauki czy przemysłu, których głównym zadaniem było opracowanie planu służącego zapobieganiu

---

[109] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 44-5.
[110] 111OECD, Computer Viruses and Other Malicious Software: A Threat to the Internet Economy [on-line], dostęp: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en#page1.
[111] International Telecommunication Union [on-line], dostęp: 1.05.2015, http://www.itu.int/en/about/Pages/overview.aspx.
[112] World Summit on the Information Society Geneva 2003 - Tunis 2005, WSIS-03/GENEVA/DOC/5-E, 12 December 2003.
[113] World Summit on the Information Society Geneva 2003 - Tunis 2005, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November2015.
[114] M. Gercke, *Understanding cybercrime: phenomena, challenges and legat response* [on-line], ITU 2012, dostęp: 3.05. 2015, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%201egislation%20EV6.pdf, s. 2-3.

cyberprzestępczości. Ich prace zakończyły się w 2008 roku publikacją raportu na temat ogólnoświatowej strategii przeciwko cyberprzestępczości pt. Global Strategie Raport[115].

Ponadto, wynikiem inicjatyw podjętych podczas WSIS było ustanowienie w 2007 roku Globalnej Agendy Cyberbezpieczeństwa (*Global Cybersecurity Agenda - GCA*), stanowiącej ramy współpracy międzynarodowej, mające na celu zwiększenie zaufania i bezpieczeństwa w społeczeństwie informacyjnym. GCA zakłada współpracę pomiędzy wszystkimi właściwymi partnerami, w oparciu o istniejące inicjatywy, aby uniknąć powielania wysiłków. Agenda działa w pięciu obszarach, obejmujących: instrumenty prawne, proceduralne oraz techniczne, struktury organizacyjne, współpracę międzynarodową i rozwój samopomocy[116].

Międzynarodowy Związek Telekomunikacyjny wydał także kilka rezolucji dotyczących cyberprzestępczości oraz był organizatorem konferencji dedykowanych temu zjawisku, a działający w ramach ITU Telecomunnication Development Sector przygotował opracowania poświęcone zwalczaniu przestępczości internetowej oraz towarzyszącym jej problemom legislacyjnym[117].

Istnieje zgodne stanowisko, co do tego, że cyberprzestępczość jest problemem, który obliguje do niezwłocznej reakcji międzynarodowej, a podjęta w odpowiednim czasie współpraca międzypaństwowa jest warunkiem koniecznym dla zapewnienia globalnego bezpieczeństwa. Nie należy jednak zapominać, że „bezpieczeństwo komputerów i sieci oparte jest na zachowaniu (...) równowagi między przeciwstawnymi czynnikami, zabezpieczeniem i dostępnością. Im bardziej system jest bezpieczny, tym trudniej dostępny i vice versa[118]". Zachowanie tej równowagi, przy jednoczesnym zapewnieniu dostatecznej ochrony, stanowi ogromne wyzwanie nie tylko dla ustawodawców, ale także dla całej społeczność międzynarodowej.

---

[115] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 32.
[116] International TelecommunicationUnion [on-line], dostęp: 3.05.2015, http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.
[117] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 33.
[118] D. Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Wydawnictwo HELION, Gliwice 2004, s. 61.

ROZDZIAŁ III
CYBERPRZESTĘPCZOŚĆ – WYBRANE ASPEKTY KRYMINOLOGICZNE

Cyberprzestępczość jest jednym z najpoważniejszych problemów, z którym muszą się zmierzyć gospodarki na całym świecie. W samych Stanach Zjednoczonych straty poniesione w 2011 roku szacuje się na 9 miliardów[119] dolarów, w Niemczech - na 6 miliardów . Natomiast w roku 2013 samo przestępstwo *phishingu* naraziło organizacje na całym świecie na straty sięgające niemal 6 miliardów dolarów[120].

Pomimo ciągnącej się pół wieku dyskusji na temat cyberprzestępstw, wykorzystywanie osiągnięć technologicznych do celów niezgodnych z prawem wciąż stanowi poważny dylemat zarówno dla ustawodawców, jak i organów egzekwujących prawo, a ataki są coraz częstsze, bardziej wyrafinowane i kosztowne.

3.1. CHARAKTER, ROZMIAR I TENDENCJE ZJAWISKA

Określenie skali zjawiska cyberprzestępczości jest niezwykle trudne, a wręcz wykracza poza zdolności poznawcze kryminologii. Zarówno Polska jak i wiele innych państw, nie dysponują wystarczającymi mechanizmami magazynowania danych, czego rezultatem są statystyki kryminalne dające jedynie przybliżony obraz rozmiaru zjawiska[121]. Decydują o tym chociażby problemy definicyjne oraz fakt, że sporządzający statystyki funkcjonariusze nierzadko mają problemy z właściwą kwalifikacją prawną czynów popełnionych w cyberprzestrzeni[122]. Ponadto, jest to zjawisko niezwykle dynamiczne, a różnorodność metod stosowanych przez sprawców praktycznie uniemożliwia ujęcie cyberprzestępczości w znanych nam mechanizmach kontroli[123].

Jest jednak jedna rzecz, którą z całą pewnością możemy powiedzieć o obszarze zagrożeń i bezpieczeństwie Internetu jako całości - zmienność. Kiedy wydawało się, że najistotniejszą kwestią jest samo naruszenie integralności i poufności danych, uwagę zwrócił sposób w jaki sprawcy uzyskują do nich dostęp. Uwidoczniło to poważne braki w systemach bezpieczeństwa. Zaczęto szukać odpowiedzi na pytanie jak sprawca wykorzystuje powstałą

[119] J. H. Peterson, L. Segal, A. Eonas, *Global Cyber Intermediary Liability: A Legal & Cultural Strategy*, 34 Pace L. Rev. 586 (2014), s. 586.
[120] RS A Cybercrime Report: The Current State of Cybercrime 2014. An Inside Look at the Changing Threat Landscape [on-line], dostęp: 5.05.2015, http://www.emc.com/collateral/white-paper/rsa-cyber- crime-report-0414.pdf.
[121] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 47-8.
[122] A. Adamski, *Cyberprzestępczość - aspekty prawne i kryminologiczne* [w:] „Studia Prawnicze", Zeszyt 4(166) 2005, Wydawnictwo Naukowe Scholar, Warszawa 2006, s. 68-9.
[123] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 47-8.

lukę, a nie jak dotychczas - jaki miała ona wpływ na wystąpienie zagrożenia[124].

Z raportu podsumowującego rok 2013 wynika, że aż 61% dorosłych użytkowników Internetu padło ofiarą cyberataków, a koszty tym spowodowane to 113 miliardów dolarów. Oznacza to, że liczba poszkodowanych w stosunku do roku 2012 nieznacznie spadła, co jednak nie przełożyło się na straty. Niepokojąca jest także liczba ataków na użytkowników telefonów komórkowych, która wynosi już 38% wszystkich posiadaczy. Badacze wskazują, że ten niepokojący stan rzeczy może wynikać z wykorzystywania tych samych urządzeń w pracy, jak i w domu, a także fakt, że wielu rodziców pozwala dzieciom na używanie ich prywatnego sprzętu[125]. Warto również zauważyć, że rozmiar i tendencje cyberprzestępczości w Polsce praktycznie nie różnią się od tych globalnych[126].

Ze względu na skalę oraz niestałość zjawiska, niemożliwym byłoby szczegółowe omówienie jego rozwoju, jednak warto zwrócić uwagę na kierunek, w którym zmierza, przedstawiony w najnowszym Raporcie Symantec Corporation.

Przede wszystkim zaobserwowano, że sprawcy działają znacznie szybciej, niż jednostki odpowiedzialne za bezpieczeństwo. Może być to spowodowane tym, że w przeciwieństwie do swoich ofiar, oni wciąż udoskonalają własne techniki działania. Dlatego też ofiarami cyberprzestępstwa są najczęściej małe i średnie organizacje, które mają zdecydowanie mniej środków do zainwestowania w bezpieczeństwo sieciowe[127]. Ponadto, dzisiejsi przestępcy są na tyle wykwalifikowani, a także dysponują odpowiednimi środkami ku temu by prowadzić swoją działalność szpiegowską miesiącami czy nawet latami[128].

Równie niepokojący jest wzrost liczby szkodliwego oprogramowania oraz ataków z jego wykorzystaniem - w 2014 roku powstało ponad 317 milionów takich programów, co oznacza, że prawie milion nowych zagrożeń trafiało do sieci każdego dnia. Samo użycie oprogramowania *ransomware* wzrosło w 2014 roku aż o 113%[129]. Polega ono na przeniknięciu do wnętrza atakowanego komputera i zakodowaniu danych będących własnością użytkownika. Następnie program umieszcza w imieniu przestępcy notatkę w komputerze, która zawiera żądania wobec właściciela cennych plików. Zwykle dotyczą one przelania pieniędzy na konto w banku elektronicznym w zamian, za które sprawca wyśle klucz oraz instrukcje,

[124]Symantec: Internet Security Threat Report 2015 [on-line], Volume 20, s. 4, dostęp: 11.05.2015: https ://www4. Symantec, co m/mktginfo/whitepaper/ISTR/21347932_GA-intemet-security-threat-report- volume-20-2015-social_v2.pdf.
[125] 2013 Norton Report [on-line], dostęp: 11.05.2015, http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-infographic.en-us.pdf.
[126] Zob. http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pl_pl.pdf.
[127] Symantec: Internet Security Threat Report, op. cit, s. 5-7.
[128] Ibidem, s. 102.
[129] Ibidem, s. 7.

umożliwiające odzyskanie danych. Przypuszcza się, że prawdopodobieństwo stania się ofiarą cyberprzestępstwa jest znacznie wyższe niż przy przestępstwie pospolitym.

Szkodliwe oprogramowanie może być także wykorzystywane do tworzenia tzw. botów, będących obecnie jednym z najbardziej popularnych i złożonych rodzajów przestępczości internetowej. Jest to odmiana programu destrukcyjnego, umożliwiająca sprawcy objęcie kontroli nad komputerem. Najczęściej boty rozprzestrzeniają się przez Internet, wyszukując pozostawione bez ochrony komputery, które można zainfekować, wykorzystując luki występujące w zabezpieczeniach. Następnie pozostają w ukryciu aż do momentu otrzymania dyspozycji. Zaatakowany komputer może zostać użyty do wykonania rozmaitych zautomatyzowanych zadań, jak np. rozsyłania spamu, wirusów, kradzieży numerów kart kredytowych, czy innych osobistych danych[130] 76% *spamu* rozesłanego w 2013 roku było efektem funkcjonowania botów[131], a liczbę aktywnie działających szacowano wtedy na ok. 62 tys. [132].

Kolejnym problemem jest wykorzystywanie przez sprawców portali społecznościowych. 70% oszustw popełnionych przy ich użyciu wynika z faktu, że jesteśmy bardziej skłonni do „klikania" w treści zamieszczone przez osoby nam znane[133] Według danych pochodzących z sieci Kaspersky Security Network, w 2013 roku strony phishingowe naśladujące platformy społecznościowe odpowiadały za ponad 35% zamachów, z czego 22% stanowiły strony imitujące Facebook'a. Produkty firmy Kaspersky rejestrują każdego dnia ponad 20 tys. prób kliknięcia w odsyłacze kierujące na fałszywe strony popularnego portalu[134].

Interesujące jest także zainteresowanie cyberprzestępców materiałami wspierającymi sprzedaż, bankomatami, czy nawet domowymi routerami. Ataki na te urządzenia pokazują, że już nie tylko nasze komputery są narażone na niebezpieczeństwo. Sytuację pogarsza fakt, że coraz więcej urządzeń może być obsługiwanych poprzez telefon komórkowy. Wynika to z faktu, że ¼ ankietowanych przyznała, że nie wie na dostęp do jakich informacji wyraziła zgodę podczas instalacji aplikacji, a aż 68% byłoby skłonnych do handlu swoją prywatnością w zamian za darmowy program[135].

---

[130] Norton, *Boty i sieci typu „ bot" - rosnące zagrożenie* [on-line], dostęp: 12.05.2015, http://pl.norton.com/botnet.
[131] Symantec: Internet Security Threat Report 2014 [on-line], Volume 19, dostęp: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_intemet_threat_report_ITU2014.pdf.
[132] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 52.
[133] Ibidem, s. 8.
[134] Securelist - Information about Viruses, Hackers and Spam, *Oszustwa wykorzystujące portale społecznościowe* [on-line], dostęp: 12.05.2015, http://securelist.pl/analysis/7280,oszustwa_wykorzystujace_portale_spolecznosciowe.html.
[135] Symantec: Internet Security Threat Report, op. cit, s. 8.

Ciągły wzrost liczy użytkowników Internetu, a przed wszystkim obniżenie się ich wieku w połączeniu ze znaczącą zależnością coraz większej ilości instytucji od technologii informacyjnych, ukazuje jak bardzo poważne konsekwencje może mieć cyberprzestępczość[136].

3.1.1. PRZESTĘPSTWA ZWIĄZANE Z PODMIOTOWYM WYKORZYSTANIEM SYSTEMÓW KOMPUTEROWYCH

Wykorzystanie Internetu w celu popełnienia takich przestępstw pospolitych jak fałszerstwo, czy oszustwo jest zarówno tańsze, jak i trudniejsze do wykrycia. Ponadto, stwarza to możliwość dotarcia do zdecydowanie większej liczby potencjalnych ofiar i rozszerza zakres działania sprawcy. Takie przestępstwa, jak publikacja fałszywych treści na zakładanych w tym celu stronach internetowych, czy oszukańczy handel za pośrednictwem sieci, pozostają w bezpośrednim związku z przemianami społeczno-gospodarczymi dokonującymi się w społeczeństwie[137].

Tab. 1. Liczba stwierdzonych przestępstw w sieci w latach 2005-2011.

Rok	**Wszystkie przestępstwa popełnione w sieci**	**Oszustwa**
2005	3.445	2.804
2006	3.922	3.597
2007	7.467	5.787
2008	4.015	2.848
2009	6.124	4.915
2010	7.733	6.260
2011	14.157	11.406
2012	19.042	15.370

Źródło: Dane Statystyczne Komendy Głównej Policji[138].

Powyższe dane świadczą o rosnącej skali zjawiska. Coraz większa liczba użytkowników komputerów, a także podmiotów oferujących w sieci towary i usługi, także wpływa na ten wynik. W 2012 roku liczba przestępstw popełnionych w Internecie wyniosła ogółem 19.042, co stanowi wzrost aż o 452,7% w porównaniu do roku 2005, a najczęściej były to różnorakie oszustwa. Na szczęście wykrywalność tego rodzaju przestępstw także jest wysoka

[136] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 61.
[137] Ibidem, s. 72.
[138] Zob. http://www.statystyka.policja.pl/st/informacje/85606,Przestepstwa-w-sieci.html?search=95332007

- w 2012 roku wyniosła ona ponad 86 %, co oznacza, że średnio w 4/5 postępowań, udało się ustalić osobę podejrzanego.

Jednak dane Komendy Głównej Policji nie podają informacji na temat innych niż oszustwo przestępstw popełnianych z wykorzystaniem Internetu. Powoduje to, że nie da się w sposób wyczerpujący określić skali tego zjawiska. Widoczny wzrost wykrytych ataków, może być także wynikiem nowelizacji, które dokonały się w ostatnich latach - przepisy Kodeksu karnego uległy zmianie, a także wprowadzono nowe rodzaje przestępstw. Niemniej, ta wyraźna tendencja wzrostowa jest także widoczna w innych państwach[139].

Zauważalny jest także wzrost liczby ataków na dobra niematerialne, stanowiące przedmiot własności intelektualnej. Wartość cyfrowego rynku muzycznego szacuje się na 15 miliardów dolarów[140], co jest równoznaczne ze zwiększeniem się zagrożeń dla interesów majątkowych twórców, czy też właścicieli prawa autorskich – nielegalne kopiowanie oraz rozpowszechnianie treści objętych ochroną[141].

Ogromnym problemem jest także handel produktami podrabianymi i pirackimi, który przyniósł szereg negatywnych skutków dla konsumentów, przemysłu, administracji, a także gospodarki jako całości. Kupujący są szczególnie narażeni na zakup podrobionych produktów, które ich zdaniem są prawdziwe. Państwo jest narażone na utratę dochodów pochodzących z podatków, czy nawet wolniejszy rozwój gospodarki spowodowany stratami poniesionymi przez sektor handlowy[142]. Rozpowszechnianie tego typu towarów wzrosło wraz z popularnością sklepów internetowych, gdzie ryzyko, jakie podejmuje nabywca jest zdecydowanie większe.

Szczególną odmianą tego zjawiska jest piractwo komputerowe, czyli bezprawne kopiowanie lub rozpowszechnianie programów komputerowych objętych ochroną prawną. Może ono polegać na powielaniu, pobieraniu, sprzedaży, czy instalowaniu większej ilości kopii programu niż przewiduje to licencja. Wiele osób nie wie, że kupno oprogramowania to jedynie nabycie licencji na korzystanie z programu, a nie jego rzeczywisty zakup. Licencja dokładnie określa, ile kopii można zainstalować. Wykonanie większej ilości duplikatów może już zostać uznane za piractwo komputerowe[143]. Straty, które ono generuje wynikają zarówno z wartości

---

[139] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 72-3.
[140] International Federation of the Phonographic Industry: Global Statistics [on-line], dostęp: 12.05.2015, http://www.ifpi.org/global-statistics.php.
[141] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 74.
[142] United States Government Accountability Office: Report to Congressional Committees, *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, GAO-10-423, April 2010.
[143] Business Software Alliance, *Czym jest piractwo komputerowe?* [on-line], dostęp: 12.05.2015, http://ww2.bsa.org/country/Anti-Piracy/What-is-Software-Piracy.aspx?sc_lang=pl-PL.

przedmiotu zamachu jakim są programy komputerowe, jak i utraconych korzyści.

W 2012 roku 75% użytkowników komputerów na świecie przyznało się do piractwa. Ankieta została przeprowadzona na grupie 15 tys. osób z 33 krajów, a wynik ten znacznie wzrósł w porównaniu do 42 % w roku 2011. Ponadto, 5 % ankietowanych otwarcie oświadczyło, że zawsze korzysta z nielegalnego oprogramowania, a jedynie 38% przyznaje, że nie korzysta z nielicencjonowanych materiałów. Warto również dodać, że 5% badanych odmówiło udzielenia odpowiedzi. Wartość handlową strat jakie poniósł przemysł zajmujący się produkcją oprogramowania szacowano w 2012 roku na pond 63 miliardy dolarów[144].

Ta krótka analiza przestępczości związanej z przedmiotowym wykorzystaniem systemów komputerowych prowadzi do niepokojących wniosków. Okazuje się, że brak dostatecznej wiedzy użytkowników na temat zagrożeń, z jakim wiąże się korzystanie z Internetu to tylko część problemów, z jakimi musimy się zmierzyć. Zdecydowanie bardziej alarmujący jest fakt, że wiele osób świadomie dopuszcza się działań niezgodnych z prawem, co nie tyle wynika z ich niewiedzy, a raczej bagatelizowania ich szkodliwego znaczenia. Wydaje nam się, że na pozór małe przewinienie, nie jest w stanie spowodować znaczących szkód, zapominając o skali zjawiska i milionach innych osób, które myślały tak samo.

3.2. ODPOWIEDZIALNOŚĆ ZA PRZESTĘPSTWA POPEŁNIONE W CYBERPRZESTRZENI

Jedną z najważniejszych materii wymagających rozstrzygnięcia jest ustalenie, kogo należy obciążyć odpowiedzialnością kamą za przestępstwo popełnione w sieci. Nie chodzi tu jednak o stwierdzenie, czy spełnione zostały przesłanki z art. 1 k.k., będące podstawą odpowiedzialności, lecz wyodrębnienie kręgu podmiotowego osób, które odpowiedzą w związku ze stwierdzonym przestępstwem sieciowym. Najpierw należy określić, czy w ogóle, a jeżeli tak, to jakiego czynu zabronionego dopuściła się dana osoba, a następnie sprawdzić czy przepisy polskiego Kodeksu karnego będą miały zastosowanie w tym przypadku[145].

Nie ulega wątpliwości, że odpowiedzialności karnej, jako sprawca wykonawczy, podlega autor materiałów wprowadzonych do sieci. Sprawcą takim będzie zarówno sam autor naruszającego prawo tekstu, jak również osoba decydująca się na jego umieszczenie na swojej stronie, z zaznaczeniem, że utożsamia się z jego treścią - przytoczenie cudzego tekstu z zamiarem podjęcia polemiki nie jest karalne. Zatem przez sprawcę wykonawczego należy

---

[144] B. Fitzgerald, *Software Piracy: Study Claims 57 Percent OfThe WorldPirates Software* [w:] The HuffingtonPost [on-line], dostęp: 13.05.2015, http://www.huffingtonpost.coin/2012/06/01/software- piracy-study-bsa_n_1563006.html.

[145] M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych,* op. cit., 62-79.

rozumieć użytkownika końcowego, popełniającego czyn niezgodny z prawem za pośrednictwem sieci. Natomiast nie będzie nim jednostka, która jedynie zapoznała się z nielegalnymi treściami zamieszczonymi przez osoby trzecie[146].

Oprócz sprawców wykonawczych, odpowiedzialność ponoszą także pomocnicy. Kodeks karny przewiduje taką odpowiedzialność w art. 18 § 3, jako zjawiskową postać przestępstwa, którego celem jest ułatwienie innej osobie popełnienia czynu zabronionego. Udzielenie pomocy może polegać m.in. na dostarczeniu narzędzia, którym będzie każdy przedmiot upraszczający dokonanie czynu niezgodnego z prawem, a osobisty kontakt udzielającego pomocy ze sprawcą nie jest konieczny. Karalne pomocnictwo może przyjąć także formę zaniechania, kiedy to na pomocnika nałożony jest szczególny, prawny obowiązek niedopuszczenia do popełnienia czynu zabronionego. Istotą pomocnictwa jest zamiar bezpośredni lub wynikowy, a ponadto, pomocnik musi posiadać wyobrażenie danego czynu[147]. Warto zatem zauważyć, że niemal wszystkie firmy udostępniają miejsce na serwerach z zastrzeżeniem w regulaminie, że umieszczanie przez użytkownika treści niezgodnych z prawem będzie stanowiło przesłankę do usunięcia strony[148].

3.2.1. Odpowiedzialność dostawców dostępu do Internetu

Dyskusyjna jest natomiast odpowiedzialność dostawców dostępu do sieci Internet. Czy można ich obciążyć odpowiedzialnością pośrednią za działania, o których wiedza będzie im trudna do udowodnienia? Dotychczas udawało im się uniknąć odpowiedzialności, mimo że, znajdują się w korzystnej sytuacji do monitorowania i kontrolowania cyberprzestępczości [149].

Usługodawca jest jednym z podmiotów pośredniczących w procesie uzyskiwania dostępu do sieci. Jednak zakres pojęcia pośrednictwa jest szerszy niż mogłoby się wydawać - do kręgu dostawców pośredniczących zaliczamy cztery grupy osób, biorące udział w udostępnianiu i rozpowszechnianiu treści w Internecie, a mianowicie: dostawców treści, operatorów sieci telekomunikacyjnej, dostawców dostępu do sieci i dysponentów oraz dostawców usług internetowych[150]. Charakteryzuje ich nie tylko odmienność świadczonych usług, ale także zróżnicowane możliwości techniczne reakcji na informacje o naruszeniach,

---

[146] B. Hołyst, *Kryminologia,* LexisNexis Polska, Warszawa 2009, s. 405.
[147] K. Buchała, A. Zoll, *Kodeks karny. Komentarz. Część ogólna. Komentarz do art. 1-116 Kodeksu karnego,* Warszawa 1998, s. 184-8.
[148] B. Hołyst, *Kryminologia,* op. cit., s. 405-6.
[149] J. H. Peterson, L. Segal, A. Eonas, *Global Cyber Intermediary Liability: A Legał & Cultural Strategy*, op. cit., s. 291.
[150] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Wolters Kluwer Polska, Warszawa 2011, s. 227.

mające bezpośredni wpływ na zakres odpowiedzialności[151]. Jednak zdarzają się sytuacje, w których ten sam podmiot pełni więcej niż jedną funkcję, np. poprzez połączenie samej dostawy Internetu z innymi usługami, co znacznie utrudnia zdefiniowanie określonych ustawodawców[152].

Zasady odnoszące się do odpowiedzialności podmiotów pośredniczących zostały sformułowane w oparciu o model horyzontalny oraz usystematyzowane w Dyrektywie o handlu elektronicznym[153], a na tle prawa polskiego, także ustawie o świadczeniu usług drogą elektroniczną [154]. Wybór takiego modelu pozwala na pociąganie usługodawców do odpowiedzialności za rozpowszechnianie materiałów naruszających nie tylko normy prawa karnego, ale również cywilnego, administracyjnego, czy też prawo autorskie.

Dyrektywa odpowiada na pytanie kogo i na jakich zasadach można obciążyć winą za wykorzystywanie sieci telekomunikacyjnych w celu rozpowszechniania informacji zabronionych przez prawo. Tematem regulacji jest nie tylko odpowiedzialność sprawcy, ale także usługodawców, czyli osób stwarzających techniczne warunki dostępu do takich treści. W zależności od możliwości wyłączenia odpowiedzialności, wyróżniono trzy sfery działalności usługodawców: *mere conduit, caching* oraz *hosting*[155].

Mere conduit, czyli zwykły przesył, to usługi polegające na byciu jedynie łącznikiem w dostępie do sieci telekomunikacyjnej, bądź przenoszeniu treści wprowadzonych przez użytkownika (np. dostawca usług internetowych). W tym przypadku o wyłączeniu możemy mówić tylko w sytuacji, gdy usługodawca nie jest inicjatorem przekazu, nie dokonuje wyboru adresatów, czy przesyłanych treści, a także nie podejmuje się ich modyfikacji. Usługodawca nie będzie również odpowiadał za automatyczny i tymczasowy zapis informacji wynikający z samej transmisji. Oznacza to, że ISP (*Internet Service Provider*) nie ponosi odpowiedzialności za popularyzowanie treści niezgodnych z prawem przy użyciu komunikacji bezpośredniej[156].

Przez *caching* należy rozumieć samoczynny, pośredni oraz krótkotrwały zapis informacji, mający na celu wzrost efektywności ich udostępniania, dokonywany na życzenie

---

[151] A. Kuczerawy, *Odpowiedzialność dostawcy usług internetowych* [on-line], Biblioteka Cyfrowa Uniwersytetu Wrocławskiego, dostęp: 6.05.2015, http://www.bibliotekacyfrowa.pl/Content/23625/Odpowiedzialnosci_dostawcy_uslug_intemetowych.pdf.
[152] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, op. cit., s. 230.
[153] Dyrektywa Parlamentu i Rady WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego tynku (2000/31/WE).
[154] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2002 nr 144, poz. 1204.
[155] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, op. cit., s. 231-2.
[156] Ibidem, s. 232.

usługobiorcy. Zwolnienie dostawcy z odpowiedzialności jest możliwe gdy: nie będzie on modyfikował przechowywanych treści, będzie respektować warunki dostępu do informacji oraz zasady ich uaktualniania, a korzystając z informacji będzie stosował technologie zgodne z prawem oraz gdy podejmie natychmiastowe działania w celu usunięcia nielegalnych treści[157].

Hosting to zapewnienie osobom trzecim miejsca na serwerach włączonych do sieci telekomunikacyjnej w celu przechowywania, gromadzenia oraz udostępniania wprowadzanych przez nie informacji. Wyłączenie odpowiedzialności ISP może nastąpić jedynie w przypadku, gdy nie ma on faktycznej wiedzy o działalności użytkownika, bądź o tym, że przechowywane treści są niezgodne z prawem, jednocześnie nie będąc świadomym co do okoliczności i faktów potwierdzających takową nielegalność[158].

Odpowiedzialność stron pośredniczących w wymianie informacji jest uzależniona od ich wiedzy o charakterze przechowywanych lub udostępnianych treści oraz technicznej możności ich usunięcia czy zablokowania, dlatego też nie może się ona opierać na regułach ogólnych. Trudno uznać za współodpowiedzialnych udostępniania oraz rozpowszechnia treści niezgodnych z prawem, operatorów sieci, czy też przedsiębiorstwa telekomunikacyjne, których rola sprowadza się jedynie do zagwarantowania fizycznego dostępu do Internetu. Choć dostawca dostępu do Internetu, a także dysponent sieci mogą zamknąć dostęp do określonego serwera, jest to o tyle skomplikowane, że blokada treści niezgodnych z prawem będzie równoznaczna z uniemożliwieniem dostępu do pozostałych informacji. Odpowiedzialności nie ponosi także ISP, jeżeli poinformowany o istnieniu nielegalnej treści zaprzestanie jej dalszego rozpowszechniania[159].

3.3 WYKRYWALNOŚĆ CYBERPRZESTĘPCZOŚCI

Internet to przedmiot dyskusji wszystkich zainteresowanych kwestią bezpieczeństwa narodowego. Niewinni ludzie codziennie padają ofiarą ataków, a większość z nich, zwłaszcza w krajach rozwijających się, nadal nie jest świadoma praw jakie przysługują im w sieci. Przestępstwa komputerowe wpływają na nasze życie i bezpieczeństwo w większym stopniu, niż mogłoby się nam wydawać. Tradycyjne metody śledcze nie są wystarczające do wykrywania, dochodzenia i ścigania cyberprzestępczości. Ten rodzaj przestępczości wymaga aktywnej współpracy na szczeblu międzynarodowym, a także partnerstwa publiczno-prywatnego, bez których powstrzymanie sprawców może okazać się niemożliwe[160].

---

[157] Ibidem.
[158] Ibidem, s. 232-3.
[159] Ibidem, s. 255-7.
[160] V. Sekgwathe, M. Talib, *Cyber Crime Detection andProtection: Third World Still to Cope-Up* [w:]

3.3.1. CZYNNIKI UTRUDNIAJĄCE ŚCIGANIE

Za przyczynę wzrostu zagrożenia przestępczością komputerową uznaje się przede wszystkim brak wystarczającej wiedzy o tym zjawisku, a także odpowiedniego oprogramowania, które umożliwiłoby jego wykrycie [161] . Cechą charakterystyczną cyberprzestępczości jest duża „ciemna liczba", niewielkie szanse na wykrycie sprawcy, niechęć podmiotów pokrzywdzonych do informowania policji o zaistniałych zamachach oraz lekceważenie przez ofiary środków bezpieczeństwa[162].

Szacuje się, że rocznie ofiarą cyberataków pada ponad 500 milionów osób[163]. Jednak prawdopodobieństwo ich wykrycia jest wciąż niewielkie, chociażby dlatego, że część ataków pozostaje niezauważona przez poszkodowanych. Problemem jest także, już wspomniana, niechęć do składania zawiadomień policji, co wynika z zamiaru uniknięcia rozgłosu i obawy przed utratą zaufania (banki, instytucje finansowe oraz rządowe, uniwersytety). Co ciekawe, wielu pokrzywdzonych nie informuje policji o zamachach, wychodząc z założenia, że zapewnienie jej dostępu do systemu komputerowego, może okazać się zbyt kłopotliwe, czy nawet ryzykowne. Wielu poszkodowanych zdaje sobie także sprawę z tego, że do naruszenia doszło na skutek ich własnych zaniedbań i braku właściwego zabezpieczenia. W momencie, gdy brak takiego zabezpieczenia stanowić będzie uchybienie obowiązku prawnego, nałożonego na administratora systemu, bądź kierownictwo pokrzywdzonej instytucji, niezawiadomienie policji ma także inne uzasadnienie. W przypadku banków bądź innych instytucji, którym szczególnie zależy na zaufaniu konsumentów, alternatywą dla powiadamiania policji jest skorzystanie z usług firm prywatnych, specjalizujących się w tematyce bezpieczeństwa sieciowego[164].

Czynnikami utrudniającymi ściganie cyberprzestępczości są także niedopracowane przepisy prawne, brak odpowiedniego przygotowania funkcjonariuszy policji oraz organów wymiaru sprawiedliwości, a także stosunkowo liberalne podejście opinii publicznej do sprawców ataków. Wielu sędziów, czy też oskarżycieli nie posiada wystarczającej wiedzy na

---

E. Ariwa, E. El-Qawasmeh, E. Sedoyeka, J. J. Yonazi (red.), *e-Technologies and Networks for Development,* Springer-Verlag, Berlin 2011, s. 171.

[161] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 77.

[162] A. Adamski, *Crimes Related to Computer NetWork. Threats and Opportunities: A Criminological Perspective*, [w:] M. Joutsen (red.), *Five Issues in European Criminal Justice: Corruption, Women in the Criminal Justice System, Criminal Policy Indicators, Community Crime Prevention and Computer Crime,* HEUNI, Publication Series No. 34, Helsinki 1999, s. 218.

[163] GO-Gulf: Cyber Crime Statistic and Trends [Infographic] [on-line], dostęp: 11.05.2015, http://www.go-gulf.com/blog/cyber-crime/.

[164] A. Adamski, *Prawo karne komputerowe,* op. cit., 17-20.

temat nowoczesnych technologii, aby móc w pełni rozumieć problematykę omawianego zjawiska. Podobnie wygląda sytuacja pełnomocników oskarżonych, którzy mają problemy z oceną dowodów występujących w postaci elektronicznej[165]. Z elektronicznym materiałem dowodowym należy obchodzić się niezwykle ostrożnie, ponieważ sprawca może go z łatwością usunąć bądź uszkodzić. Brak wystarczającej wiedzy w tym zakresie może skutkować odrzuceniem dowodu przez sąd, niezależnie od tego, jak dosadnie udowadnia on winę oskarżonego[166].

Ściganie przestępstw popełnianych z wykorzystaniem Internetu utrudnia także, a może przede wszystkim, ich transgraniczny charakter - transfer danych przebiega zazwyczaj przez terytorium kilku państw. Stawia to współczesnych ustawodawców przed niezwykle trudnym zadaniem, jakim jest unifikacja prawa karnego oraz współpracy organów ścigania reprezentujących dotknięte przestępstwem państwa. Ujęcie sprawcy jest nie tylko uzależnione od ustalenia miejsca jego pobytu, czy zgromadzenia dowodów, ale przede wszystkim od pogodzenia, często bardzo odmiennych, standardów kryminalizacji poszczególnych przestępstw. Utrudnia to także fakt, że przestępcy coraz częściej wybierają na miejsce działania kraje, których system legislacyjny nie jest kompletny, bądź legislacja może okazać się trudna do wyegzekwowania[167].

3.3.2. Działalność Prokuratury i sądów

Mimo wciąż rosnącej skali cyberzagrożeń liczba postępowań karnych w sprawach o przestępstwa przeciwko przetwarzanej elektronicznie informacji, wszczynanych na terenie Rzeczypospolitej Polskiej jest wciąż niezadowalająca. Do okoliczności tłumaczących taki stan rzeczy, zalicza się wymienione wcześniej czynniki, jak: technologicznie zaawansowana natura zjawiska, nieujawnianie przez pokrzywdzonych nadużyć, niedoskonałość regulacji prawnych, czy niewystarczająca wiedza reprezentantów wymiaru sprawiedliwości o charakterze postępowania dowodowego z zakresu cyberprzestępczości. Potwierdzeniem tej teorii są przedstawione poniżej dane statystyczne, ukazujące dynamikę i rozkład zgłaszanych zamachów w stosunku do liczby prawomocnych wyroków[168].

---

[165] Ibidem, 22-3.
[166] D. Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, op. cit., s. 546-7.
[167] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 78.
[168] A. Adamski, *Cyberprzestępczość - aspekty prawne i kryminologiczne*, op. cit., s. 73.

Tab. 2. Prawomocne skazania osób dorosłych w latach 2001-2012.

Rok	Uzyskanie dostępu do informacji (art. 267 § 1)	Podsłuch (art. 267 § 3)	Zniszczenie bądź zmiana istotnej informacji (art. 268 § 2)	Zniszczenie bądź zmiana istotnej informacji (art. 269 § 1-2)	Oszustwo komputerowe (art. 287 § 1-2)
2001	14	5	2	6	31
2002	18	2	5	3	23
2003	14	4	3	1	46
2004	22	5	7	-	45
2005	25	10	6	5	43
2006	22	8	7	1	58
2007	23	16	7	3	51
2008	29	6	13	3	62
2009	42	3	5	1	49
2010	52	-	11	2	46
2011	37	1	5	-	52
2012	29	3	2	-	56

Źródło: Informator Statystyczny Wymiaru Sprawiedliwości[169].

Już z pobieżnej analizy danych statystycznych wynika, że dwie zasadnicze kategorie cyberprzestępstw, jakimi są czyny skierowane przeciwko mieniu oraz czyny naruszające bezpieczeństwo systemów komputerowych, spotykają się z bardziej stanowczą reakcją podmiotów pokrzywdzonych, co bezpośrednio przekłada się na liczbę wyroków - są one zdecydowanie częściej ścigane niż zamachy na bezpieczeństwo przetwarzanej elektronicznie informacji[170].

Potwierdzają to wyniki badań praktyki prokuratorskiej zarówno w sprawach przestępstw skierowanych przeciwko bezpieczeństwu sieci i systemów komputerowych jak i popełnionych z ich wykorzystaniem. Wśród 658 spraw o tego typu przestępstwa, w których postępowanie przygotowawcze zakończyło się decyzją o jego umorzeniu bądź skierowaniem aktu oskarżenia do sądu, aż 79% stanowiły czyny zakwalifikowane jako oszustwa. Zamachy na dostępność, poufność, czy integralność danych teleinformatycznych, będących przecież cyberprzestępstwami w dosłownym tego słowa znaczeniu, stanowiły niewiele ponad 3% spraw będących tematem badań. Choć dane te pochodzą z lat 2001-2002, sytuacja praktycznie nie uległa zmianie. Mimo dużej liczby ataków, ich celem są przede wszystkim dobra niemajątkowe i prawdopodobnie dlatego tolerancja społeczna jest większa niż w przypadku zamachów na mienie[171].

[169] Zob. http://isws.ms.gov.pl/pl/baza-statystyczna/.
[170] A. Adamski, *Cyberprzestępczość - aspekty prawne i kryminologiczne*, op. cit., s, 73.
[171] Ibidem, s. 73-4.

Nie można jednak zapominać, że Internet stale się rozwija, co stwarza nie tyko nowe możliwości, ale będzie także przyczyną coraz to nowszych konfliktów i napięć, a brak podjęcia odpowiednich działań w kierunku ochrony sieci i systemów komputerowych, w sytuacji wciąż rosnącej od nich zależności człowieka, może być katastrofalny w skutkach[172].

3.4. ZAPOBIEGANIE CYBERPRZESTĘPCZOŚCI

Podejmowane środki zapobiegania cyberprzestępczości nie mogą się jedynie ograniczać do stanowienia odpowiednich dla tej materii przepisów prawa, bowiem te nie są w stanie powstrzymać wszystkich przypadków nielegalnego wykorzystania Internetu[173]. Ze względu na złożoność omawianego zjawiska, realizacja przepisów prawa karnego wciąż stanowi pewną nowość w ujęciu kryminologicznym, a także samym systemie prawa oraz wkracza niezwykle głęboko w obszar techniczny funkcjonowania systemów przetwarzania danych[174]. Sprawcy często korzystają z różnic w zakresie kryminalizacji, czy też rozwiązań technologicznych znacznie utrudniających ich identyfikację. Dlatego też, z punktu widzenia eliminacji zachowań przestępczych, o wiele bardziej skuteczną metodą od represji karnej wydaje się być zredukowanie ryzyka popełnienia tego typu nadużyć w oparciu o dostawców usług internetowych oraz samych użytkowników[175].

3.4.1. PROCEDURY TECHNICZNE SŁUŻĄCE PRZECIWDZIAŁANIU CYBERPRZESTĘPCZOŚCI

Ochrona systemów komputerowych i elektronicznie przetwarzanej informacji jest specjalnością zabezpieczeń techniczno-organizacyjnych. Są one tematem rozważań stosunkowo nowej gałęzi wiedzy - bezpieczeństwa komputerowego, a także przedmiotem zainteresowania producentów urządzeń i programów komputerowych, tworzonych w celu zapewnienia ochrony informacji. Przemysł zajmujący się produkcją dla potrzeb bezpieczeństwa sieciowego jest jednym z najlepiej rozwijających się modułów rynku komputerowego, którego obroty w skali globalnej, pochodzące jedynie ze sprzedaży oprogramowania antywirusowego, szacuje się na miliardy dolarów rocznie[176].

Doskonalenie oraz samo stosowanie metod i procedur technicznych mających na celu ochronę dobra prawnego jakim jest elektronicznie przetwarzana informacja, sprowadza się

---

[172] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 80.
[173] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, op. cit., s. 258.
[174] J. W. Wójcik, *Cyberprzestępczość. Wybrane zagadnienia kryminologiczne i* prawne, „Problemy Prawa i Administracji" 2011, nr 1, s. 155.
[175] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, op. cit., s. 258.
[176] Adamski, *Prawo karne komputerowe,* op. cit., s. 24.

przede wszystkim do zabezpieczeń wbudowanych w system operacyjny i działających na zasadzie kontroli dostępu. Ponadto, stosowane są uzupełniająco inne rozwiązania, mające przede wszystkim charakter programowy, jak np. zapory sieciowe (ang. *firewall),* oprogramowania antywirusowe, antyszpiegowskie i antyreklamowe czy antyspamowe. Popularne, a przede wszystkim dostępne dla każdego, są także rozwiązania dotyczące identyfikacji i uwierzytelniania podmiotu uprawnionego - hasła, kody dostępu, czy filtrowania treści, czego najlepszym przykładem jest tzw. kontrola rodzicielska[177].

Możliwe jest również uwierzytelnienie, czy też szyfrowanie informacji za pomocą metod kryptograficznych, uznawanych za niezastąpiony środek ochrony treści zamieszczanych w Internecie. Pozwalają one na ochronę poufności (może być poprawnie odczytana tylko przez osoby upoważnione) i autentyczności (jedynie upoważnione osoby mogą ją wygenerować w taki sposób, aby dała się potem poprawnie odczytać) informacji, poprzez ukrycie jej treści przed osobami nieupoważnionymi[178]. Według Adamskiego w środowisku jakim jest Internet, asymetryczne systemy kryptograficzne, działające na zasadzie klucza publicznego i prywatnego, najlepiej spełniają wymogi bezpieczeństwa oraz mają ogromne perspektywy rozwojowe, z uwagi na możliwość ich zastosowania w wielu dziedzinach życia[179]. Potwierdza to stanowisko Komisji Europejskiej, która uznaje stosowanie metod kryptograficznych za skuteczny sposób zapobiegania przestępstwom popełnianym przy użyciu kart płatniczych czy też szpiegostwa gospodarczego, nadużycia telekomunikacyjnego oraz innym formom piractwa w zakresie ochrony własności intelektualnej i mediów[180].

Podejmowane są również liczne inicjatywy zmierzające do blokowania bądź ograniczenia dostępu do nielegalnych treści poprzez zastosowanie technologii filtrujących. Możemy wyróżnić przynajmniej trzy systemy filtrowania: słowa klucze, pozytywne i negatywne listy oraz filtrowanie na podstawie oceny strony WWW.

Pierwsza metoda polega na skanowaniu stron WWW pod kątem występowania konkretnych słów czy elementów budowy. Wykorzystywane w tym celu oprogramowanie filtrujące blokuje dostęp do niechcianych treści. Wiele portali udostępnia takie oprogramowania, jak np. Liga Przeciwko Zniesławieniu *{The Anti-Defamation League* - ADL), ale można także nabyć filtry komercyjne, których zadaniem jest blokowanie wybranych przez

---

[177] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 80-1.
[178] D. Łydziński, *Kryptograficzne metody ochrony informacji* [on-line], dostęp: 9.05.2015, http://www.4itsecurity.pl/index.php/kategorie/hacking/62-kryptograficzne-metody-ochrony-informacji.
[179] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 26.
[180] EU Commision: Ensuring security and trust in electronic communication. Towards a European framework for digital signatures and encryption. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, (COM (97) 503 final).

użytkownika treści. Choć system pozwala na faktyczne zablokowanie określonych słów, może także dojść do uniemożliwienia dostępu do stron zawierających niegroźne treści, np. wyjaśniających szkodliwość rozpowszechniania zawartości, które chcieliśmy zablokować[181].

Oprócz systemów filtrujących na podstawie słów kluczy, istnieją również pozytywne i negatywne listy stron, czyli filtrowanie według adresów URL, polegające na ukryciu dostępu do konkretnych stron, bądź umożliwieniu dostępu tylko do wybranych witryn. Niewątpliwą zaletą tej metody jest możliwość dopisania kolejnych pozycji do listy „zakazanych" przez użytkowników końcowych, co jednak wiąże się z koniecznością częstej aktualizacji, wynikającą bezpośrednio z nieustannego powstawania nowych stron WWW. Problematyczne jest także tworzenie nowych list przez usługodawców, gdyż często użytkownicy końcowi czy też dostawcy nie mają wpływu na ich zawartość[182].

Warto również zwrócić uwagę na stworzony w 1995 roku system PICS (*Platform for Internet Content Selection*), działający w oparciu o klasyfikację treści storn WWW, która to pozwala na dołączenie stosowych etykiet do udostępnianych w Internecie materiałów. Podstawą klasyfikacji jest ocena sporządzona nie tylko przez autora, ale także odpowiedni program czy suwerenną organizację - każda etykieta zawiera również przynajmniej jedną ocenę urzędu klasyfikacji. Etykiety są umieszczane w nagłówkach stron, ich grupach, bądź całych witrynach [183]. Skuteczność systemu jest jednak zależna od liczby stron podlegających konkretnej kwalifikacji. Choć jego dopuszczalność budzi liczne wątpliwości ze względu na możliwe nadużycia w samoocenie autorów, ma on pozytywny wpływ na w rozwój kontroli indywidualnej dokonywanej przez użytkownika końcowego i może mieć wpływ na zmianę architektury Internetu[184].

Istotną kwestią dotyczącą ochrony systemów komputerowych i elektronicznie przetwarzanej informacji jest jej dobrowolny charakter. Wyjątkiem są jedynie te systemy komputerowe, w których przetwarzane są zbiory danych osobowych - ze względu na interes osób trzecich, administrator zbioru ma obowiązek ochrony ich poufności i integralności. Obowiązek ten wynika z samego prawa i należy do międzynarodowych standardów normatywnych z zakresu ochrony danych osobowych. Natomiast w sferze stosunków publiczno-prawnych jest on ograniczony do danych przetwarzanych przez sektor bankowy, telekomunikacyjny oraz organy administracji państwowej[185].

---

[181] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, op. cit., s. 279.
[182] Ibidem, s. 279-80.
[183] Ibidem, 280.
[184] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 82.
[185] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 27.

Zdarzają się także przypadki, w których polskie prawo warunkuje ochronę poufności i integralności informacji stosowaniem przez jej posiadacza stosowych zabezpieczeń. Wymóg ten wynika z art. 267 § 1 k.k., uzależniającego odpowiedzialność kamą za naruszenie bezpieczeństwa informacji od przełamania zastosowanych zabezpieczeń[186].

Niepokojący jest jednak fakt, że rozwiązania umożliwiające zabezpieczenie się przed zamachem nie są w pełni wykorzystywane, a świadomość zagrożeń związanych za użytkowaniem Internetu jest wciąż zatrważająco niska.

3.4.2. WSPÓŁPRACA Z WYSPECJALIZOWANYMI ORGANIZACJAMI

Kolejna metoda zwalczania cyberprzestępczości opiera się na rozwijaniu kooperacji pomiędzy organami ścigania, sektorem prywatnym oraz użytkownikami końcowymi[187]. Oceny zagrożeń dokonują także organizacje pozarządowe, opracowujące programy zapobiegania przestępczości[188].

W sferze współpracy oraz wsparcia operacyjnego między krajowymi i międzynarodowymi organami ścigania na szczególną uwagę zasługuje - wcześniej wspomniane - Centrum ds. Walki z Cyberprzetępczością, które ma chronić przedsiębiorstwa i obywateli UE przed zagrożeniami w sieci[189].

Istotna jest także działalność Zespołu ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego (CERT), którego zadaniem jest prowadzenie całodobowego nadzoru ruchu internetowego oraz podejmowanie natychmiastowych czynności w przypadku pojawienia się zagrożenia. W ramach tej organizacji powołany został CERT Polska, który działa od 1996 roku w strukturach Naukowej i Akademickiej Sieci Komputerowej (NASK) - instytutu badawczego kierującego działalnością naukową, krajowym rejestrem domen oraz dostarczającego zaawansowanych usług teleinformatycznych. Rdzeniem działalności zespołu jest rejestrowanie oraz obsługa zdarzeń zagrażających bezpieczeństwu sieci oraz współpraca z innymi zespołami, zarówno w Polsce, jak i na świecie. Ponadto, CERT prowadzi działania mające na celu zwiększenie świadomości w zakresie bezpieczeństwa teleinformatycznego i regularnie publikuje raporty dotyczące bezpieczeństwa polskich zasobów Internetu[190].

Działalność NGO w zakresie przeciwdziałania wykorzystywaniu Internetu w celach

---

[186] Ibidem, s. 28.
[187] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 83.
[188] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, op. cit., s. 265.
[189] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 83-4.
[190] CERT.PL, dostęp: 12.05.2015, http://www.cert.pl/o-nas.

sprzecznych z prawem powinna opierać się na współpracy z państwem, które jednocześnie powinno ułatwiać wymianę informacji oraz najskuteczniejszych sposobów blokowania szkodliwych treści. Konieczna jest także ocena efektywności dostępnych systemów filtrujących i udostępnienie tych danych opinii publicznej. Działania te powinny iść w parze ze staraniami w zakresie zwiększenia świadomości obywateli o występujących zagrożeniach oraz sposobach radzenia sobie z nimi[191].

Poza krokami podejmowanymi w celu zwalczania cyberprzestępczości u jej podstaw, istotna jest także współpraca z sieciami numerów interwencyjnych, umożliwiającymi zawiadomienie organów ścigania o sprzecznych z prawem działaniach mających miejsce w Internecie. Na szczególną uwagę zasługuje tzw. procedura notyfikacji - w przypadku wykrycia rozpowszechniania treści niezgodnych z prawem, dostawca świadczący usługę zostaje zawiadomiony o zaistniałej sytuacji i zobligowany do ich usunięcia. W przypadku braku odpowiedzi, zawiadomienie trafia do organów ścigania[192].

3.4.3. ZWIĘKSZANIE POZIOMU ŚWIADOMOŚCI UŻYTKOWNIKÓW

Nawet najlepsze przepisy nie będą skuteczne, jeżeli użytkownicy nie będą świadomi zagrożenia jakie niesie za sobą rozwój nowoczesnych technologii - dążenie do bezpieczeństwa to także propagowanie świadomego korzystania z sieci[193]. W wielu krajach programy edukowania w tym zakresie skierowane są już do najmłodszych konsumentów, co ma na celu nauczenie ich dokonywania oceny i klasyfikacji treści, na które mogą natrafić w Internecie. Szczególną aktywnością w tym obszarze wykazują się organizacje pozarządowe, organizujące szkolenia zarówno dla dzieci jak i młodzieży. W tym celu powstają także specjalne portale, jak np. chrondziecko.pl[194], dostarczające informacji o coraz to nowszych zagrożeniach oraz udostępniające oprogramowania filtrujące[195].

[191] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, op. cit., s. 265-271.
[192] Ibidem, s. 84.
[193] D. Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, op. cit., s. 394.
[194] Zob. http://www.chrondziecko.pl/.
[195] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 82.

ROZDZIAŁ IV
KONWENCJA RADY EUROPY Z 23 LISTOPADA 2001 ROKU I JEJ ODZWIERCIEDLENIE W POLSKIM KODEKSIE KARNYM

Konwencja Rady Europy o cyberprzestępczości z 23 listopada 2011 roku jest traktatem międzynarodowym, który ma na celu harmonizację krajowych przepisów dotyczących cyberprzestępczości, poprawę wewnątrzpaństwowych zdolności do jej wykrywania oraz zwiększenie współpracy międzynarodowej w tym zakresie. Oprócz państw członkowskich, udział w przygotowywaniu projektu Konwencji - w charakterze obserwatorów - wzięły także Kanada, Japonia, RPA i USA. Stany Zjednoczone, pomimo statusu obserwatora, odegrały szczególnie istotną rolę, przede wszystkim ze względu na większe doświadczenie w tej materii i przystąpiły do procesu z ugruntowanymi poglądami[196].

Zespół ekspertów - Europejski Komitet ds. Przestępczości, opracowywał projekt Konwencji przez prawie cztery lata, a jego prace zakończyły się przyjęciem tekstu przez Komitet Ministrów Rady Europy w dniu 8 listopada 2001 roku[197]. Podczas 109 sesji Komitetu w Budapeszcie, 23 listopada 2001 roku, Konwencja została otwarta do podpisu. Podpisała ją zdecydowana większość państw członkowskich, a także kraje, które wcześniej pełniły rolę obserwatorów. Weszła w życie 1 lipca 2004 roku po ówczesnej ratyfikacji przez 5 państw[198].

Konwencja Rady Europy jest pierwszym i jak dotąd jedynym aktem międzynarodowego prawa karnego z zakresu ścigania cyberprzestępstw, ponadto określającym jej podstawy. Przyczyną wszczęcia prac nad Konwencją była świadomość konieczności podjęcia wspólnej polityki kryminalnej w sferze sieci teleinformatycznych. Nowopowstałe, cyfrowe środowisko, przyczyniło się do rozwoju nowych form przestępczości, zasługujących na penalizację. Zauważono, że cyberprzestępczość stanowi poważne zagrożenie dla takich dóbr prawnych, jakimi są poufność, integralność czy też dostępność danych i systemów informatycznych, jak również dla elementarnych wartości respektowanych przez wszystkie państwa demokratyczne, którymi są poszanowanie praw mniejszości narodowych, religijnych i etnicznych, brak dyskryminacji oraz ochrona dzieci i młodzieży przed wykorzystywaniem seksualnym. Podkreślono także potrzebę zachowania równowagi między instrumentami mającymi zapewnić ochronę przed nowymi przestępstwami, a zabezpieczeniem podstawowych praw

[196] M. A. Vatis, The Council of Europę Convention on Cybercrime, s. 207 [on-line], dostęp: 13.05.2015, http://cs.brown.edu/courses/cscil950-p/sources/lecl6Watis.pdf.
[197] Ibidem, s. 209.
[198] Uzasadnienie projektu ustawy o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r., s. 4.

człowieka. Przede wszystkim chodzi tu prawo do wyrażania własnej opinii, co bezpośrednio wiąże się z możliwością pozyskiwania oraz dzielenia się wszelakiego rodzaju informacjami i ideami, bez względu na granice państwowe[199]. Konwencja ma na celu zapobieganie cyberprzestępczości, przy jednoczesnej ochronie prawnie umotywowanych interesów w użytkowaniu i rozwoju technologii informatycznych.

Konwencja przewiduje dotychczas nieznane rozwiązania, które mają ułatwić ściganie sprawców przestępstw popełnionych przy użyciu Internetu. Formułuje wytyczne dotyczące karalności oraz zasady odpowiedzialności osób prawnych, a także określa zasady jurysdykcji i przesłanki ekstradycji sprawców. Ponadto, Konwencja kładzie duży nacisk na szerzenie współpracy międzynarodowej w sprawach karnych. Sieci komputerowe o zakresie międzynarodowym umożliwiają swoim użytkownikom podejmowanie działań wykraczających poza terytorium jednego państwa, a mimo to wywołujących jednoczesne stuki na obszarze wielu krajów. Dlatego też konieczna jest bliska współpraca międzynarodowa, pozwalająca na stworzenie skutecznych ram prawnych ścigania cyberprzestępczości, mimo ograniczenia w postaci zasady terytorialności[200].

Z uwagi na fakt, że stronami Konwencji są aż 53 państwa, stanowi ona jedno z najefektywniejszych narzędzi międzynarodowej ochrony podmiotów wykorzystujących technologie komputerowe. Dotychczas jej ustalenia weszły w życie w 45 z nich, a 1 czerwca 2015 roku do tego grona dołączyła Polska. Przy obecnym natężeniu istniejących oraz pojawianiu się coraz to nowszych zagrożeń związanych z wykorzystywaniem sieci teleinformatycznych, nie jest możliwym eliminowanie tego typu przestępstw jedynie przez pojedyncze państwa.

Za przystąpieniem Polski do Konwencji Rady Europy przemawiał interes narodowy, a przede wszystkim potrzeba ochrony bezpieczeństwa teleinformatycznego państwa oraz pozostałych dóbr narażonych na ataki ze strony użytkowników Internetu. Istotna była także kwestia relacji politycznych wynikających z procesu integracji Polski z Unią Europejską, która to problemowi zwalczania cyberprzestępczości nadaje bardzo duże znaczenie[201].

4.1. PRAWO KARNE MATERIALNE

Aby współpraca międzynarodowa w zakresie zwalczania cyberprzestępczości była efektywna, konieczne jest przyjęcie jednorodnych środków karnych w ustawodawstwie

[199] Ibidem, s. 2-3.
[200] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Wydawnictwo „Dom Organizatora", Toruń 2001, s. 10-11.
[201] Ibidem, s. 11-12.

poszczególnych krajów. Transgraniczny charakter Internetu oraz sposobność naruszenia przy jego użyciu prawa innych państw przez sprawcę działającego na terenie jednego z nich, nie posiadającego odpowiednich unormowań, wskazuje na konieczność kryminalizacji nadużyć komputerowych w prawodawstwie jak największej liczby krajów. Warto tutaj zauważyć, że Polska należy do państw, które w istotnym stopniu przystosowały swój system prawny do obowiązujących w tym zakresie kanonów[202].

Podstawowym celem Konwencji Rady Europy o cyberprzestępczości jest unifikacja standardów prawnych w zakresie ścigania przestępstw teleinformatycznych - definicja czynów zabronionych oraz określenie reguł, na których ma się opierać współpraca międzypaństwowa. Sprzyja temu otwarta forma dokumentu, umożliwiająca przystąpienie państw, które nie są członkami Rady Europy, a także klauzule opcjonalne, będące przejawem kompromisu wypracowanego podczas pracy nad tekstem Konwencji i sprzyjające zaakceptowaniu jej postanowień przez państwa o różnorodnej kulturze oraz tradycji prawnej[203].

Przestępstwa konwencyjne sformułowano w taki sposób, aby zawierały one sugestie reprezentantów wszystkich krajów, które brały udział w pracach nad tą umową międzynarodową, a także odwoływały się do obowiązujących w tych państwach unormowań prawnych i praktyki związanej z ich wykorzystaniem. Ze względu na to, że w Konwencji posłużono się tzw. standardami minimalnymi karalności, przy implementacji możliwe było zrezygnowanie z pewnych elementów reglamentujących zakres odpowiedzialności karnej. Dotyczy to również subiektywnych przesłanek odpowiedzialności za przestępstwa konwencyjne, ograniczających się do umyślności, zarówno z zamiarem bezpośrednim, jak i ewentualnym[204].

Mogłoby się wydawać, że przepisy prawa polskiego w przeważającej części pozostają w zgodzie z postanowieniami Konwencji. Całkowitą zgodność rodzimego porządku prawnego z nowymi wymogami miała zapewnić ustawa z dnia 4 kwietnia 2014 roku o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw [205], wprowadzająca do polskiego ustawodawstwa postanowienia dyrektywy Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011[206] roku w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania

[202] Ibidem, s. 15-16.
[203] Ibidem, s. 16-17.
[204] Ibidem, s. 17.
[205] Ustawa z dnia 4 kwietnia 2014 r. o zmianie ustawy - Kodeks kamy oraz niektórych innych ustaw (Dz.U. 2014, poz. 538).
[206] Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (2011/93/UE), zastępująca decyzję ramową Rady 2004/68/WSiSW.

seksualnego dzieci oraz pornografii dziecięcej[207].

4.1.1. PRZESTĘPSTWA PRZECIWKO POUFNOŚCI, INTEGRALNOŚCI ORAZ DOSTĘPNOŚCI DANYCH INFORMATYCZNYCH I SYSTEMÓW KOMPUTEROWYCH

Ogromna wartość gospodarcza, jaką osiągnęła informacja w obecnych czasach jest bezsporna i tłumaczy fakt, że zaczęła być ona traktowana jak towar, którego posiadanie umożliwia osiągnięcie korzyści porównywalnych do tych, które wynikają z posiadania praw majątkowych. Konieczne jest zatem właściwe scharakteryzowanie przedmiotu ochrony, co może okazać się dość problematyczne, z uwagi na różnorodność przyjętej terminologii, a także brak konsekwencji w jej stosowaniu w polskim systemie prawnym[208].

Czym zatem jest informacja? Zgodnie ze słownikiem języka polskiego jest to „powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, pouczenie" [209]. Informacja jest wiadomością, która ma na celu zmniejszenie niepewności, czynnikiem zwiększającym prawdopodobieństwo podjęcia właściwej decyzji. Jednak aby zrozumieć czym jest informacja w pojmowaniu nauk prawnych, a sprzede wszystkim prawa karnego, należy dokonać rozróżnienia często utożsamianych ze sobą pojęć „informacja" i „dane" [210].

W kontekście prawnym na te określenia i występujące pomiędzy nimi różnice zwrócono po raz pierwszy uwagę w roku 1998 w raporcie niderlandzkiej komisji ds. przestępstw komputerowych, z którego to dowiadujemy się, że „przez dane, komisja (...) rozumie przedstawienie faktów, pojęć lub poleceń w ustalony sposób, który umożliwia ich przesyłanie, interpretację lub przetwarzanie zarówno przez ludzi, jak i w sposób zautomatyzowany. Informacja, to wywołany danymi efekt - zamierzony lub doświadczony przez ich użytkowników. Uzyskiwanie informacji lub informowanie innych polega na posługiwaniu się danymi (...). W przeciwieństwie do „informacji", „dane" są neutralne i przybierają uzgodnioną postać liter, znaków, wzorów, które mogą być przechowywane, przetwarzane lub przesyłane (...) [211]. Podobnie zinterpretowano omawiane zagadnienia w rekomendacji Organizacji Rozwoju i Współpracy Gospodarczej, przyjętej w sprawie Bezpieczeństwa Systemów Informatycznych, zgodnie z którą „dane" to „przedstawienie faktów, pojęć lub poleceń w sposób sformalizowany i umożliwiający ich komunikowanie,

---

[207] Uzasadnienie projektu ustawy o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r., s. 5-6.
[208] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 86.
[209] E. Sobol (red.), *Słownik Języka Polskiego,* Wydawnictwo Naukowe PWN, Warszawa 1994, s. 265.
[210] I. A. Jaroszewska, *Dostęp do informacji za pośrednictwem Internetu przez osoby nieuprawnione. Studium prawnokarne,* XLIV Międzynarodowe Seminarium Kół Naukowych "Koła Naukowe szkoła twórczego działania", Olsztyn 2015, s. 2.
[211] *Information Technology and Criminal Law, Report of Dutch Committee on Computer Crime, Ministry of Justice, the Hague, 1988* [w:] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 38.

interpretację lub przetwarzanie, zarówno przez ludzi, jaki i urządzenia;" informacja" (...) to znaczenie, jakie nadajemy danym przy pomocy konwencji odnoszących się do tych danych"[212].

„Należy zatem zauważyć, że dane są zapisem konkretnej informacji, jej nośnikiem, a informacja jako taka jest dopiero rezultatem ich interpretacji. Samo dysponowanie dostępem do danych nie jest tożsame z dostępem do zwartych w nich informacji. Podobnie, jak ich zniszczenie nie musi oznaczać zniszczenia informacji, a niedozwolone kopiowanie nie ma związku z kradzieżą - informacja to przedmiot ochrony przestępstw *stricte* komputerowych, a dane są przedmiotem wykonawczym tych przestępstw"[213].

W związku z rozwojem nowych systemów teleinformatycznych, elektronicznie przetwarzana informacja zyskała status samodzielnego dobra prawnego, i jako takie wymagała ochrony. Do kategorii przestępstw zagrażających jej bezpieczeństwu zakwalifikowano pięć rodzajów czynów:

a. nielegalny dostęp do systemu komputerowego,
b. nielegalne przechwytywanie danych,
c. naruszenie integralności danych polegające na ich uszkodzeniu, modyfikacji, zablokowaniu, usunięciu lub zniszczeniu,
d. naruszenie integralności systemu komputerowego, powodujące poważne zaburzenia w ich funkcjonowaniu, oraz
e. niewłaściwe użycie urządzeń polegające na produkcji, sprzedaży, imporcie, dystrybucji, pozyskiwaniu z zamiarem wykorzystania oraz udostępnianiu w jakikolwiek inny sposób.

Choć polski system prawny przewiduje penalizację większości z wyżej wymienionych czynów, to jednak standardy karalności zawarte w Kodeksie karnym nie zawsze odpowiadają tym, które zostały określone w Konwencji[214].

4.1.1.1. *Nielegalny dostęp*

Jak słusznie zauważył Adamski, uzyskanie nielegalnego dostępu do systemu komputerowego jest standardową postacią zamachu na bezpieczeństwo przetwarzanej elektronicznie informacji, a jego skuteczne dokonanie, skutkujące przejęciem kontroli nad

---

[212] R*ecommendation of the Council of the OECD concerning Guidelines for the Security of Information Systems OECD/GD (92) 10 Paris, 1992 (Aneks)* [w:] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 38.
[213] I. A. Jaroszewska, *Dostęp do informacji za pośrednictwem Internetu przez osoby nieuprawnione. Studium prawnokarne,* op. cit., s. 3.
[214] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* op. cit., s. 18.

zaatakowanym systemem, umożliwia popełnianie kolejnych przestępstw wymierzonych przeciwko różnorodnym dobrom prawnym[215]. Osobę, która dokonuje takiego włamania, pokonując przy tym zabezpieczenia w postaci haseł i kodów broniących dostępu do przechowywanej tam informacji w międzynarodowym żargonie informatycznym określa się mianem *hackera*[216].

Na działania *hackerów* składa się bardzo wiele metod, umożliwiających im przenikanie do systemów i sieci teleinformatycznych. Uzyskanie takiego dostępu jest przeważnie procedurą wieloetapową - najpierw przestępca przeszukuje system z zamiarem zlokalizowania obiektu ataku, aby następnie, najczęściej przy użyciu złośliwego oprogramowania, przejąć kontrolę nad sprzętem. Sprawca może dostać się do systemu komputerowego także poprzez przełamanie zabezpieczeń sieci bezprzewodowej lub wykorzystując jej słabość w celu zdobycia dostępu do Internetu lub zalogowanych tam komputerów[217].

Warto zauważyć, że *hackerzy* są w stanie dotrzeć nawet do usuniętych informacji, podłączyć się do domowych sieci bezprzewodowych czy też dokonywać internetowych transakcji bankowych za pomocą wygenerowanych przy użyciu specjalnego oprogramowania fałszywych numerów kart płatniczych[218].

Choć motywy *hackingu* mogą być bardzo różne i obejmować chociażby chęć zemsty, czy uzyskania publicznego rozgłosu, niezależnie od intencji sprawcy, jest to zjawisko społecznie szkodliwe, mogące powodować znaczne szkody. Ponadto, często jest tylko początkiem drogi ku dalszym przestępstwom.

A. KONWENCJA RADY EUROPY

Zgodnie z art. 2 Konwencji przestępstwo *hackingu* polega na umyślnym, bezprawnym dostępie do całości lub części systemu informatycznego. Strony zobowiązane są do podjęcia takich środków prawnych (i nie tylko), które będą niezbędne dla uznania wyżej wymienionych działań za przestępstwo, przy czym pozostawiono im możliwość zastosowaniach dodatkowych wymogów karalności, jak to, że „przestępstwo musi zostać popełnione poprzez naruszenie zabezpieczeń z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innymi systemem informatycznym” [219].

---

[215] Ibidem, s. 19.
[216] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 45.
[217] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 96-7.
[218] Ibidem, s. 97.
[219] Art. 2 Konwencji o cyberprzestępczości.

Choć zbyt wąskie pojęcie „systemu komputerowego", które nie obejmowało wszystkich urządzeń wykorzystywanych do przetwarzania danych i mogło wpłynąć na zakres karnoprawnej ochrony informacji zostało zastąpione znacznie bardziej adekwatnym „systemem informatycznym", wciąż wątpliwości budzi samo określenie „nielegalny dostęp".

Za czyn zabroniony uznaje się zachowanie, które zmierza do uzyskania dostępu do system informatycznego, bez względu na to czy sprawca dokonuje „włamania", czy też korzysta z występujących luk. Cel i sposób działania nie należą do elementów kształtujących odpowiedzialność karną, nawet gdy sprawca działał jedynie z zamiarem sprawdzenia własnych możliwości. Ponadto, karalne nie jest także stadium usiłowania[220].

Użyte na gruncie Konwencji określenie „dostępu" można porównać do włamania do cudzego mieszkania. Jednak nie można zapominać o tym, że współcześni *hackerzy* dysponują takimi technikami, które umożliwiając im przeniknięcie do systemów informatycznych bez uprzedniej konieczności przełamywania zabezpieczeń. Ponadto, przyjmując takie rozumienie, nie można uznać nieudanej próby rozszyfrowania hasła za uzyskanie dostępu, mimo iż zachowanie sprawcy doprowadziło do modyfikacji danych. Jednak już próba zapoznania się z informacjami znajdującymi się w zabezpieczonym pliku może zostać uznana za dostęp, choć użytkownik finalnie nie zaznajomił się z ich treścią, ani też nie wpisał hasła. Wątpliwości budzi także sytuacja, w której korzystając z Internetu przypadkowo trafiamy na zabezpieczoną stronę - teoretycznie nie uzyskujemy dostępu do informacji, lecz już samo wejście na taką witrynę jest równoznaczne z rozpoczęciem komunikacji z innymi systemem[221].

W wielu państwach istnieje pogląd, że walka z *hackingiem* powinna opierać się już na penalizacji samej nielegalnej interakcji z system informatycznym, a możliwość zastosowaniach dodatkowych wymogów karalności wpłynie negatywnie na karalność przestępstw. W art. 2 Konwencji podkreślono także, że warunkiem pociągnięcia sprawcy do odpowiedzialności jest uzyskanie przez niego dostępu bezprawnego, zatem niemożliwe będzie wyciągnięcie konsekwencji z działań podjętych przez osobę upoważnią przez właściciela systemu, bądź jakąkolwiek osobę uprawioną (osoby odpowiedzialne za ochronę systemów czy przeprowadzanie testów)[222].

[220] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 99.
[221] O. S. Kerr, *The Problem of perspective in Internet law* [on-line], Georgetown Law Journal 2003, Vol. 91, February 2003, s. 60, dostęp: 19.05.2015, http://papers.ssm.com/sol3/papers.cfm7abstract_kU310020.
[222] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 104-7.

B. USTAWODAWSTWO POLSKIE

W polskim porządku prawnym przestępstwu konwencyjnemu odpowiada przestępstwo z art. 267 k.k. Zgodnie ze stanowiskiem doktryny, dobrem, którego ochronę zapewnia ów przepis jest poufność informacji, bezpieczeństwo jej przekazywania i prawo do dysponowania w sposób wyłączny. Przedmiotem ochrony jest więc zabezpieczenie informacji przed osobami nieuprawnionymi, a nie jak w poprzednich wersjach Kodeksu karnego - ochrona korespondencji pojmowanej jako sfera prywatności człowieka[223]. Wróbel z kolei wskazuje, że bezpośrednio zabezpieczeniu podlega szeroko rozumiane prawo do rozporządzania informacją, mające tutaj charakter podmiotowy. Ustalenie kto może dysponować określoną informacją, musi być oparte o regulacje konstytucyjne, prawo cywilne oraz pozostałe ustawy szczególne. Kodeks ma w tym zakresie charakter subsydiarny, a przestępstwa ujęte w art. 267 k.k. - zdaniem autora - uchybiają temu ujęciu prawa do rozporządzania informacją, które wyraża się w prawie do wyłącznego dostępu oraz prawie do tajemnicy przekazu[224]. Marek natomiast uważa, że po zmianach wprowadzonych ustawą z dnia 24 października 2008 roku[225], ochronie podlega nie tylko strefa prywatna jednostki, ale także wszelkie informacje będące w jej posiadaniu, bądź dedykowane osobom prawnym, instytucjom oraz organizacjom, których pozyskanie jest niezgodne z życzeniem posiadacza, a w tym także informacje zaszyfrowane elektronicznie lub magnetycznie[226].

Podmiotem przestępstwa z art. 267 k.k. jest każdy[227], kto bez uprawnienia uzyskuje dostęp do nieprzeznaczonej dla niego informacji, bądź systemu przeznaczonego do ich gromadzenia i przetwarzania. Jeżeli dojdzie do ujawniania informacji pozyskanej w sposób spełniający przesłanki czynu z omawianego artykułu innej osobie, sprawcą może stać się każdy, kto wszedł w jej posiadanie[228]. Pomimo zmiany opisu czyny zabronionego, z którą mamy do czynienia w § 1, wciąż ma on, jak zachowania określone w § 2 i 4, materialny charakter[229].

Czynnością sprawczą jest bezprawne uzyskanie dostępu do informacji poprzez podjęcie czynności opisanych w omawianym przepisie. Zaktualizowane brzmienie, które zastąpiło sformułowanie „uzyskanie informacji", pozwala na zastosowanie sankcji karnej nie

---

[223] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* Wydawnictwo C.H. Beck, Warszawa 2015, s. 1235.
[224] W. Wróbel [w:] A. Zoll (red.) *Kodeks karny. Część szczególna. Komentarz do artykułów 117-277 k.k,* Wolters Kluwer Polska, Warszawa 2013, s. 1497.
[225] Ustawa z dnia 24 października 2008r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw, Dz.U. 2008 nr 214, poz. 1344.
[226] A. Marek, *Kodeks karny. Komentarz,* Wolters Kluwer Polska, Warszawa 2010, s. 570.
[227] Jest to przestępstwo należące do kategorii przestępstw powszechnych, więc sprawcą może być każdy,kto jest zdolny do ponoszenia odpowiedzialności karnej.
[228] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny – komentarz,* op. cit., s. 1236.
[229] Ibidem, s. 1237.

tylko w sytuacji, kiedy sprawca zapoznaje się nieprzeznaczoną dla niego treścią, ale również wtedy, gdy przejmuje kontrolę nad nośnikiem informacji, kopiuje zapis bądź pokonuje zabezpieczenie uzyskując w ten sposób dostęp. Natomiast podłączenie do sieci telekomunikacyjnej oznacza przyłączenie do sieci takiego urządzenia, które umożliwi przechwycenie transmitowanych za jej pośrednictwem informacji. Przy czym, przez sieć telekomunikacyjną należy rozumieć - zgodnie z art. 2 pkt. 35 ustawy Prawo telekomunikacyjne [230] - „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju". Przełamanie lub ominięcie zabezpieczeń skutkuje uzyskaniem dostępu do chronionych treści.

W świetle omawianego przepisu samo uzyskanie dostępu do informacji praktycznie nie podlega karze, a w szczególnych przypadkach może stanowić jedynie usiłowanie. Dopiero spełnienie dwóch warunków postawionych przez art. 267 § 1 k.k., polegających na konieczności przełamania lub ominięcia zabezpieczeń chroniących informację oraz uzyskania dostępu do niej, pozwala na pociągnięcie *hackera* do odpowiedzialności[231]. Nowelizacja, wprowadzając sformułowanie „uzyskuje dostęp do informacji", usunęła dotychczasowe wątpliwości, czy sprawca musiał zapoznać się z treścią informacji, do której uzyskał dostęp[232]. Problem polega jednak na tym, że działanie przestępców komputerowych nie ogranicza się jedynie do przełamywania zabezpieczeń, lecz obejmuje także inne metody, które umożliwiają im wniknięcie do systemów informatycznych bez potrzeby forsowania istniejącej zapory. Mogą posłużyć się zarówno podstępem (*spoofing*), jak i przechwycić pożądaną informację podczas jej transmisji (*sniffing*), czy po prostu wykorzystać lukę powstałą w systemach zabezpieczających (*bug*), co przekłada się na niewielką przydatność art. 267 § 1 k.k. w praktyce osądzania zamachów na poufność systemów informatycznych i przetwarzanej w nich informacji[233].

Wątpliwości budzi także art. 267 § 2 k.k., którego celem nie jest kryminalizacja pozyskania informacji nieprzeznaczonej dla sprawcy, ani także nielegalnej interakcji z cudzym

---

[230] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2004 nr 171, poz. 1800.).
[231] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, op. cit., s. 20-1.
[232] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 112.
[233] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, op. cit., s. 23.

systemem, a nieuzasadniony zakaz uzyskania dostępu do całości lub części systemu informatycznego. Wieloznaczność tego terminu nie pozwala na jednoznaczne określenie, jakie dobra chciał wyróżnić ustawodawca oraz przed jakimi zamachami chciał je ochronić. Należy jednak stosować możliwie wąskie rozumienie pojęcia, aby uniknąć penalizacji takich czynów, jak: dostęp do procedur i metod przetwarzania (instrukcje, regulaminy), czy urządzeń peryferyjnych (monitor, klawiatura, nagrywarka)[234].

Niezależnie jednak od wątpliwości terminologicznych, jakie budzi art. 267 § 2 k.k., może on być podstawą pociągnięcia do odpowiedzialności *hackera*, który uzyskuje nieuprawniony dostęp do informacji za pośrednictwem Bluetooth'a (*bluesnarfing*) lub poprzez przechwycenie sesji legalnego użytkownika (*session hijacking).* Przepis ten stwarza również podstawę karalności działań sprawcy opierających się na wyszukiwaniu punktów dostępu do niezabezpieczonych sieci bezprzewodowych (*wardriving*), choć nie ma tutaj mowy o przełamywaniu, ani omijaniu zabezpieczeń. Podobnie jest w przypadku tzw. *piggyhackingu,* czyli korzystania z sieci bezprzewodowej, bez zgody, a przeważnie także i wiedzy jej dysponenta, z zamiarem uzyskania dostępu do Internetu. Jest to możliwe dlatego, że warunkiem zastosowania art. 267 § 2 k.k. jest jedynie uzyskanie dostępu do systemu informatycznego, w całości, bądź w części. Budzi to jednak wątpliwości, co do zasadności stosowania środków karnych również w stosunku do tego rodzaju czynów i rodzi pytanie, czy nie stanowi to nadmiernej penalizacji. Ilość stanów faktycznych, które mogę wypełniać znamiona ustawowe omawianego przepisu jest ogromna przez co szczególnej wartości nabiera kontratyp działania w zakresie uprawnień i obowiązków[235].

Za popełnienie czynów wymienionych w art. 267 k.k. przewidziana jest kara grzywny, ograniczenia lub pozbawienia wolności do lat 2, a ściganie następuje na wniosek poszkodowanego.

C. WNIOSKI

Sposób kryminalizacji bezprawnego dostępu przyjęty na gruncie ustawodawstwa polskiego wykazuje pewne podobieństwa do regulacji europejskiej. W obu przypadkach cel oraz sposób działania sprawcy nie są elementami kształtującymi odpowiedzialność kamą za omawiane czyny. Rodzime przepisy nie zakładają jednak zaostrzenia kary w przypadku, gdy przestępstwo zostało popełnione w ramach działalności organizacji przestępczej, z zamiarem

[234] M.Siwicki, *Cyberprzestępczość*, op. cit., s. 116-7.
[235] Ibidem, s. 117-8.

uszkodzenia znacznej liczby systemów informatycznych, bądź spowodowania pokaźnych szkód, czy też przez sprawcę ukrywającego swoją rzeczywistą tożsamość[236].

Choć uzależnienie odpowiedzialności sprawcy od tego, czy jego działanie będzie można zakwalifikować jako naruszenie lub ominięcie zabezpieczeń jest zgodne z możliwością zastosowaniach dodatkowych wymogów karalności, jakie przewiduje Konwencja to raczej osłabia to funkcję ochroną przepisu i spotkało się z krytyką na arenie międzynarodowej.

Nowelizacja, która miała miejsce w 2008 roku, nakłada na oskarżyciela i sąd obowiązek udowodnienia sprawcy jedynie tego, że uzyskał on dostęp do systemu informatycznego, nie zaś do samej informacji w nim przechowywanej. Jest to zgodne z uregulowaniami zawartymi w art. 2 Konwencji, jednak w polskim ustawodawstwie brak określenia „umyślne", co może doprowadzić do sytuacji, w której do odpowiedzialności zostanie pociągnięta osoba, która przypadkowo uzyskała dostęp do cudzego systemu informatycznego.

Konwencja nie nakłada na strony obowiązku rozszerzenia karalności na stadium usiłowania - standardem minimalnym jest tutaj odpowiedzialność karna za popełnienie przestępstwa *hackingu.*

4.1.1.2. Nielegalne przechwytywanie danych

Podsłuch komputerowy, czyli nielegalne przechwycenie informacji, może polegać zarówno na przejmowaniu danych pochodzących bezpośrednio z transmisji teleinformatycznej, jak i analizie fal elektromagnetycznych[237].

Pierwszy sposób nieuprawnionego pozyskiwania informacji jest często określany jako tradycyjne szpiegostwo komputerowe. *Hacker*, posługując się specjalnym oprogramowaniem, nie tylko uzyskuje dostęp do nieprzeznaczonych dla niego treści, ale także jest w stanie gromadzić nośniki danych i monitorować ruch w sieci [238]. Stosowanie programów szpiegujących umożliwia również nagrywanie dźwięków oraz tworzenie zrzutów ekranu. Istnieje bardzo wiele programów typu *spyware*, spośród których sprawca może wybierać w zależności od tego, co jest celem jego ataku. Zwykle nie rozpowszechniają się one same, a do zainfekowania dochodzi poprzez wykorzystanie luk bądź wprowadzenie użytkowników w błąd [239].

Podsłuch komputerowy polegający na przechwytywaniu danych z transmisji

[236] Ibidem, s. 118-9.
[237] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kantor Wydawniczy „Zakamycze", Kraków 2000, s. 66.
[238] Ibidem, s. 69.
[239] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 122-3.

teleinformatycznej obejmuje zarówno dane o ruchu, jak i samo pozyskiwanie informacji. W zakresie technik komputerowych dominują wysokie częstotliwości, które emitują fale elektromagnetyczne, a ich stan oraz intensywność bezpośrednio wiążą się ze zmianą funkcji wykorzystywanych urządzeń. Jednak ze względu na wysoki koszt wykorzystywanego sprzętu, ten typ podsłuchu jest zdecydowanie rzadziej stosowany przez sprawców indywidualnych. Budzi on natomiast zainteresowanie przestępczości zorganizowanej, czy przedsiębiorstw konkurencyjnych. Nie można jednak wykluczyć, że popularność tej metody wzrośnie wraz ze spadkiem cen i dostępnością urządzeń[240].

A. KONWENCJA RADY EUROPY

Zgodnie z art. 8 EKPC[241] każda nielegalna ingerencja w prywatność komunikacji międzyludzkiej jest naruszeniem prawa do prywatności korespondencji i powinna podlegać sankcji karnej. Wychodząc z takiego założenia, Europejski Komitet ds. Przestępczości określił swoje stanowisko w tym przedmiocie w art. 3 Konwencji, zobowiązując strony do kryminalizacji „umyślnego, bezprawnego przechwytywania z pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne."

Celem cytowanego przepisu jest ochrona prywatności użytkowników systemów informatycznych komunikujących się przy użyciu elektronicznych systemów transmisji danych. Podobnie, jak w przypadku nielegalnego dostępu, warunkiem penalizacji jest umyślność oraz bezprawność czynu. Należy także zaznaczyć, że w rozumieniu Konwencji, podsłuch komputerowy obejmuje przechwytywanie danych za pomocą urządzeń technicznych, jak i analizę fal elektromagnetycznych wytwarzanych przez systemy komputerowe.

Ograniczenie odpowiedzialności sprawcy do sytuacji, w których posługuje się on urządzeniami technicznymi jest próbą uniknięcia nadmiernej kryminalizacji życia społecznego. Pojęcie, jakim posługuje się Konwencja, odnosi się do słuchania, monitorowania lub nadzorowania treści komunikatów w celu przechwycenia informacji, bezpośrednio - poprzez dostęp i wykorzystanie systemu komputerowego, albo pośrednio, poprzez zastosowanie elektronicznego podsłuchu lub urządzeń podsłuchowych. Ponadto, przechwytywanie może

[240] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne,* op. cit., 67-8.
[241] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2., Dz.U. 1993 nr 61, poz. 284.

również obejmować nagrywanie[242].

Użycie sformułowania „niepubliczna transmisja" zwraca uwagę na charakter procesu transmisji, a nie rodzaj danych, jakie są przesyłane. Dlatego też art. 3 Konwencji można również zastosować do transmisji danych w sieciach publicznych, pod warunkiem, że strony podjęły decyzję o poufności przekazu[243]. Adamski zwraca także uwagę na konieczność unormowania dopuszczalności kontrolowania przez pracodawców rozmów telefonicznych, bądź też innych form przekazywania informacji dokonywanych przez pracowników. Orzecznictwo Trybunału Praw Człowieka uznaje takie zachowanie za łamanie przez pracodawcę prawa do ochrony życia prywatnego i tajemnicy korespondencji, przysługujących pracownikowi także na trenie zakładu pracy[244].

B. USTAWODAWSTWO POLSKIE

Nielegalny dostęp do informacji z użyciem środków technicznych jest w polskim prawie przestępstwem, którego znamiona określa art. 267 § 3 k.k. Karalne jest nie tylko samo posługiwanie się urządzeniem podsłuchowym, wizualnym bądź też innym urządzeniem, czy oprogramowaniem, ale także ich zakładanie. Nie ulega wątpliwości, że penalizacji podlega również uzyskanie z ich wykorzystaniem informacji przez osoby to tego nieuprawnione. W przeciwieństwie do § 1 omawianego przepisu, karalność nie jest uzależniona od przełamania lub ominięcia zabezpieczenia. Przestępstwo z § 3 jest formalne w odniesieniu do posługiwania się urządzeniem, natomiast materialne w przypadku jego montażu[245].

Przestępstwo to można popełnić jedynie umyślnie, z zamiarem bezpośrednim kierunkowym, na co wskazuje zwrot „w celu uzyskania informacji". Osoba, która korzysta ze wskazanych w przepisie urządzeń, ponosi odpowiedzialność tylko wtedy, gdy ma świadomość, że nie jest do takiego działania uprawniona. Zleceniodawca natomiast będzie odpowiadał za sprawstwo kierownicze bądź polecające[246].

Zwrot „inne urządzenie lub oprogramowanie" poszerza zakres kryminalizacji o wszystkie stany faktyczne, w których obserwacja jest prowadzona z wykorzystaniem urządzeń technicznych albo programów komputerowych przystosowanych do pozyskiwania nieprzeznaczonych dla sprawcy informacji, a także służących do podsłuchu, czy podglądu

[242] Cybercrime Convention: Explanatory Report, pkt. 53.
[243] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 124.
[244] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* op. cit., s. 27.
[245] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1237.
[246] Ibidem.

cudzej komunikacji[247].

Omawiane przestępstwo ma charakter formalny w zakresie posługiwania się urządzeniem, natomiast materialny w stosunku do czynności montażu - skutek występuje tylko wtedy, gdy urządzenie zostanie założone zgodnie z wolą sprawcy[248]. Pomimo zmiany opisu czynu zabronionego, z którym mamy do czynienia w § 1, wciąż ma on, jak zachowania określone w § 2 i 4, materialny charakter. Jeżeli chodzi o przestępstwo z § 3, jest ono formalne w odniesieniu do posługiwania się urządzeniem, natomiast materialne w przypadku jego montażu[249].

Przestępstwo z art. art. 267 § 3 k.k. ma charakter powszechny, ale oczywiście nie może być popełnione przez osobę, która jest uprawniona do uzyskania informacji. Natomiast jego bezprawność może zostać uchylona, jeżeli zachowanie wypełniające znamiona jest działaniem organów ścigania, prokuratury lub sądu.

Jednak ocena słuszności i legalności stosowania podsłuchu, bądź też innych form kontroli przez funkcjonariuszy publicznych, zobowiązuje do wzięcia pod uwagę zarówno norm ustawowych, jak i wzorowanych na nich przepisów wykonawczych, które to określają, w jaki sposób podjęte czynności powinny zostać przeprowadzone i udokumentowane oraz użycie jakich środków technicznych będzie właściwe w tym przypadku. Jest to działanie w ramach szczególnych uprawnień, stanowiące kontratyp pozakodeksowy, a zatem musi spełniać ogólnie przyjęte warunki[250].

Podobnie jak przestępstwo uzyskania nielegalnego dostępu do informacji, za przestępstwo podsłuchu przewidziana jest kara grzywny, ograniczenia lub pozbawienia wolności do lat 2 i także jest ono ścigane wyłącznie na wniosek poszkodowanego.

C. WNIOSKI

Sposób kryminalizacji wynikający z art. 267 § 3 k.k. jedynie częściowo odpowiada założeniom Konwencji. Kierunkowy charakter tego przepisu wyłącza jakąkolwiek inną formę umyślności, niż działanie z zamiarem bezpośrednim. Zatem na gruncie polskiego ustawodawstwa, oskarżony może powoływać się na fakt, że skorzystał on z urządzeń podsłuchowych jedynie w celu wypróbowania własnych umiejętności lub sprawdzenia, czy będą one skuteczne. Udowodnienie w procesie strony podmiotowej będzie niezwykle trudne,

[247] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 130.
[248] P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks karny. Komentarz*, LexisNexis Polska, Warszawa 2013, s. 622.
[249] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz*, op. cit., s. 1237.
[250] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 61.

nie mówiąc już o samym zamiarze bezpośrednim, z jakim miał działać sprawca[251]. Wskazuje to na potrzebę zastąpienia dotychczasowego określenia „w celu uzyskania", bardziej adekwatnym „z zamiarem uzyskania".

Jednak, w odróżnieniu od rozwiązania przewidzianego w Konwencji, polski ustawodawca penalizuje już samo narażenie informacji na niebezpieczeństwo - wystarczające jest zainstalowanie odpowiedniego oprogramowania, bez konieczności jego wykorzystania, czy też uzyskania dostępu do chronionych treści, tym samym wykraczają poza art. 3 traktatu.

4.1.1.3. Naruszenie integralności danych

Przepisy chroniące integralność danych są odpowiednikiem norm karnych zakazujących niszczenia lub uszkadzania rzeczy. Wprowadzenie tego unormowania do porządku prawnego wynika z niematerialnego charakteru informacji, wobec której nie są adekwatne zakazy dotyczące niszczenia cudzego mienia[252].

Kasowanie plików, uszkodzenie lub modyfikacja zasobów systemowych, czy zakłócenie ich funkcjonowania, mogą stanowić zarówno cel, jak i środek działania sprawców. Pobudki, jakimi się kierują, bywają bardzo zróżnicowane, lecz każde z tych zachowań uderza w integralność zapisu danych i może prowadzić do kolizji z prawem[253].

Dane mogą być niszczone zarówno fizycznie, jak i przez ingerencję zmierzającą do destrukcji softwarowej - wielokrotnego, losowego nadpisywania informacji. Działania fizyczne opierają się na zwykłym uszkodzeniu, a także mechanicznym, magnetycznym lub chemicznym zniszczeniu. Znacznie trudniejsze do wykrycia są metody destrukcji programowej. Najczęściej jest to umieszczenie w cudzych programach segmentu wykonywalnego kodu, przyjmującego postać wirusa lub robaka[254]. Powodują one dodanie do danych nowych elementów, lecz mogą także oddziaływać na procesy mające miejsce w systemach komputerowych, a w efekcie wpływać na ich prawidłowy przebieg, powodować spowolnienie, a nawet zniekształcenie lub modyfikację gromadzonych danych[255].

A. KONWENCJA RADY EUROPY

Naruszenie integralności danych może przyjmować przeróżne formy, do których

[251] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 134.
[252] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, op. cit., s. 29.
[253] A. Adamski, *Prawo karne komputerowe*, op. cit., s. 64.
[254] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, op. cit., 40.
[255] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 135.

Europejski Komitet ds. Przestępczości zalicza ich „niszczenie, wykasowanie, uszkadzanie, dokonywanie zmian lub usuwanie”[256]. Warunkiem popełnienia przestępstwa z art. 4 Konwencji jest działanie umyślne.

Nie będą zatem przestępstwem czynności z zakresu serwisowania, wymiany oprogramowania, czy też testowania zabezpieczeń systemu informatycznego, podejmowane przez osoby do tego uprawnione. Zgodna z prawem jest także modyfikacja danych ruchowych dokonywana w celu zagwarantowania anonimowości nadawcy korespondencji elektronicznej, czy też zmiana zapisu wysyłanej informacji podjęta z zamiarem zabezpieczenia poufności przekazywanych treści[257].

Kryminalizacja wskazanego zachowania ma służyć zapewnieniu bezpieczeństwa danych komputerowych i chronić je przed bezprawnymi atakami. Zdawano sobie sprawę z tego, że już samo włączenie systemu komputerowego może doprowadzić do nieuprawnionej modyfikacji danych, dlatego też do art. 4 dodano pkt 2, który daje stronom możliwość wprowadzenia dodatkowego warunku karalności, którym jest wystąpienie poważnej szkody[258].

B. USTAWODAWSTWO POLSKIE

Na gruncie prawa polskiego, ochronę integralności danych gwarantują aż dwa przepisy: art. 268 oraz art. 268a k.k. Pierwszy z nich chroni możliwość swobodnego korzystania z informacji przez osoby uprawnione, podczas gdy drugi kryminalizuje nieuprawnione zniszczenie, uszkodzenie, usuwanie lub zmienienie danych oraz utrudnianie dostępu do ich zapisu.

Artykuł 268 k.k.

Przepis ten ma chronić integralność, kompletność i poprawność istotnej informacji, a także zapewnić dostęp do niej osobom uprawnionym. Należy zwrócić uwagę, że przedmiotem ochrony nie będzie zatem każda informacja, a jedynie ta, która posiada szczególną wartość w rozumieniu obiektywnym. Ocena jej znaczenia powinna być dokonana z uwzględnieniem uzasadnionego interesu właściciela informacji, osób upoważnionych do wglądu w jej treść, a w przypadku danych osobowych, także podmiotu, którego dana informacja dotyczy[259]. Wróbel natomiast zauważa, że dobrem bez pośrednio chronionym przez art. 268 k.k. jest, w aspekcie

[256] Art. 4 Konwencji o cyberprzestępczości.
[257] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* op. cit., s. 29.
[258] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 139.
[259] A. Adamski, *Prawo karne komputerowe,* op. cit., s. 65.

zachowanie integralności - prawo do dysponowania informacją, a także prawo dostępu do niej[260]. Natomiast niektóre osoby zawracają także uwagę na postać, w jakiej została utrwalona informacja.

Przedmiot czynności wykonawczych, którym są dane zapisane na nośniku informatycznym, można podzielić na dwie grupy. Pierwsza z nich to czyny godzące w integralność danych, polegające przede wszystkim na działaniach o charakterze logicznym, czyli kasowanie i usuwanie. Drugą grupę stanowią zachowania mające na celu utrudnienie, a nawet udaremnienie, osobie uprawnionej zapoznania się z treścią informacji. W tym wypadku, zachowanie sprawcy może polegać na zmianie hasła dostępu, czy ukryciu nośnika[261].

Typ kwalifikowany został wyróżniony w § 3 przestępstwa naruszenia integralności danych. W doktrynie istnieje spór, czy jest to spowodowane szkodą, jaką rzeczywiście ponosi dysponent, czy wartością nośnika informacji. Marek uważa, że jest to wynikiem wyrządzonej przez sprawcę szkody, gdyż wartość nośnika może być symboliczna[262]. Natomiast Hałas wskazuje, że znamieniem kwalifikującym jest typ nośnika informacji, jakim jest informatyczny nośnik danych[263]. Moim zdaniem, ze względu na różnorodność występujących nośników, bardziej zasadny wydaje się pierwszy pogląd.

Wyższa sankcja kama jaką przewiduje art. 268 § 2 k.k. stanowi odstępstwo od ogólnie przyjętych standardów międzynarodowych, a związana jest z typem nośnika, na którym została utrwalona informacja. Wydaje się to jednak uzasadnione, biorąc pod uwagę fakt, że przestępstwo to, powodując zakłócenia pracy całych systemów, często narusza interes majątkowy uprawnionego. Ponadto, także nośnik posiada określoną wartość majątkową, przez co spełnia cechy rzeczy ruchomej, a jego zniszczenie lub uszkodzenie spełnia również przesłanki z art. 288 § 1 k.k. Podwyższona karalność takich czynów wynika także z wyrządzenia dysponentowi informacji szkody majątkowej. Natomiast, gdy sprawca zmienia lub usuwa zapis zawarty na nośniku w celu wyrządzenia szkody majątkowej, obejmując przy tym swoim zamiarem ewentualnym skutek w postaci wyrządzenia poważnej szkody majątkowej, możliwa jest kumulatywna kwalifikacja pomiędzy art. 268 § 3 k.k. a art. 287 § 1 k.k.[264].

Omawiane przestępstwo o charakterze powszechnym można popełnić zarówno przez

---

[260] W. Wróbel [w:] A. Zoll (red.) *Kodeks karny. Część szczególna. Komentarz do artykułów 117-277 k.k.,* op. cit., s. 1292.
[261] F. Randoniewicz, *Odpowiedzialność karana za przestępstwo hackingu* [on-Line], dostęp: 21.05.2015, http://www.iws.org.pl/pliki/files/IWS_Radoniewicz_Odp%20za%20przest%20hackingu.pdf.
[262] A. Marek, *Kodeks karny. Komentarz,* op. cit., s. 573.
[263] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1238.
[264] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 146.

działanie, jak i zaniechanie, jednak jedynie z winy umyślnej, w obu postaciach zamiaru[265] - sprawca musi przynajmniej godzić się na to, że podejmowane przez niego działanie może uniemożliwić, bądź w znaczący sposób utrudnić zapoznanie się przez osobę uprawniona z istotną dla niego informacją. Ponadto, wszystkie czyny z art. 268 k.k. mają charakter materialny, z zaznaczeniem, że skutek w formie znacznej szkody majątkowej jest okolicznością kwalifikującą jedynie w § 3[266].

Typ podstawowy przestępstwa naruszenia integralności danych jest zagrożony karą grzywny, ograniczenia lub pozbawienie wolności do lat 2. Podczas gdy, za typ kwalifikowany z § 2 ustawodawca przewidział sankcję do 3 lat pozbawienia wolności, czyn wyrządzający znaczną szkodę majątkową podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Podobnie, jak w przypadku wcześniej omówionych przestępstw, ściganie (we wszystkich typach) odbywa się na wniosek poszkodowanego.

Artykuł 268a k.k.

Przepis ten, wprowadzony do Kodeksu karnego nowelizacją z 2004 roku[267], jest następstwem dostosowywania polskiego prawa do Konwencji Rady Europy. Obejmuje zachowania analogiczne do tych z art. 268 k.k., pod warunkiem, że godzą one w dane informatyczne. Zatem karalne zachowanie polega na nielegalnym niszczeniu, uszkadzaniu, usuwaniu, czy też zmienianiu, bądź utrudnianiu dostępu do danych informatycznych. Zabronione jest również ich zakłócanie albo uniemożliwianie automatycznego przetwarzania, gromadzenia czy przechowywania. Przestępstwo to ma charakter materialny, a kwalifikowana odpowiedzialność z § 2 wynika ze znacznej szkody majątkowej wyrządzonej przez sprawcę. Ponadto, karalność nie jest zależna od charakteru bądź treści danych[268].

Przedmiotem ochrony jest bezpieczeństwo systemów komputerowych oraz przetwarzanej elektronicznie informacji, na które składają się nienaruszalność zapisu informacji w formie danych informatycznych, prawidłowe funkcjonowanie systemów cyfrowych oraz dostępność danych, czy możliwość korzystania przez osoby uprawnione[269].

Przedmiot wykonawczy tego przestępstwa jest podobny do zachowań penalizowanych przez art. 268 k.k. Choć art. 268a § k.k. nie uwzględnia karalności uniemożliwienia dostępu do

[265] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz*, op. cit., s. 1238.
[266] F. Randoniewicz, *Odpowiedzialność karana za przestępstwo hackingu*, op. cit., s. 25.
[267] Ustawa z dnia 18 marca 2004r. o zmianie ustawy - Kodeks kamy, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń (Dz.U. 2004 nr 69, poz. 626.).
[268] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz*, op. cit., s. 1238.
[269] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 147.

danych to można je uznać za najdalej idącą formę zakłócenia dostępu. Natomiast, w przeciwieństwie do 168 § 1 k.k., daje on możliwość pociągnięcia sprawcy do odpowiedzialności za każde utrudnienie w uzyskaniu wglądu do danych. Podkreśla to, że dobrem bezpośrednio chronionym jest bezpieczeństwo przesyłanych informacji, a nie jak w art. 268 k.k. - dostępność zapisu[270].

Pierwsza część przepisu dotyczy omawianych już wcześniej działań, polegających na niszczeniu lub modyfikacji danych oraz utrudniania dostępu do nich. Natomiast w drugiej części, penalizowane jest istotne zakłócenie, czyli działanie utrudniające lub uniemożliwiające prawidłowe działanie systemu oraz gromadzenie, przetwarzanie i przekazywanie danych[271]. Według Wróbla, takim zakłóceniem jest każda czynność skutkująca nieprawidłowym przebiegiem wyżej wymienionych procesów, ich spowolnieniem, wypaczeniem lub modyfikacją[272]. Kunicka-Michalska zwraca także uwagę na trudności w ocenie stopnia zakłócenia, będącego w jej opinii pojęciem nieostrym. Uważa, że z taką sytuacją mamy do czynienia, gdy w ocenie użytkownika, nie jest możliwe szybkie i względnie bezproblemowe usunięcie powstałego wskutek działania sprawcy zakłócenia[273].

Przestępstwo ma charakter powszechny i można je popełnić zarówno poprzez działanie jak i zaniechanie. W obu odmianach ma charakter umyślny, jednak w przypadku formy wykonawczej konieczne jest działanie z zamiarem bezpośrednim, natomiast istotność zakłóceń oraz wielkość szkody, wymagają jedynie zamiaru ewentualnego[274].

Warto zauważyć, że przedmiotem wykonawczym są dane informatyczne, które nie zostały zdefiniowane przez ustawodawcę polskiego oraz proces ich przetwarzania, gromadzenia albo przekazywania[275]. W rozumieniu art. 1 lit. b. Konwencji o cyberprzestępczości oznaczają one „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny". Zatem, w myśl art. 268a k.k., danymi informatycznymi będą nie tylko dane, które funkcjonują w sieci, ale także te utrwalane na nośnikach elektronicznych poza systemem[276].

Natomiast poprzez znamię „przetwarzania danych informatycznych", w myśl ustawy

---

[270] Ibidem, s. 147.
[271] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1239.
[272] W. Wróbel [w:] A. Zoll (red.) *Kodeks karny. Część szczególna. Komentarz do artykułów 117-277 k.k.,* op. cit., s. 1302.
[273] B. Kunicka-Michalska [w:] A. Wąsek, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316,* Wydawnictwo C.H. Beck, Warszawa 2010, s. 736.
[274] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 147-8.
[275] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1239.
[276] M.Siwicki, *Cyberprzestępczość*, op. cit., s. 148.

o ochronie danych osobowych, należy rozumieć „jakiekolwiek operacje wykonywane na danych (...), takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych” [277]. Przetwarzanie ma charakter automatyczny, pod warunkiem, że chociaż część tego procesu odbywa się przy użyciu urządzeń sterujących, bez udziału człowieka lub, gdy jest on bardzo ograniczony. Gromadzeniem z kolei będzie zbieranie danych, a przekazywanie to nie tylko ich transmisja, ale również przekazanie nośnika[278].

Sprawcy kierują się różnorodnymi motywami, a ich ustalenie, podobnie jak w przypadku poprzedniego przepisu, jest konieczne do ustalenia, czy nie zostały spełnione znamiona innego czynu zabronionego, jak np. oszustwa komputerowego z art. 287 k.k.[279].

C. WNIOSKI

Podczas gdy art. 4 Konwencji formułuje zakaz bezprawnej ingerencji w dane informatyczne, na gruncie prawa polskiego penalizowane jest jedynie utrudnienie dostępu do nich. W sytuacji nieuprawnionego przekształcenia programu komputerowego, sprawca może odpowiadać za przestępstwo z art. 268 § 2 lub 3 k.k., jedynie wtedy, gdy będzie miało to także wpływ na zakłócenie lub udaremnienie automatycznego przetwarzania, gromadzenia czy transferu danych informatycznych. Rozwiązanie te odbiega od standardów jakie przyjęto w dokumencie międzynarodowym. Problematyczny jest także brak definicji ustawowej „danych informatycznych” oraz ujęcie omawianego przestępstwa aż w dwóch przepisach[280].

Ponadto, popełnienie przestępstwa z art. 268a k.k. jest uzależnione od wystąpienia „istotnego zakłócenia” bądź „uniemożliwienia” przetwarzania, gromadzenia lub transferu danych - nie wystarcza sama bezprawna interakcja z dowolnym urządzeniem służącym do obsługi danych lub programów komputerowych. Pozwala to na uniknięcie zbyt rozbudowanego zakresu kryminalizacji dotyczącego oddziaływania na którykolwiek proces mający miejsce w systemach komputerowych[281].

4.1.1.4. Naruszenie integralności systemów

Sposób działania *hackerów* obejmuje nie tylko wykorzystywanie złośliwego

[277] Art. 7 pkt. 2 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
[278] P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks karny. Komentarz*, LexisNexis Polska, Warszawa 2013, s. 507.
[279] F. Randoniewicz, *Odpowiedzialność karana za przestępstwo hackingu,* op. cit., s. 28.
[280] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 150.
[281] Ibidem, 150-1.

oprogramowania, lecz także bogaty repertuar metod, dzięki którym sprawca może doprowadzić do naruszenia integralności systemu komputerowego[282]. Włamanie może być przypadkowe, bądź celowe. Ataki popełnianie umyślnie są przed wszystkim punktem wyjścia dla przeważającej większości przestępstw komputerowych. Choć za głównych sprawców tego rodzaju przestępstw uznaje się właśnie *hackerów* to może wśród nich wyodrębnić także personel własny firmy, czy też osoby z zewnątrz, które nimi nie są. Mogę one działać w zakresie wywiadu gospodarczego, zorganizowanej grupy przestępczej, a nawet konkurencyjnej organizacji. Co ciekawe, początkowo włamanie do obcego systemu nie miało na celu manipulacji lub szpiegostwa, a chodziło jedynie o osiągnięcie satysfakcji z pokonania zabezpieczeń. Jednak, wraz ze wzrostem znaczenia sieci informatycznych w codziennym życiu, działania te mają rozmaity charakter, począwszy od ambicji programistycznych, a na terroryzmie kończąc[283].

A. KONWENCJA RADY EUROPY

Zgodnie z art. 5 Konwencji „każda strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowadzenie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych". Zatem przepis ten ma na celu ochronę systemów komputerowych przed naruszaniem ich funkcjonowania, będącego wynikiem nielegalnej ingerencji w dane oraz programy komputerowe.

Na podstawie Raportu wyjaśniającego do Konwencji, należy stwierdzić, że omawiany artykuł odnosi się do przestępstwa sabotażu komputerowego i ma na celu penalizację celowego utrudniania legalnego wykorzystania systemów komputerowych. Ochronie podlega interes prawny operatorów i użytkowników systemów informatycznych[284], pod warunkiem, że dojdzie do celowego i poważnego zakłócenia działania owego systemu będącego następstwem działania osoby nieuprawnionej. Rodzaj informacji oraz charakter powiązanych z nią dóbr prawnych nie stanowią elementów kształtujących odpowiedzialność karną. Znaczenia nie ma także status podmiotów pokrzywdzonych[285], a Konwencja nie daje stronom możliwości wdrożenia dodatkowych warunków karalności.

---

[282] Ibidem, 151.
[283] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspektyprawno-kryminalistyczne,* op. cit., 52-4.
[284] Cybercrime Convention: Explanatory Report, pkt. 65.
[285] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* op. cit., s. 32.

Termin „zakłócanie funkcjonowania" odnosi się do działań, które pokrywają się z właściwym funkcjonowaniem systemu komputerowego i odbywają się poprzez wprowadzanie, przesyłanie, niszczenie, usuwanie, uszkadzanie lub zmienianie lub danych informatycznych[286]. W Raporcie nie sprecyzowano jednak na czym ma polegać, „poważne zakłócenie", a jedynie wskazano na konieczność wystąpienia tego znamienia, jako warunku stanowiącego podstawę do zastosowania sankcji karnej. Każda ze stron powinna sama określić jakie kryteria muszą zostać spełnione, aby zakłócenie uznać za „poważne". Można powiązać to pojęcie z takim działaniem sprawcy, które naraża poszkodowanego na istotne straty bądź ma znaczący negatywny wpływ na zdolność właściciela lub operatora do korzystania z systemu, czy też komunikację z innymi systemami informatycznymi[287].

W komentarzu do Konwencji wskazano również, kiedy możliwe jest pociągnięcie do odpowiedzialności karnej za przestępstwo *spammingu* - takie zachowanie powinno być karalne tylko wtedy, gdy komunikacja jest celowo i poważnie utrudniona[288].

B. USTAWODAWSTWO POLSKIE

Podobnie, jak w przypadku naruszenia integralności danych, ochronę systemu także gwarantują dwa przepisy: art. 269 oraz art. 269a k.k. Dobrem chronionym przez pierwszy z nich są dane o szczególnej wartości dla obronności, komunikacji oraz działalności instytucji państwowych, gwarantujące poprawne działania systemów informatycznych. Z kolei drugi z nich zapewnia niezakłócone funkcjonowanie systemów lub sieci informatycznych, w czym zawiera się również bezpieczeństwo elektronicznie przetwarzanej informacji[289].

Artykuł 269 k.k.

Celem przestępstwa sabotażu jest sparaliżowanie systemu komputerowego. Wyróżnienie tego rodzaju przestępstw wynika z zagrożenia, jakie stwarzają ona dla bezpieczeństwa państwa i jego mieszkańców. Do sparaliżowania kluczowych systemów informatycznych może dojść poprzez uszkodzenie bądź zniszczenie obiektów materialnych, jak i programów lub zbiorów danych. Natomiast metody stosowane przez sprawców mogą mieć charakter fizyczny albo logiczny[290]. Art. 269 k.k. przewiduje przestępstwo sabotażu wyróżnione za względu na kategorię danych informatycznych, będących przedmiotem

[286] Cybercrime Convention: Explanatory Report, pkt. 66.
[287] Ibidem, pkt. 67.
[288] Ibidem, pkt. 69.
[289] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 157-8.
[290] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne,* op. cit., 51.

działania sprawcy[291].

Głównym dobrem chronionym przez ten przepis jest bezpieczeństwo danych i systemów komputerowych o szczególnym znaczeniu, objawiające się poprzez ich integralność. Ze względu na to, że ochronie podlega specyficzny rodzaj informacji, dobrami obocznymi stały się: obronność kraju, bezpieczeństwo w komunikacji, działalność administracji rządowej oraz innych organów państwowych, instytucji lub samorządu terytorialnego[292].

Jednak niektórzy autorzy uważają, że wyszczególnienie konkretnego rodzaju informacji powoduje, że dobra oboczne wysuwają się na pierwszy plan i to właśnie one podlegają ochronie w myśl art. 296 § 1 k.k., a nie, jak mogłoby się wydawać - bezpieczeństwo informacji samej w sobie[293].

Niezależnie jednak od tego, czynność sprawcza obejmuje:

a. niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o specjalnym znaczeniu,
b. zakłócanie automatycznego przetwarzania, gromadzenia oraz transmisji takich danych,
c. uniemożliwienie automatycznego przetwarzania, gromadzenia oraz transmisji takich danych,
d. dokonanie czynu wymienionego w § 1 przepisu, poprzez zniszczenie lub wymianę nośnika informatycznego,
e. dokonanie czynu wymienionego w § 1 przepisu, poprzez zniszczenie lub uszkodzenie urządzenia wykorzystywanego do automatycznego przetwarzania, gromadzenia oraz transmisji danych informatycznych[294].

Przestępstwo sabotażu ma charakter materialny - konieczne jest wystąpienie skutku, czy to w postaci uszkodzenia lub zniszczenia danych, czy też zakłócenia, bądź uniemożliwienia ich automatycznego przetwarzania, gromadzenia albo transmisji, niezależnie od tego, czy atak miał formę działania logicznego czy fizyczną[295]. Ponadto, przestępstwo to ma charakter powszechny.

---

[291] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz*, op. cit., s. 1240.
[292] Ibidem, s. 1240.
[293] B. Kunicka-Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz*, Wydawnictwo C.H. Beck, Warszawa 2010, s. 515.
[294] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 157.
[295] P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks karny. Komentarz*, LexisNexis Polska, Warszawa 2013, s. 627.

Czyn z art. 269 k.k. jest przestępstwem umyślnym we wszystkich jego postaciach i może zostać popełniony z zamiarem bezpośrednim, a także ewentualnym. Sprawca musi chcieć popełnienia konkretnego ataku albo przynajmniej godzić się na to, że podejmowane przez niego działanie wypełni znamiona przestępstwa. Ponadto, musi zdawać sobie sprawę z tego, że dane, którymi się posługuje, mają lub też mogą mieć szczególne znaczenie, bądź też, że jego działanie może albo będzie skutkowało zakłóceniem, czy też uniemożliwieniem przeprowadzenia procesu przetwarzania, gromadzenia, czy też transmisji danych. W przypadku § 2 musi mieć on także świadomość przeznaczenia niszczonych nośników lub urządzeń[296].

Sabotaż komputerowy uznaje się za typ kwalifikowany w relacji do przestępstw z art. 268 § 2, 268a oraz 269a k.k. - art. 269 k.k. ma tu charakter *lex specialis*[297], a znamieniem kwalifikującym jest rodzaj podlegających ochronie danych. Ponadto, gdy popełnienie omawianego czynu zabronionego spowoduje zagrożenie dla życia lub zdrowia znacznej liczby osób bądź też mienia w znacznych rozmiarach, możliwe wystąpienie takiego zachowania w zbiegu realnym z art. 165 § 1, określającym przestępstwo przeciwko bezpieczeństwu powszechnemu. Natomiast w zbiegu kumulatywnym - z art. 174 k.k.[298].

Przestępstwo z art. 269 k.k. jest zagrożone karą pozbawiania wolności od 6 miesięcy do lat 8, a ze względu na wysoki stopnień szkodliwości, jego ściganie odbywa się z urzędu.

Warto również zauważyć, że przestępstwo sabotażu komputerowego jest często połączone z szantażem komputerowym - sprawca, w zamian za spełnienie postawionych przez niego warunków, najczęściej o charakterze finansowym, gotów jest zrezygnować ze sparaliżowania systemu komputerowego.

Artykuł 269a k.k.

Podobnie jak w przypadku art. 268a k.k. dobrem podlegającym ochronie jest bezpieczeństwo danych, systemów komputerowych oraz sieci informatycznych[299]. Kunicka-Michalska uważa jednak, że przedmiotem bezpośredniej ochrony jest poufność, integralność oraz dostępność danych i systemów, a także bezpieczeństwo elektronicznie przetwarzanej informacji[300].

Zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej jest karalne

---

[296] F. Randoniewicz, *Odpowiedzialność karana za przestępstwo hackingu,* op. cit., s. 31.
[297] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1240.
[298] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 158.
[299] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1240.
[300] B. Kunicka-Michalska [w:] A. Wąsek, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316,* Wydawnictwo C.H. Beck, Warszawa 2010, s. 736.

tylko wtedy, gdy jest ono istotne i zostało dokonane poprzez: transmisję, zniszczenie, uszkodzenie, usunięcie, utrudnienie dostępu lub też zmianę danych informatycznych[301]. Tworzy to katalog zamknięty.

Przestępstwo to ma charakter powszechny, a do jego popełnienia nie są wymagane żadne szczególne umiejętności, jedynie odpowiednie narzędzia. Ma charakter materialny, a jego skutkiem jest istotne zakłócenie pracy systemu komputerowego albo sieci informatycznej. Może być popełnione jedynie z winy umyślnej, zarówno z zamiarem bezpośrednim jak i ewentualnym. Choć przeważnie do zakłócenia dochodzi przez działanie, wykluczone nie jest także np. utrudnienie dostępu poprzez zaniechanie[302].

Zarówno Wróbel, jak i Adamski uważają, że zakresowo art. 269a k.k. jest zbliżony do art. 268a k.k., choć przewiduje on wyższe zagrożenie sankcją karną. Określenia „w istotnym stopniu zakłóca lub niemożliwa automatyczne przetwarzanie, gromadzenie lub przechowanie danych[303]" jest w zasadzie tożsame z „w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej[304]. Zarówno praca systemu komputerowego, jak i sieci teleinformatycznej sprowadza się właśnie do przetwarzania, gromadzenia oraz przekazywania danych. Podczas, gdy Adamski proponuje, żeby przepis z art. 268a był traktowany, jako narzędzie kryminalizacji takich działań, które nie spełniły znamion strony podmiotowej przewidzianych w art. 269a[305], Wróbel sugeruje, że art. 269a powinien być stosowany w sytuacji, w której mamy do czynienia z kwalifikowanym zakłóceniem pracy systemu, czy sieci[306].

Przestępstwo zakłócenia pracy sieci podlega karze pozbawienia wolności od 3 miesięcy do lat 5 i także ściganie jest z oskarżenia publicznego.

C. WNIOSKI

Ustawą z dnia 18 marca 2004 roku dodano do art. 269 k.k. dwa kolejne przepisy - art. 269a i 269b k.k., co miało na celu dostosowanie polskiego ustawodawstwa karnego do wymogów Konwencji. Przed nowelizacją, karalność sabotażu komputerowego znajdowała odbicie jedynie w art. 269 k.k., którego zakres znaczeniowy był stosunkowo wąski w porównaniu do standardów międzynarodowych.

---

[301] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1240.
[302] G. R. Hałas w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1241.
[303] Art. 268a Kodeksu karnego.
[304] Art. 269a Kodeksu karnego.
[305] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* op. cit., s. 58.
[306] W. Wróbel [w:] A. Zoll (red.) *Kodeks karny. Część szczególna. Komentarz do artykułów 117-277 k.k.,* op. cit., s. 1309.

Art. 5 Konwencji zapewnia ochronę każdemu użytkownikowi systemu informatycznego, w sytuacji, gdy dojdzie do celowego zakłócenia jego działania przez osobę nieuprawnioną. Natomiast art. 269 k.k. gwarantuje bezpieczeństwo jedynie tych serwerów, które są związane z sektorem rządowym, praktycznie pozostawiając bez ochrony wszystkie pozostałe.

Przedmiotem czynności wykonawczej są dane informatyczne wraz z procesem ich przetwarzania, gromadzenia oraz transmisji. Trudno jednak stwierdzić, aby omawiane przepisy odnosiły się do programów komputerowych w sposób jednoznaczny, a brak ustawowej definicji pojęcia dane informatyczne wskazuje na to, że polski prawodawca zapewnia ochronę tylko przed niektórymi atakami na integralność systemów i sieci informatycznych. Ukazuje to wadliwość przyjętego rozwiązania, które nie jest w stanie właściwie wypełnić nadanej mu polityczno- kryminalnej funkcji. Ustawodawca zapomniał, że nie każde przestępstwo sabotażu musi wiązać się ze zniszczeniem, uszkodzeniem, usunięciem, bądź też zmianą danych - jego celem może być np. kopiowanie z użyciem mocy obliczeniowej procesora w efekcie prowadzące do jego przeciążenia[307].

4.1.1.5. Niewłaściwe użycie urządzeń

Choć niewłaściwe użycie urządzeń jest pojęciem bardzo szerokim to do podjęcia większości działań, które obejmuje ono swoim zakresem, konieczne jest posiadanie szczególnej wiedzy lub umiejętności.

W tym wypadku, nie można zapominać o tym, że Internet jest tak obszernym źródłem informacji, w którym bez problemu znajdziemy wskazówki dotyczące produkcji urządzeń lub programów komputerowych, czy też zdobędziemy wiedzę o lukach i słabościach występujących w zabezpieczeniach konkretnych systemów[308].

Zatem zasadne wydaje się rozszerzenie zakresu kryminalizacji zamachów na bezpieczeństwo przetwarzanej elektronicznie informacji i systemy komputerowe na stadium przygotowania przestępstwa i wprowadzenie karalności tworzenia, pozyskiwania, udostępniania, a także zbywania narzędzi, które mogłyby posłużyć do ataków na bezpieczeństwo danych oraz systemów informatycznych.

[307] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 161.
[308] Ibidem, s. 162.

A. KONWENCJA RADY EUROPY

Zgodnie z art. 6 Konwencji „każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnych i bezprawnych:

a. produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:

i. urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5,

ii. hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2 -5,

b. posiadania jednostki wymienionej powyżej w punktach a. i. lub ii. z zamiarem wykorzystania w celu popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5. Strona może w swoim prawie wprowadzić wymóg, że odpowiedzialność karna dotyczy posiadania większej ilości takich jednostek."

Ustawodawca unijny dał stronom możliwość wprowadzenia w wewnętrznych systemach prawnych wymogu posiadania większej liczby jednostek wymienionych w punktach a. i. lub ii., aby pociągnięcie do odpowiedzialności karnej było możliwe. Wskazuje to na próbę przeciwdziałania trendom z zakresu automatyzacji cyberprzestępczości[309].

Ponadto, Europejski Komitet ds. Przestępczości zaznaczył, że niniejszy artykuł nie ma na celu penalizacji zachowań, o których mowa w ustępie 1, jeżeli nie są one dokonywane z zamiarem popełnienia przestępstw określonych w art. 2-5 omawianej Konwencji, jak np. dozwolonego testowania czy też ochrony systemu informatycznego[310].

Wskazany przepis zakazuje produkcji, sprzedaży czy też rozpowszechniania urządzeń, które mogą zostać wykorzystane w celu popełnienia któregokolwiek z wcześniej omówionych przestępstw. Zakaz ten obejmuje także inne środki, które umożliwiają nielegalny dostęp treści zawartych w systemach informatycznych. Nałożenie na strony obowiązku penalizacji takich zachowań miało zapobiec wymianie sprzętu oraz aplikacji wykorzystywanych w celu ominięcia zabezpieczeń oraz uniemożliwić mniej zaawansowanym technologicznie

[309] Ibidem, s. 163.
[310] Art. 5 ust. 2 Konwencji o cyberprzestępczości.

użytkownikom dokonywania zamachów[311].

Twórcy Konwencji długo zastanawiali się nad tym czy omawiany przepis powinien dotyczyć jedynie tych urządzeń, które są przeznaczone wyłącznie do popełniania przestępstw, czy także tych, które mają podwójne zastosowanie - mogą być wykorzystywane zarówno przez administratorów systemów, jak i przestępców. Możliwość dwojakiego zastosowania oprogramowania stwarza wiele problemów natury dowodowej i może skutkować pociągnięciem do odpowiedzialności karnej osoby, która zajmuje się produkcją lub dystrybucją. Niemożliwa jest kryminalizacja wytwarzania i rozpowszechniania wszystkich urządzeń, które mogłyby zostać wykorzystane w celach przestępczych. Dlatego też, Konwencja ogranicza zakres penalizacji do przypadków, w których urządzenia są obiektywnie zaprojektowane lub przeznaczone do popełnienia przestępstwa. Zarazem wyklucza to urządzenia podwójnego zastosowania[312], a narzędzia produkowane w celu dokonywania analizy sieci i testowania zabezpieczeń należy tarkować, jak produkty legalne.

Odpowiednio do ustępu 3, strony mogą zagwarantować sobie prawo do niestosowania postanowień ustępu 1, z zastrzeżeniem, że sytuacja taka nie dotyczy sprzedaży, rozpowszechnia, bądź innego udostępniania jednostek wyszczególnionych w ustępie 1 a.ii.

B. USTAWODAWSTWO POLSKIE

Art. 269b rozszerza przyjęte standardy kryminalizacji ataków na bezpieczeństwo przetwarzanej elektronicznie informacji na stadium przygotowania i w ślad za art. 6 Konwencji, przewiduje odpowiedzialność karną każdego, kto „wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 2, art. 286a § 1 albo 2 w zw. z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej". Ponadto, ustawodawca przewiduje obligatoryjny przepadek tzw. urządzeń hakerskich, nawet, jeśli nie były one własnością sprawcy.

Dobrem chronionym przez wyżej cytowany przepis jest bezpieczeństwo informacji oraz danych informatycznych mieszczących się w systemach i sieciach. Zakres ochrony obejmuje także te dobra prawne, których bezpieczeństwo jest uzależnione od właściwego

[311] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* op. cit., s. 42-3.
[312] Cybercrime Convention: Explanatory Report, pkt. 73.

funkcjonowania sieci informatycznych[313].

Czynność sprawcza sprowadza się do wytwarzania narzędzi hakerskich przez sprawcę samodzielnie bądź poprzez przystosowanie urządzeń i programów przeznaczonych do innych celów. Może on tego dokonać wyłącznie przez działanie, pozyskiwanie, które jest uzyskaniem dostępu do narzędzi gotowych, przeniesienie własności narzędzi na inną osobę, czyli zbycie oraz udostępnienie, będące umożliwieniem korzystania z narzędzi osobom trzecim, przy zachowaniu władztwa czy też dostępu do nich[314].

Choć ustawodawca przy opisie przedmiotów wykonawczych użył liczby mnogiej, penalizacją objęte jest udostępnienie już jednego hasła, czy zbycie pojedynczej kopii programu. Inaczej jednak wygląda kwestia wypełnienia znamion czasownikowych - dopuszczenie się czynności sprawczej wobec tylko jednej osoby nie będzie stanowiło dokonania. Gdyby było to wystarczające, prawodawca posłużyłby się liczbą pojedynczą także w innych przepisach, jak chociażby w art. 265 § 2 k.k.[315]. Sytuacja, w której sprawca dokonuje jednej z wymienionych przepisie czynności względem konkretnej osoby, przynajmniej licząc się z tym, że może ona wykorzystać dany program, bądź hasło do popełnienia czynu zabronionego, pozwala na kwalifikację jego zachowania, jako pomocnictwa przy przestępstwie popełnianym przez wspomnianą osobę[316].

Przestępstwo z art. 269b jest przestępstwem powszechnym oraz materialnym, którego skutek stanowi wytworzenie, pozyskanie, sprzedaż, czy też udostępnienie innym osobom urządzeń albo programów komputerowych dostosowanych do popełniania przestępstwa jak również haseł komputerowych, kodów dostępu oraz danych, które umożliwiają dostęp do informacji zawartych w systemach komputerowych i sieciach informatycznych. Choć co do zasady jest to przestępstwo z działania, może również zostać popełnione z zaniechania[317], lecz wyłącznie z winy umyślnej, w obu postaciach zamiaru (wytwarzanie i pozyskiwanie tylko z zamiarem bezpośrednim).

Warto jednak zauważyć, że dozwolone jest posiadanie urządzeń lub programów wymienionych w § 1, ponieważ penalizacji podlega tylko i wyłącznie ich rozpowszechnianie. Jednak ich zbycie lub udostępnienie może być już kwalifikowane jako pomocnictwo, a sprawca, w zależności od wymiaru kary, będzie odpowiadał za przestępstwo z art. 269b lub

---

[313] W. Wróbel [w:] A. Zoll (red.) *Kodeks karny. Część szczególna. Komentarz do artykułów 117-277 k.k.,* op. cit., s. 1528.
[314] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1241.
[315] Ibidem, s. 1243.
[316] F. Randoniewicz, *Odpowiedzialność karana za przestępstwo hackingu,* op. cit., s. 35-6.
[317] B. Kunicka-Michalska [w:] A. Wąsek, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316,* op. cit., s. 746.

za pomocnictwo do przestępstwa, za które przewidziana jest równa, bądź wyższa sankcja[318].

Za omawiane przestępstwo grozi kara pozbawienia wolności od 1 miesiąca do lat 3 i jest ono ścigane z oskarżenia publicznego.

C. WNIOSKI

Wprowadzenie art. 269b k.k. do polskiego prawa miało na celu jego dostosowanie do Konwencji o cyberprzestępczości. Przepis ten miał być rozwiązaniem problemu powszechnej dostępności narzędzi hakerskich, umożliwiających dokonywanie ataków nawet takim osobom, które dysponują zaledwie podstawową wiedzą z zakresu informatyki. Choć od początku był szeroko krytykowany, ze względu na liczne wady, do tej pory nie został on skorygowany.

Obecna konstrukcja omawianego artykułu jest przejawem przesadnej kryminalizacji życia społecznego. Gienas zauważa, że w przypadku zastosowania niewłaściwej wykładni, pod znakiem zapytania stanęłoby funkcjonowanie chociażby forów oraz list dyskusyjnych, dedykowanych wymianie informacji o bezpieczeństwie informatycznym. Konieczne jest zatem wprowadzenie klauzuli niekaralności osób, które wykorzystują narzędzia hakerskie w celach zgodnych z prawem, jak np. testowanie zabezpieczeń systemów[319]. Możliwe jest również zaliczenie takich działań do kontratypu szczególnych uprawnień lub obowiązków, bądź też eksperymentu poznawczego. Należy to uznać za przeoczenie ustawodawcy, zwłaszcza, że takie rozwiązanie zostało zastosowane w art. 6 ust. 2 Konwencji, które postanowienia miał realizować art. 269b k.k.

W praktyce stosunkowo trudno jest ustalić czy dane urządzenie bądź program zostały celowo stworzone lub przystosowane do popełniania wymienionych w przepisie przestępstw, czy też będą wykorzystywane do kontroli zabezpieczeń. Takie ujęcie może powodować liczne problemy interpretacyjne, gdyż, w przeważającej części, odróżnienie celu zakładanego przez twórcę aplikacji od jej faktycznego zastosowania w praktyce może być niezwykle trudne[320]. Adamski zauważa również, że omawiany przepis wprowadza ogólny, nieuzasadniony zakaz pozyskiwania danych, które umożliwiają dostęp do informacji mieszczących się w systemach informatycznych, co jest równoznaczne z kryminalizacją korzystania z wyszukiwarek internetowych[321]. Przepis ten pozostaje w sprzeczności z art. 6 Konwencji, który obejmuje

---

[318] G. R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny – komentarz,* op. cit., s. 1242.
[319] K.Gienias, *Zwalczanie cyberprzestępczości w świetle art. 296b Kodeksu karnego – problem tzw. hacking tools*, „Prawnik na łączach" 2006, nr 4, s. 2.
[320] A.Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem,* Wolters Kluwer Polska, Warszawa 2010, s. 232.
[321] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę* [w:] G. Szpor (red.), *Internet. Ochrona wolności, własności i bezpieczeństwa,* Wydawnictwo C.H. Beck, Warszawa 2011, s. 349.

swym zakresem te narzędzie hakerskie, które są „przeznaczone lub przystosowane przede wszystkim dla celów popełnienia", a nie jak art. 269b każde „oprogramowanie przystosowane" do popełnienia przestępstwa[322].

Ponadto, w odróżnieniu od rozwiązania przyjętego w Konwencji, omawiany przepis nie obliguje sprawcy do działania w zamiarze bezpośrednim - wystarczającą podstawę pociągnięcia do odpowiedzialności stanowi zamiar ewentualny. W efekcie umożliwia to ściganie np. operatorów witryn internetowych, którzy udostępniają oprogramowania do symulowania obciążenia systemów komputerowych [323] . Takie ukształtowanie odpowiedzialności może doprowadzić do represji wobec osób, którym będzie można jedynie udowodnić posiadanie oprogramowania, wymienionego w art. 269b k.k. Jednak możliwe jest wyłącznie odpowiedzialności na zasadach ogólnych, czyli poprzez działanie w ramach praw i obowiązków[324].

Problematyczne jest także zastosowanie zwrotu „inne dane", który otwiera bardzo szerokie możliwości interpretacji praktycznej. Można za nie uznać np. literaturę akademicką czy też inne publikacje, które mogą zainteresować potencjalnych sprawców. W skrajnym przypadku mogłoby to skutkować zakazem wydawania artykułów dotyczących problemu bezpieczeństwa informatycznego [325] . Ponadto, polski prawodawca nie skorzystał z przewidzianej w Konwencji możliwości ewentualnego wprowadzenia minimalnej liczby oprogramowań, czy też urządzeń, których posiadanie będzie podstawą do pociągnięcia do odpowiedzialności.

4.1.2. PRZESTĘPSTWA POPEŁNIONE Z WYKORZYSTANIEM KOMPUTERA

Poprzez przestępstwa popełniane z wykorzystaniem komputera należy rozumieć ataki skierowane przeciwko tradycyjnym dobrom prawnym, dokonywane z wykorzystaniem nowoczesnych technologii. Nie są one bezpośrednio skierowane przeciwko integralności, poufności oraz dostępności danych informatycznych, dlatego też, działania prewencyjne nie są związane z potrzebą zapewnienia systemom informatycznym należytego stopnia ochrony[326].

Konwencja Rady Europy definiuje dwa rodzaje czynów, należących do kategorii przestępstw popełnianych z wykorzystaniem komputera, a mianowicie oszustwo i fałszerstwo

---

[322] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 175.
[323] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem,* op. cit., s. 233.
[324] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 175.
[325] K. Gienias, *Zwalczanie cyberprzestępczości w świetle art. 296b Kodeksu karnego - problem tzw. hacking tools,* s. 5.
[326] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem,* Wolters Kluwer Polska, Warszawa 2010, s. 235-6.

komputerowe. Chodzi tu o klasyczne typy przestępstw, które wraz z rozwojem technik informatycznych, zaczęły wymagać nadania nowej postaci normatywnej[327].

4.1.2.1. Fałszerstwo komputerowe

Przez fałszerstwo komputerowe zazwyczaj rozumie się manipulowanie treścią dokumentu w jego multimedialnej postaci[328]. Przestępstwo to może być rozpatrywane w dwóch aspektach:

a. pod względem wykorzystania komputera, oprogramowania oraz urządzeń peryferyjnych, jako narzędzi fałszowania dokumentów klasycznych,
b. fałszerstwa dokumentów elektronicznych, poprzez wprowadzanie zmian w pamięci komputera czy wszelkich nośnikach informacji gdzie są one tworzone i gromadzone[329].

W odniesieniu do pierwszej grupy przestępstw możliwości oferowane przez współczesną technikę, powodują, że praktycznie nie istnieje dokument, którego nie dałoby się sfałszować. Kwestią podstawową, z punktu widzenia sprawcy, jest odpowiedni dobór sprzętu oraz materiałów, a także zapewnienie właściwych odwzorowań stosowanych zabezpieczeń[330]. Popełnienie tego przestępstwa ułatwia także proces przejmowania ról, które niegdyś spełniały maszyny do pisania, przez technologicznie zaawansowane komputery i dopasowane do nich drukarki.

Dokumentami elektronicznymi, będącymi obiektem drugiej grupy fałszerstw, są wszystkie treści przechowywane na komputerowych dyskach twardych, jak np. księgi handlowe, podatkowe, wszelkie ewidencje czy kartoteki. Ze względu na możliwość dokonania niezauważalnych zmian, które mogą dotyczyć wybranej kwestii lub wycinka danych, szansa ich wykrycia jest niewielka i często możliwa jedynie dla osoby posiadającej specjalistyczną wiedzę. Przestępstwa z tej grupy można dodatkowo podzielić na:

a. przestępstwa dokonywane przez właściciela dokumentu - zapis jawny nie ma nic wspólnego ze stanem rzeczywistym i służy jedynie jego ukryciu, jak np. w przypadku prowadzenie podwójnej księgowości, oraz
b. fałszerstwa będące wynikiem działania osób trzecich, polegające na dokonaniu niedostrzegalnej zmiany zarówno w danych przekazywanych, jak i gromadzonych[331].

---

[327] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 241.
[328] Ibidem, s. 298.
[329] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne,* op. cit., 36.
[330] Ibidem, s. 36.
[331] Ibidem, s. 38.

Cechą charakterystyczną fałszerstwa każdego typu jest to, że zachowanie sprawcy ma posłużyć jakiemuś wcześniej określonemu celowi dalszemu. Sprawca nie działa jedynie z zamiarem naruszenia wiarygodności danych lub programów komputerowych, tylko zmierza do osiągnięcia konkretnego rezultatu, jakim może być np. uzyskanie dostępu do poczty elektronicznej, czy konta bankowego poszkodowanego[332].

Przeciwdziałanie fałszerstwu komputerowemu nie ogranicza się jedynie do zapewnienia ochrony treści elektronicznego dokumentu, ale także zapobiegania ingerencji w wiarygodność programów oraz danych komputerowych, z zamiarem wykorzystania ich dla celów niezgodnych z prawem[333].

A. KONWENCJA RADY EUROPY

Według art. 7 Konwencji „każda strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego, bezprawnego wprowadzania, dokonywania zmian, wykasowywania lub usuwania danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to czy są one możliwe do bezpośredniego odczytania i zrozumiałe". Strony mogą także wprowadzić wymóg, uzależniający odpowiedzialność kamą od wystąpienia po stronie sprawcy zamiaru dokonania oszustwa lub podobnego, nieuczciwego zamiaru.

Cytowany artykuł miał wypełnić istniejącą w prawie karnym lukę, związaną z fałszerstwem tradycyjnym. Manipulacja treścią elektronicznego dokumentu, który ma wartość dowodową, może mieć tak samo poważne konsekwencje, jak tradycyjne akty fałszerstwa, jeśli osoba trzecia zostanie w ten sposób wprowadzona w błąd. Fałszerstwo komputerowe dotyczy nieautoryzowanego tworzenia lub zmieniania przechowywanych danych tak, aby nadać im inną wartość dowodową w ramach czynności prawnych. Przedmiotem ochrony jest bezpieczeństwo i wiarygodność danych elektronicznych mogących mieć wpływ na kształtowanie się stosunków prawnych[334].

Obiektywnym kryterium fałszerstwa komputerowego na tle Konwencji o cyberprzestępczości jest powstanie „danych nieautentycznych", które to sprawca zamierza wykorzystać w celach sprzecznych z prawem. Chcąc przypisać sprawcy winę, należy mu nie tylko udowodnić, że dokonał on sfałszowania danych lub programów komputerowych, ale

[332] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 300.
[333] Ibidem, s. 301.
[334] Cybercrime Convention: Explanatory Report, pkt. 81.

także, że podjęte przez niego działania miały na celu wzbudzenie u konkretnej osoby błędnego przeświadczenia, co do prawa, stosunku prawnego czy okoliczności mających znaczenia dla sprawy. Należy jednak dodać, że dane i programy są związane z prawem tylko w takim znaczeniu, że stanowią nośnik informacji posiadającej znaczenie prawne. Zatem brak wiarygodności danych nie zawsze będzie tożsamy z brakiem autentyczności informacji[335].

Art. 7 Konwencji ma stanowić ochronę równoległą wraz z przepisami kryminalizującymi tradycyjne fałszerstwo dokumentów, skupiając się przy tym na danych, które są odpowiednikiem publicznego lub prywatnego dokumentu, i wywołują skutki prawne. Bezprawne działanie, które doprowadza do postania danych nieidentycznych powoduję sytuację, która odpowiada tworzeniu fałszywego dokutemu[336].

B. USTAWODAWSTWO POLSKIE

Art. 270 § 1 k.k. penalizuje działanie polegające na podrabianiu, przerabianiu bądź też używaniu jako autentycznego dokumentu, który został podrobiony lub przerobiony. Dobrem chronionym jest autentyczność dokumentów w ich aspekcie dowodowym[337]. Ponadto, pośrednio ochronie podlega także poprawne funkcjonowanie organów sprawiedliwości czy tez innych organów władzy publicznej, które prowadzą postępowanie dowodowe[338].

Podmiotem przestępstwa z omawianego artykułu może być każda osoba, która podrabia lub przerabia dokument z zamiarem użycia go, jak autentycznego. Odmianą takiego zachowania może być używanie, jak autentycznego, dokumentu, który został podrobiony lub przerobiony. Sprawca może się posługiwać dokumentem, który sfałszował samodzielnie lub takim, który został sfałszowany przez inną osobę. Ponadto, użycie sfałszowanego dokumentu nie jest tożsame z każdym przypadkiem fizycznego wykorzystywania owego dokumentu - konieczne jest użycie go zgodnie z funkcją, jaką ma przypisaną w obrocie prawnym[339].

Przestępstwo z art. 270 § 1 k.k. mam charakter wieloodmianowy, a do czynności sprawczych należy: podrobienie, przerobienie oraz użycie dokumentu, który został przerobiony lub podrobiony, jako autentycznego. Sprawca, który w pierwszej kolejności podrobi lub przerobi dokument, a później wykorzysta go, jako autentyczny, odpowiada tylko za jeden czyn, z wyjątkiem, kiedy te zachowania dzielił dłuższy odstęp czasowy[340].

Przedmiotem wykonawczym fałszerstwa komputerowego jest dokument, a pojęcie te

---

[335] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 301-2.
[336] Cybercrime Convention: Explanatory Report, pkt. 83.
[337] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 304.
[338] Glosa do wyroku SN z dnia 4 września 2008 r., V KK 171/08.
[339] M. Gałązka [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1245-6.
[340] Ibidem, s. 1245.

należy rozumieć zgodnie z art. 115 § 14 k.k., co przesądza o tym, że przestępstwo z art. 270 § 1 k.k. należy traktować na równi z fałszerstwem tradycyjnym[341]. Pojawił się także pogląd, że z uwagi na logiczną sprzeczność między określeniami „podrobiony" i „dokument", bardziej zasadne byłoby posługiwanie się w tym przypadku terminem „imitacja dokumentu" sporządzona przez sprawcę[342].

Omawiane przestępstwo ma charakter formalny, a dla realizacji jego znamion nie jest konieczne, aby przedstawienie innej osobie sfałszowanego dokumentu wywołało u niej przekonanie o jego prawdziwość[343]. Jest to przestępstwo umyślne o charakterze kierunkowym, bowiem podrobienie i przerobienie wymagają podjęcia działań w celu posłużenia się dokumentem, jako autentycznym, więc mogą być popełnione jedynie z zamiarem bezpośrednim[344].

W przypadku przepisu z art. 267 § 1 k.k. należy także zwrócić uwagę na nowelizację z 18 marca 2004 roku, która zmieniła dotychczas obowiązującą definicję: „każdy przedmiot lub zapis na komputerowym nośniku informacji" na „każdy przedmiot lub inny zapisany nośnik informacji". Zmiana ta przyczyniła się do powstania poważnych rozbieżności interpretacyjnych i, jak zauważa Adamski, powinna zostać oceniona negatywnie, ze względu na zawężenie ochrony prawnokarnej dokumentu elektronicznego. Nadmienia on także, że przyjęte rozwiązanie powoduje, że ochronie podlegają tylko te nośniki danych, które są przedmiotami, a odbiera ten przywilej danym jako takim[345].

Oczywistym jest jednak, że pojęcie dokumentu nie powinno być rozpatrywane jedynie w nawiązaniu do pomiotów materialnych, lecz powinno obejmować wszystkie przedmioty materialne wraz z ich elektronicznymi zapisami, pod warunkiem, że umożliwiają one określenie treści powiązanego z nimi prawa. Natomiast, przy tworzeniu definicji dokumentu należy się skupić na problematyce funkcjonowania prawa ujawnianego, a nie samym przedmiocie[346].

Warto również zauważyć, że na gruncie kodeksowej definicji, dokument elektroniczny wysyłany ze stacjonarnego urządzenia, w momencie przesyłania traci właściwość dokumentu, ponieważ nie jest zapisany, a wyłącznie przesyłany. Po dotarciu do urządzenia odbiorczego podlega on zapisowi na nośniku materialnym, odzyskując tym samym status dokumentu.

---

[341] Ibidem, s. 1245.
[342] Wyrok SN z dnia 17.03.2015r., IKZP 2/05, OSNKW 2005, nr 3, poz. 25.
[343] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 305.
[344] M. Gałązka [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* Wydawnictwo C.H. Beck, Warszawa 2015, s. 1247.
[345] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 306.
[346] Ibidem, s. 307.

Wynika z tego, że choć na etapie przesyłania istnieje możliwość sfałszowania, taka ingerencja nie będzie traktowana jako fałsz materialny, a jako szkoda w bazie danych bądź sabotaż informatyczny[347].

Przestępstwo z art. 267 § 1 k.k. jest zagrożone karą grzywny, ograniczania lub pozbawienia wolności od 3 miesięcy do lat 5, a w wypadku mniejszej wagi, podlega grzywnie, karze ograniczenia albo pozbawienia wolności do lat 2. Taka sama kara jest przewidziana za przygotowanie do popełnienia przestępstwa z art. 267 § 1 k.k. Ściganie następuje z urzędu.

C. WNIOSKI

Adamski uważa, że próba skorygowania definicji prawnej dokumentu z art. 115 § 14 k.k., w celu implementacji do Kodeksu karnego art. 7 Konwencji o cyberprzestępczości, zakończyła się porażką ustawodawcy. Był to krok wstecz, który dodatkowo ograniczył prawnokarną ochronę elektronicznego dokumentu przed fałszerstwem, przede wszystkim podczas transmisji danych[348]. Niezależnie od prezentowanego w doktrynie stanowiska w kwestii wykładni art. 115 § 14 k.k. należy stwierdzić, że prawodawca przyjął rozwiązanie odmienne od tego, które jest prezentowane w art. 7 Konwencji. Jest ono również niezgodne ze standardami promowanymi przez ONZ[349].

Co ciekawe, Adamski uważał ustawodawstwo polskie sprzed nowelizacji za „w zasadzie zgodne z art. 7 projektu konwencji i nie wymagające podejmowania zabiegów dostosowawczych w zakresie karalności fałszerstwa komputerowego”[350]. Należy w tym miejscu zaznaczyć, że projekt jedynie nieznacznie różni się od obecnego brzmienia Konwencji. Jednak już wtedy zwrócił on uwagę na konieczność zmiany treści z art. 115 § 14 k.k., proponując jednocześnie sformowanie „zapis na nośniku informacji”, które jego zdaniem usunęłoby wątpliwości interpretacyjne występujące na gruncie ówczesnego uregulowania.

4.1.2.2. Oszustwo komputerowe

Postęp techniczny oraz nieustający rozwój komunikacji elektronicznej wymusiły dostosowanie się sprawców do panujących warunków, czego efektem było powstanie nowego typu przestępstwa - oszustwa komputerowego[351]. Klasyczna postać oszustwa okazała się

---

[347] Ibidem, s. 308.
[348] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę* op. cit., s. 349.
[349] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 309.
[350] Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* s. 47.
[351] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspektyprawno-kryminalistyczne,* op. cit., 33.

niewystarczająca, gdyż w skutek automatyzacji procesów wymiany dóbr i usług, relacje interpersonalne zostały wyparte przez relacje człowiek-maszyna[352].

W praktyce, przestępstwo oszustwa komputerowego przyjmuje jedną z trzech form manipulacji:

a. manipulację danymi,
b. manipulację programami komputerowymi, oraz
c. manipulację rezultatami przetwarzanych danych.

Najprostszą z form, a przez to też najbardziej rozpowszechnią, jest manipulacja danymi, polegająca na wprowadzeniu do systemu błędnych danych, w celu uzyskania nieuprawnionych korzyści majątkowych [353].

Manipulacja programem jest przestępstwem bardzo trudnym do wykrycia, w którym to sprawca steruje istniejącym programem w taki sposób, aby wykonywał on nadprogramowe operacje pozwalające na dokonywanie nadużyć[354]. Co do zasady są one realizowane bez woli operatora, ale mogą być także podejmowane przez niego, w celu prowadzenia, wcześniej już wspomnianej, podwójnej księgowości[355].

W ostatnim przypadku, sprawca steruje rezultatami przetwarzanych danych, w efekcie osiągając korzyści majątkowe[356].

Przestępstwa te zaczęły występować już w latach 80., a pojedyncze nadużycia, nie powodujące dużych strat finansowych, są statystycznie najczęściej dokonywanymi przestępstwami z użyciem komputera na świecie[357].

A. KONWENCJA RADY EUROPY

Artykuł 8 Konwencji definiuje oszustwo komputerowe, jako „umyślne, bezprawne spowodowania utraty majątku przez inną osobę poprzez:

a. wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych,
b. każdą ingerencję w funkcjonowanie systemu komputerowego, z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.”

Celem niniejszego artykułu jest kryminalizacja wszelkich bezprawnych modyfikacji,

[352] Adamski A., *Prawo karne komputerowe,* s. 115.
[353] Ibidem, s. 241.
[354] A. Suchorzewska, *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzem,* s. 241.
[355] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne,* op. cit., 34.
[356] A. Suchorzewska, *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzem,* s. 241.
[357] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne,* op. cit., 33.

mających miejsce w trakcie przetwarzania danych, dokonywanych z zamiarem nielegalnego uzyskania korzyści majątkowych[358]. Adamski wskazuje, że definicja ta ma sporo cech wspólnych z ujęciem natury oszustwa komputerowego zaprezentowanym w zaleceniu Rady Europy z 1989 roku, także w tym względzie, że ustanawia typ przestępstwa skutkowego[359].

Także w przypadku oszustwa komputerowego, podobnie jak to miało miejsce w wypadku wcześniej omawianych artykułów Konwencji, konieczne jest wystąpienie znamienia bezprawności, które w tej sytuacji dotyczy także samego uzyskania korzyści majątkowych.

Pominięto jednak kluczowy dla klasycznego oszustwa element, jakim jest oddziaływanie sprawcy na osobę zarządzającą mieniem, który zastąpiło oddziaływanie sprawcy na przebieg automatycznego przetwarzania, gromadzenie lub transmisji danych komputerowych, bądź jego ingerencja w funkcjonowanie systemu komputerowego[360].

B. USTAWODAWSTWO POLSKIE

Art. 287 k.k. przewiduje karalność przestępstwa określanego mianem oszustwa komputerowego oraz jego wypadku mniejszej wagi. Chociaż w § 3 pojawia się termin „oszustwo" to omawiane przestępstwo znacznie różni się od swojej tradycyjnej formy z art. 286 § 1 k.k.[361] . Nie pojawia się znamię wprowadzenia w błąd, czy też spowodowania skutku w postaci uzyskania korzyści majątkowych bądź wyrządzenia szkody innej osobie. W tym zakresie jest to przestępstwo formalne, a określony w nim czyn różni się od definicji przyjętej w Konwencji[362].

Dobrem chronionym przez omawiany artykuł jest mienie w zakresie związanym z danymi informatycznymi - przedmiotem ataku są bowiem te prawa majątkowe, do których można się dostać jedynie za pośrednictwem danych informatycznych. Nie jest jednak wykluczone, że jego dalszym następstwem może być szkoda w mieniu niepowiązanym w żaden sposób z danymi. Pobocznej ochronie podgalają także systemy przetwarzania, gromadzenia i transmisji danych związanych z prawem majątkowym oraz integralność, poufność, a także dostępność tych danych[363]. Przepis ten nie obejmuje jednak ochroną osoby pokrzywdzonej.

Oszustwo z art. 287 k.k. staje się czynem dokonanym we wcześniejszym stadium niż

---

[358] Cybercrime Convention: Explanatory Report, pkt. 86.
[359] Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy,* s. 48.
[360] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 245.
[361] M. Gałązka [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1304.
[362] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 252.
[363] M. Gałązka [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1304.

jego klasyczna forma, a więc z chwilą podjęcia czynności sprawczych oddziaływania na urządzenia związane z przetwarzaniem danych oraz procesy techniczne[364].

Polski prawodawca przyjął inny niż wcześniej zaprezentowany podział postaci oszustwa komputerowego i wyróżnił dwie grupy czynności sprawczych:

a. wpływania na proces automatycznego przetwarzania, gromadzenia lub transmisji danych informatycznych, oraz
b. zmieniania, usuwania, bądź wprowadzania nowego zapisu danych informatycznych[365].

Pierwsza z wymienionych czynności sprawczych jest ingerencją w funkcje realizowane przez system informatyczny, druga natomiast - w zapisane dane informatyczne. Są one objęte zakazem karnym, gdy zostały podjęte bez upoważnienia, czyli stosowanego umocowania ze strony podmiotu uprawnionego. Ponadto, jeżeli któraś z wymienionych ingerencji zostaje poprzedzona przełamaniem lub też ominięciem specjalnego zabezpieczenia danych informatycznych, sprawca dopuścił się także czynu z art. 267 k.k., który to może zostać uznany za czyn współukarany uprzedni albo fragment czynu ciągłego[366].

Jak już wspomniano wcześniej, nie jest konieczne wystąpienie skutku w postaci jakiejkolwiek dyspozycji majątkowej, która byłaby odpowiednikiem rozporządzenia mieniem z art. 286 § 1 k.k. Mimo wszystko, nie decyduje to jednoznacznie o formalnym charakterze oszustwa komputerowego, gdyż nie rozstrzyga, czy znamiona opisujące czynności sprawcze wyrażają skutek sprowadzający się do efektywnego wywarcia wpływu na funkcjonowanie systemu, bądź też zmodyfikowaniu danych informatycznych. Jednak za taką interpretacją przemawia to, że w Kodeksie karnym, oprócz zastosowanego w omawianym przepisie pojęcia „wpływa", występuje także określenie „wywiera wpływ", które ma już wyraźne znaczenie skutkowe[367].

Uważa się, że skutkowe ujęcie tego przestępstwa mogłoby doprowadzić do pozostawienia poza ramami odpowiedzialności szereg zachowań uderzających bezpośrednio w urządzenia oraz systemy komputerowe. Zachowanie sprawcy zmierzające jedynie do osiągnięcia korzyści lub też wyrządzenia szkody innej osobie, jednocześnie nie prowadzące do powstania zmian w świecie zewnętrznym, znalazłoby się poza zakresem kryminalizacji art. 287 k.k.[368]. Jednak w literaturze występują także głosy przeciwne i np. Kardas uważa, że jest to

[364] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 252.
[365] A. Suchorzewska, *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzem,* s. 242.
[366] M. Gałązka [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1304-5.
[367] Ibidem, s. 1305.
[368] A. Suchorzewska, *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzem,* s. 243.

przestępstwo skutkowe, którego znamieniem jest skutek w postaci przeprowadzenia zmiany w automatycznym przetwarzaniu, gromadzeniu oraz transmisji lub też zmiana, usunięcie, czy też wprowadzenie nowego zapisu na nośniku[369].

W przeciwieństwie do art. 286 § 1 k.k., przedmiotem wykonawczym działania sprawcy nie jest człowiek, a urządzenie będące fragmentem systemu informatycznego, który funkcjonuje samodzielnie lub też nośnikiem zawierającym dane informatyczne. Sprawca wywiera wpływ nie tylko na proces decyzyjny innej osoby, ale również na procesy zachodzące automatycznie[370].

Przestępstwo oszustwa komputerowego można popełnić jedynie umyślnie, a ponadto ma ono charakter kierunkowy o zmiennym celu. Sprawca działa z zamiarem osiągnięcia korzyści majątkowej, bądź też wyrządzenia szkody innej osobie. Należy jednak pamiętać, że termin „szkoda" odnosi się wyłącznie do uszczerbku mającego charakter majątkowy[371]. Jest to przestępstwo powszechne.

Adamski zwraca także uwagę na to, że znamiona ustawowe omawianego przestępstwa pozwalają na kwalifikację wielu stanów faktycznych, w tym także dotyczących wyłudzeń usług telekomunikacyjnych na szkodę operatorów lub abonentów. Pozwala to na penalizację nie tylko oszustwa komputerowego, ale także telekomunikacyjnego, ponieważ w niektórych przypadkach wyznaczenie granicy między tymi przestępstwami jest niezwykle trudne[372].

Przestępstwo z art. 287 k.k. jest występkiem i podlega karze pozbawienia wolności od 3 miesięcy do lat 5, a wypadu mniejszej wagi, sprawcy grozi kara grzywny, ograniczenia lub pozbawienia wolności do roku. Ściganie następuje z urzędu, chyba, że poszkodowanym jest osoba najbliższa - wtedy na jej wniosek.

C. WNIOSKI

Polski prawodawca nadał przestępstwu oszustwa komputerowego charakter przestępstwa opierającego się na konstrukcji usiłowania, co doprowadziło do pozostawienia poza zakresem znamion ustawowych skutku tego czynu, występującego w postaci uzyskania korzyści majątkowych lub wyrządzenia szkody[373]. Stanowi to odstępstwo od definicji określonej w art. 8 Konwencji, w której znamiona ustawowe obejmują również skutek czynu w wyżej wymienionej postaci. Zatem należy zgodzić się z panującym poglądem, że czyn z art.

---

[369] P. Kardas, *Oszustwo komputerowe w kodeksie karnym,* „Przegląd Sądowy" 2000, nr 11-12, s. 43.
[370] M. Gałązka [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1304-5.
[371] Ibidem, s. 1305-6.
[372] Adamski A., *Prawo karne komputerowe,* s. 128-9.
[373] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę* op. cit., s. 349.

287 k.k. jest raczej manipulacją danymi informatycznymi w ramach prawa majątkowych, a nie oszustwem[374].

Ponadto, poza zakresem polskich unormowań pozostaje, penalizowana przez Konwencję, manipulacja systemem komputerowym niezwiązanym bezpośrednio z danymi informatycznymi [375].

Adamski wskazuje, że przepis spełnia raczej funkcję subsydiarną, zamiast pełnić rolę samodzielnego przepisu przeciwdziałającemu bezprawnym uszczupleniom majątkowym dokonywanym z wykorzystaniem nowoczesnych technologii. Ponadto, przepis ten wręcz utrudnia przyporządkowanie stanów faktycznych typowych dla dzisiejszej przestępczości internetowej[376].

4.1.3. PRZESTĘPSTWA ZWIĄZANE Z PORNOGRAFIĄ DZIECIĘCĄ

Dzięki sieciom oraz systemom informatycznym, a przede wszystkim Internetowi, niemal każdy ma możliwość udostępniania i publicznego przekazywania informacji o swoim życiu, aktualnych wydarzeniach, opiniach, ideach, być zarówno dziennikarzem, jaki i redaktorem czy wydawcą. Praktycznie każda upubliczniona informacja jest ogólnodostępna, bez względu na kraj pochodzenia dysponenta. Mimo wszystkich zalet jakie niesie za sobą ta szczególna możliwość, nie można zapominać o konieczności przeciwdziałania rozpowszechnianiu lub prezentowaniu informacji zakazanych przez prawo[377].

Na wstępie należy zaznaczyć, że zagadanie pornografii dziecięcej jest na tyle obszerne, że z powodzeniem mogłoby stanowić temat oddzielnego opracowania, dlatego też należy się ograniczyć jedynie do najważniejszych kwestii.

W obecnych czasach, w związku z niepowstrzymanym rozwojem technologicznym oraz wciąż postępującą skłonnością do rozluźniania więzów o charakterze moralnym i społecznym, zagadnienia powiązane z dostępem do treści pornograficznych, a także obrotem nimi, wymagają coraz to większej uwagi, a nurt ten widoczny jest także na gruncie prawa karnego[378].

Choć brak jest powszechnego porozumienia, co do zakresu znaczeniowego terminu pornografii, przez to pojęcie należy rozumieć „przedstawienie przejawów życia seksualnego ze

---

[374] M. Gałązka [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1304-5.
[375] Ibidem, s. 1304.
[375] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 258.
[376] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę* op. cit., s. 350.
[377] M. Siwicki, *Cyberprzestępczość*, op. cit., s. 177-8.
[378] M. Wrześniewski, *Krytycznie o przestępstwach pornograficznych*, „Prokuratura i Prawo" 2011, nr 11, s. 98.

szczególnym zwróceniem uwagi na uwidocznienie narządów płciowych i z wyłączeniem wszelkich aspektów psychicznych oraz społecznych związanych z seksualnością człowieka”[379]. Natomiast pojęcie pornografii dziecięcej zazwyczaj definiuje się w oparciu o powyższe wytłumaczenie, z zaznaczeniem, że prezentowane treści przedstawiają wykorzystywaną seksualnie osobę małoletnią, bądź jej genitalia, w celu pobudzenia seksualnego odbiorcy[380].

Pornografia dziecięca jest niezwykle istotnym problem, który niewątpliwie wymaga podjęcia działań na szczeblu międzynarodowym. Skuteczna walka z tym zjawiskiem wymaga przyjęcia wspólnych standardów kryminalizacji, dotyczących wszelkich form wykorzystania seksualnego małoletniego, a także przeciwdziałania popytowi na tego typu materiały[381].

A. KONWENCJA RADY EUROPY

Definicja pornografii dziecięcej zawarta w art. 9 Konwencji obejmuje materiał pornograficzny przedstawiający w widoczny sposób:

a. osobę małoletnią w trakcie czynności wyraźnie seksualnej,

b. osobę, która wydaje się być nieletnią, w trakcie czynności wyraźnie seksualnej,

c. realistyczny obraz przedstawiający osobę małoletnią w trakcie czynności wyraźnie seksualnej.

Rada Europy stanęła na stanowisku, że pojęcie pornografii dziecięcej obejmuje taki materiał pornograficzny, który w sposób wyraźny przedstawia osobę małoletnią podczas odbywania czynności seksualnej - takie ujęcie wyklucza materiały występujące w formie plików audio. Choć ustawodawca pozostawił w gestii stron zdefiniowanie pojęcia „materiału pornograficznego”, to jednak niezwykle drobiazgowo określił nadużycia seksualne wobec dzieci, które powinny być przedmiotem penalizacji. Zwrot „czynność wyraźnie seksualna” należy rozumieć co najmniej, jako rzeczywisty lub symulowany:

a. stosunek seksualny (kontakt między narządami płciowymi, pozycje genitalno- analne oraz genitalno-oralne) między małoletnimi oraz małoletnim i dorosłym, tej samej albo przeciwnej płci,
b. sodomię,
c. masturbację,

[379] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne,* op. cit., s. 132.
[380] M. Siwicki, *Cyberprzestępczość,* op. cit., s. 178.
[381] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne,* op. cit., s. 149.

d. masochistyczne lub sadystyczne wykorzystanie w kontekście seksualnym, oraz

e. lubieżne obnażanie narządów płciowych, czy miejsc intymnych ciała dziecka[382].

Granica wieku dojrzałości seksualnej określana jest w bardzo różnorodny sposób, lecz w dokumentach międzynarodowych, przez małoletniego rozumie się osobę poniżej 18 roku życia. Taki standard przyjęto także w ust. 3 art. 9 Konwencji, choć strona ma prawo wprowadzić wymóg niższej granicy wieku, która jednak nie może być niższa niż 16 lat.

Przepis ten penalizuje różne aspekty elektronicznej produkcji, posiadania i rozpowszechniania pornografii dziecięcej. Większość państw będących stronami Konwencji, dokonało kryminalizacji tradycyjnej produkcji i dystrybucji pornografii dziecięcej, jednak wciąż wzrastające użycie Internetu, jako podstawowego instrumentu do obrotu tego typu materiałami, wymagało wprowadzenia szczegółowych postanowień na szczeblu międzynarodowym, w celu efektywnego zwalczania tej nowej formy wykorzystywania seksualnego dzieci[383]. Dlatego też każda strona jest zobowiązana do pojęcia odpowiednich środków prawnych (i innych), niezbędnych do uznania za przestępstwo w jej prawie krajowym umyślnego i bezprawnego:

a. produkowania pornografii dziecięcej dla celów jej rozpowszechniania za pomocą systemu informatycznego,

b. oferowania lub udostępniania pornografii dziecięcej za pomocą systemu informatycznego,

c. rozpowszechniania lub transmitowanie pornografii dziecięcej za pomocą systemu informatycznego,

d. pozyskiwanie pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby,

e. posiadanie pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych.

Art. 9 Konwencji penalizuje nie tylko produkowanie pornografii dziecięcej z zamiarem jej rozpowszechniania, ale także jej oferowanie, udostępnianie oraz dystrybucję przy użyciu systemów informatycznych. Karalne jest również jej pozyskiwanie, a także samo posiadanie - ustawodawca uważa, że posiadanie pornografii dziecięcej stymuluje popyt na tego typu materiały. Skutecznym sposobem na ograniczenie produkcji pornografii dziecięcej ma być

[382] Cybercrime Convention: Explanatory Report, pkt. 100.
[383] Ibidem, s. 93.

więc obciążenie odpowiedzialnością karną każdego uczestnika procesu, od produkcji do posiadania[384].

Strony są zobowiązane do kryminalizacji czynów, jeżeli zostały one popełnione. Zgodnie z tym standardem, osoba nie ponosi odpowiedzialności, chyba że ma zamiar zaoferować, udostępniać, rozpowszechniać, przekazywać, produkować lub posiadać pornografię dziecięcą. Strony mogą także przyjąć bardziej szczegółowe normy[385].

B. USTAWODAWSTWO POLSKIE

Przestępstwa dotyczące zjawiska pornografii zostały stypizowane przez ustawodawcę w Kodeksie karnym z 1932 roku, a później, poddane pewnym modyfikacjom, znalazły się również w obowiązującej obecnie ustawie karnej, a konkretnie, w art. 202 k.k. Omawiana regulacja swym zakresem obejmuje niezwykle wrażliwą problematykę, którą jest życie seksualne człowieka oraz obyczajności w tej sferze. Podczas konstruowania tego typu uregulowań, prawodawca musi postępować niezwykle ostrożnie, gdyż nawet jeden błąd może spowodować dotkliwe konsekwencje, nie tylko dla sprawcy, ale również dla pokrzywdzonego[386].

W art. 202 k.k. prawodawca zawarł 6 typów czynów zabronionych poświęconych przeciwdziałaniu zjawisku pornografii dziecięcej, którego istotą jest wytwarzanie oraz obrót treściami przedstawiającymi inne osoby podczas czynności seksualnych albo osoby obnażone. Dodanie do art. 200 k.k., na skutek nowelizacji z 2014 roku, paragrafów 3-5 miało doprowadzić do ograniczenia prezentowania czy też udostępniania osobom małoletnim treści i przedmiotów o charakterze pornograficznym.

Ponadto, produkcja, utrwalanie bądź też sprowadzanie z zamiarem rozpowszechniania materiałów pornograficznych z udziałem małoletnich jest objęte zakazem bezwzględnym, co wpływa również na ujęcie przedmiotu ochrony w tym zakresie.

Dobrem chronionym będzie zatem szeroko pojmowana wolność seksualna dziecka, nie mogącego nią dysponować w racjonalny sposób, ze względu na swój wiek[387]. Pośrednio art. 202 § 3 k.k. chroni także obyczajność, a w jej granicach - prawidłowy rozwój dziecka, mogący zostać narażony na poważne zaburzenia w wyniku uczestniczenia w zakazanym procederze[388].

---

[384] Ibidem, pkt. 94-8.
[385] Ibidem, pkt. 105.
[386] M. Wrześniewski, *Krytycznie o przestępstwach pornograficznych,* op. cit. 98.
[387] J. Warylewski, Przestępstwa przeciwko wolności seksualnej i obyczajności. Rozdział XXV Kodeksu karnego. Komentarz, Wydawnictwo C.H. Beck, Warszawa 2001, Warszawa 2001, s. 91.
[388] J. Piórkowska-Flieger, *Przestępstwa przeciwko wolności seksualnej i obyczajności,* [w:] T. Bojarski (red.), *Kodeks karny. Komentarz,* LexisNexis, Warszawa 2013, s. 667.

Hypś uważa natomiast, że omawiany przepis ma celu ochronę obyczajności w aspekcie seksualnym, rozumianą jako potrzebę ochrony małoletniego przez niszczącym oddziaływaniem pornografii na jego rozwój psychofizyczny[389].

Czynnością sprawczą przestępstwa z 202 § 3 k.k. jest takie działanie sprawcy, które polega na produkcji, utrwalaniu lub sprowadzaniu treści pornograficznych z udziałem małoletnich w celu rozpowszechniania, a także ich posiadaniu, przechowywaniu oraz prezentacji. § 4b wskazuje, że zakaz ten obejmuje także treści przedstawiające wytworzony lub przetworzony wizerunek małoletniego, co określane jest mianem, tzw. pornografii pozorowanej. Wizerunek wytworzony obejmuje wszystkie treści o charakterze pornograficznym, przedstawiające wizerunek nierzeczywistego dziecka, np. narysowanego. Natomiast przez wizerunek przetworzony należy rozumieć zarówno osoby dorosłe ucharakteryzowane lub też przebrane za małoletniego, a także nierzeczywiste obrazy dorosłych, których wizerunek został przetworzony w podobny sposób[390].

Przestępstwo z art. 202 § 3 jest przestępstwem formalnym, którego dokonanie następuje wraz z podjęciem czynności wypełniających znamiona omawianego czynu. Jednak częściowo można je uznać za kierunkowe, ponieważ zakazuje podejmowania określanych działań z zamiarem rozpowszechniania - tylko wtedy jest możliwa ochrona. Zatem poza zakresem ochrony pozostają treści, które zostały stworzone na własny, prywatny użytek. Nie dotyczy to jednak typu kwalifikowanego z § 4, który wprowadza bezwzględny zakaz produkcji materiałów pornograficznych z udziałem małoletniego, niezależnie od celu, w którym działał sprawca. Zakres kryminalizacji obejmuje nie tylko producentów, ale także odbiorców zakazanych treści[391].

Przedmiotem czynności wykonawczej przestępstw z art. 202 k.k. są nośniki treści pornograficznych, czyli konkretne wytwory służące wywołaniu u odbiorcy efektu zaspokojenia lub pobudzenia seksualnego[392]. Ponadto, art. 202 § 4a k.k. obejmie również uzyskiwanie dostępu do treści pornograficznych za pośrednictwem systemów teleinformatycznych.

Przestępstwo pornografii ma charakter powszechny i może być popełnione jedynie umyślenie, zarówno z zamiarem bezpośrednim, jak i indywidualnym. Przy czym, przestępstwa z art. 202 § 3 i 4c występują jedynie w zamiarze bezpośrednim. Wszystkie przestępstwa z art. 202 k.k. są występkami, których ściganie następuje z urzędu[393].

---

[389] S. Hypś [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1017.
[390] Ibidem, s. 1018-20.
[391] Ibidem, s. 1019-20.
[392] Ibidem, s. 1021.
[393] Ibidem, s. 1021.

C. WNIOSKI

Krajowy model prawnokarnej kontroli pornografii dziecięcej skierowany jest przeciwko producentom oraz dystrybutorom, a ponadto przewiduje także odpowiedzialność kamą konsumentów i w tym zakresie odpowiada on standardom międzynarodowym. Jednak niektóre negatywne zachowania zawarte w Konwencji znajdowały się poza regulacją kodeksową, aż do nowelizacji z 2014 roku. Podstawową kwestią, w której polska regulacja odbiegała od europejskiej był wiek osoby małoletniej. Krajowy prawodawca uzależnił bowiem ochronę od dwóch kategorii małoletnich: tych, którzy nie ukończyli 15 lat oraz tych, którzy nie ukończyli 18. Nowelizacja wprowadziła jedną granicę wieku - wynoszącą 18 lat[394], co jest zgodne zarówno z wymogami Konwencji, jak i dyrektywą Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej[395].

Istotną zmianą jest także wprowadzenie przestępstwa przewidującego odpowiedzialność karną osób, które w celu zaspokojenia seksualnego uczestniczyły w przedstawieniach pornograficznych z uczestnictwem małoletnich[396].

Koniecznym wydaje się jednak uzupełnienie katalogu czynności wykonawczych art. 202 k.k. o czynność „przesyłania", co wzmocni funkcję ochronną tego przepisu, a także umożliwi jego dostosowanie standardu normatywnego wyrażonego w art. 9 Konwencji. Natomiast na aprobatę zasługuje wzmocnienie ochrony prawnej dzieci przed zjawiskiem pornografii internetowej oraz pozorowanej[397].

4.1.4. PRZESTĘPSTWA ZWIĄZANE Z NARUSZENIEM PRAW AUTORSKICH I POKREWNYCH

Naruszenia praw własności intelektualnej, w szczególności praw autorskich, są jednymi z najczęściej popełnianych przestępstw w Internecie, co powoduje niepokój zarówno posiadaczy praw autorskich, jak i tych, którzy są zawodowo związani z sieciami komputerowymi. Kopiowanie i rozpowszechnianie w Internecie utworów chronionych, dokonywane bez zgody właściciela praw autorskich, jest zjawiskiem niezwykle powszechnym. Łatwość z jaką nieautoryzowane kopie są wykonywane oraz skala ich rozpowszechniania

[394] Ibidem, 1016.
[395] Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (2011/93/UE).
[396] S. Hypś [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny - komentarz,* op. cit., s. 1020.
[397] P. Kozłowska, M. Kucharska, *Prawnokarne aspekty pornografii*, „Prokuratura i Prawo" 1999, nr 4, 210-12.

w ramach sieci informatycznych, spowodowały konieczność zwiększenia współpracy międzynarodowej w tym zakresie oraz wypracowania przepisów gwarantujących sankcje karne[398].

A. KONWENCJA RADY EUROPY

Zgodnie z art. 10 Konwencji dotyczącym przestępstw związanych z naruszaniem praw autorskich oraz praw pokrewnych, każda strona jest zobowiązana podjąć takie środki prawne (i inne) jakie okażą się konieczne do uznania za przestępstwo w jej prawie krajowym:

a. naruszeń prawa autorskiego zdefiniowanych w prawie danej strony zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Aktu Paryskiego z dnia 24 lipca 1971 roku zmieniającego Konwencję Berneńską o ochronie dzieł literackich i artystycznych, Porozumienia w sprawie handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o prawach autorskich, z wyłączeniem praw osobistych przewidzianych przez te Konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego, oraz
b. naruszeń praw pokrewnych zdefiniowanych w prawie danej strony, zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Międzynarodowej Konwencji o ochronie wykonawców, producentów fonogramów oraz organizacji nadawczych zawartej w Rzymie (Konwencja Rzymska), Umowy w sprawie handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o wykonaniach i fonogramach, z wyłączeniem praw osobistych przewidzianych przez te konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego.

Ustęp 3 daje stronom możliwość zastrzeżenia sobie prawa do niepociągania do odpowiedzialności karnej za wskazane wyżej czyny w „pewnych wypadkach" tak długo, jak inne skuteczne środki zaradcze, w tym także środki cywilne i/lub administracyjne, są dostępne[399]. Jednak nie może to stanowić odstępstwa od międzynarodowych zobowiązań jakimi związana jest strona, wynikających z dokumentów wymienionych w ustępie 1 i 2. Ponadto, z zakresu kryminalizacji naruszeń prawa autorskiego i praw pokrewnych, wyłącza się

[398] Cybercrime Convention: Explanatory Report, pkt. 107.
[399] Ibidem, pkt. 116.

prawa ograniczone przewidziane przez Konwencję.

Każda ze stron ma obowiązek kryminalizacji umyślnego naruszenia prawa autorskiego oraz praw pokrewnych, zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z umów wymienionych w omawianym artykule, jeśli takie naruszenia miały miejsce z wykorzystaniem systemów informatycznych i na skalę komercyjną[400].

Warto zauważyć, że termin „bezprawnie" został pominięty w tekście tego artykułu, jako zbędny, - samo „naruszenie" oznacza korzystanie z materiałów chronionych bez zezwolenia[401].

C. USTAWODAWSTWO POLSKIE

Odpowiedzialność karna za omawiane przestępstwa została uregulowana w ustawie o prawie autorskim i prawach pokrewnych (art. 115-123 pr. aut.). Wszystkie czyny zabronione są przestępstwami umyślnymi[402] o charakterze powszechnym. Natomiast sprawcą nie jest tylko ten, kto samodzielnie lub też wspólnie dokonuje czynu zabronionego, ale również ten, kto kieruje jego wykonaniem przez inną osobę bądź też wykorzystując stosunek zależności, który łączy go z nią osobą - poleca jej wykonanie konkretnego czynu (art. 18 § 1 k.k.). W większości przypadków możliwa jest także odpowiedzialność podmiotów zbiorowych[403].

Przestępstwem jest każdy czyn naruszający przepisy ustawy, pod warunkiem, że został on popełniony z zamiarem osiągnięcia korzyści majątkowej. Jednak, w wielu przypadkach, istnieją wątpliwości co do tego czy dane zachowanie jest naruszeniem prawa autorskiego, np. ze względu na trudności z ustaleniem czy dany wytwór intelektualny jest faktycznie utworem, a w efekcie rodzi niepewność sprawcy co do jego odpowiedzialności. W tym wypadku szczególne znaczenie ma art. 30 k.k., zgodnie z którym „nie popełnia przestępstwa, kto dopuszcza się czynu zabronionego w usprawiedliwionej nieświadomości jego bezprawności; jeżeli błąd sprawcy jest nieusprawiedliwiony, sąd może zastosować nadzwyczajne złagodzenie kary". Warto również zauważyć, że przewidziane w ustawie sankcje są relatywnie wysokie - nawet do 5 lat pozbawienia wolności, w sytuacji, gdy sprawca traktuje przestępstwo jak stałe źródło dochodu[404].

Ustawa kładzie szczególny nacisk na ochronę prawa do autorstwa, integralności dzieła oraz wykonania artystycznego. W tym przypadku odpowiedzialność karna jest niezależna od

[400] Ibidem, pkt. 108.
[401] Ibidem, s. 115.
[402] Przestępstwa z art. 116 ust. i art. 118 ust. 3 pr. aut. mogą być także popełnione z winy nieumyślnej.
[403] J. Barta, R. Markiewicz (wstęp), *Prawo autorskie i prawa pokrewne*, Wolters Kluwer Polska, Warszawa 2007, s. 190.
[404] Ibidem, s. 190.

tego czy sprawca działał z zamiarem uzyskania korzyści majątkowej, a dotyczy to: przywłaszczenia autorstwa, wprowadzenia w błąd co do niego, rozpowszechniania dóbr objętych ochroną bez wskazania autorstwa oraz ich publicznego zniekształcenia. Wprowadzono także odrębną regulację w odniesieniu do: rozpowszechniania, utrwalania oraz zwielokrotniania utworu bez uprawnień, bądź niezgodnie z ich warunkami[405].

Karze podlega również paserstwo w odniesieniu do utworów, wykonań artystycznych, fonogramów i wideogramów. We wszystkich przypadkach przewidziany został typ kwalifikowany, wynikający z sytuacji, w której traktuje przestępstwo jak stałe źródło dochodu bądź taką działalnością kieruje. Regulacja przyjęta w tym zakresie (art. 116-18 pr. aut.) jest podstawowym instrumentem do walki z tzw. piractwem w zakresie prawa autorskiego[406].

Karalne jest także wytwarzanie, posiadanie, przechowywanie oraz wykorzystywanie „urządzenia lub ich komponentów przeznaczonych do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów”[407]. Wskazuje się tu na błędne sformułowanie przepisu, ze względu na trudności w dokonaniu oceny przeznaczenia urządzeń używanych w celach niedozwolonych. Ponadto, sprawca może wykazać, że określone urządzenie jest przeznaczone również do dopuszczalnego uzyskiwania dostępu do utworu, obywającego się w ramach realnego użytku[408].

C. WNIOSKI

Adamski wskazuje na potrzebę zachowania równowagi między interesem społecznym a interesem twórców, co wydaje się być niezwykle istotne w czasach, w których rozpowszechnianie treści za pośrednictwem sieci informatycznych jest codziennością. Choć naruszenie praw własności intelektualnej jest jednym z najczęściej popełnianych przestępstw, nie należy zapominać o prawie obywateli do nieskrępowanego dostępu informacji oraz dóbr kultury. Stosowanie środków karnych w celu zapewnienia ochrony praw autorskich wymaga umiaru oraz ostrożności w dostosowywaniu prawa krajowego do międzynarodowych standardów normatywnych. Wydawałoby się, że polski prawodawca ma skłonność do nadmiernej penalizacji naruszeń tych praw, na co wskazuje chociażby rozszerzenie karalności na nieumyślne naruszenie praw majątkowych twórców oraz producentów programów.

---

[405] Ibidem, s, 191.
[4]Ibidem, s. 192.
[407] Art. 118[1] § 1 pr. aut.
[408] J. Barta, R. Markiewicz (wstęp), *Prawo autorskie i prawa pokrewne*, op. cit., s. 192.

4.2. WNIOSKI

Ocena zgodności przepisów Kodeksu karnego z rozwiązaniami, jakie przewiduje Konwencja o cyberprzestępczości, była podejmowana już kilkukrotnie, zawsze z tym samym skutkiem - stwierdzano częściowy brak spójności pomiędzy tymi regulacjami prawnymi. Głównym zarzutem były luki prawne występujące w polskim ustawodawstwie karanym, wynikające z pominięcia niektórych przestępstw konwencyjnych, bądź ich nieprawidłowej transpozycji do krajowego porządku prawnego[409].

Za nie w pełni zgodne ze standardami normatywnymi wyrażonymi w Konwencji należy uznać kodeksowe unormowania aż pięciu z ośmiu rodzajów przestępstw, a mianowicie: ingerencję w dane, nadużycie narzędzi, fałszerstwo oraz oszustwo komputerowe, a także kwestię pornografii dziecięcej. Wskazuje to na konieczność wprowadzenia kolejnych zmian do Kodeksu karnego z 1997 roku, aby w pełni odpowiadał on standardom międzynarodowym.

Adamski wskazuje ponadto, ze lista rozbieżności pomiędzy Kodeksem karnym a materialnoprawną częścią Konwencji jest znacznie dłuższa niż wynika to z uzasadnienia wniosku o wyrażenie zgody na ratyfikację Konwencji, które to w zasadzie dowodziło o zgodności prawa procesowego z postanowieniami Konwencji[410].

[409] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę* op. cit., s. 353.
[410] Ibidem, s. 354.

ZAKOŃCZENIE

Trwający już ponad czterdzieści lat rozkwit technologii komputerowych pokazał, że korzystanie z najnowszych osiągnięć techniki oraz wolności informacji wymaga wyznaczenia jasno określonych granic oraz stosowania spójnych regulacji. Międzynarodowy charakter cyberprzestępczości oraz nieustający wzrost strat przez nią powodowanych podkreślają konieczność podjęcia współpracy międzypaństwowej, będącej gwarantem globalnego bezpieczeństwa.

Ponadto, jest to zjawisko niezwykle dynamiczne, a różnorodność metod stosowanych przez sprawców będzie przyczyną coraz to nowszych konfliktów. Brak podjęcia odpowiednich działań w kierunku ochrony sieci i systemów komputerowych, w sytuacji wciąż rosnącej od nich zależności człowieka, może być katastrofalny w skutkach.

Aby współpraca międzynarodowa w zakresie zwalczania cyberprzestępczości była efektywna, konieczne jest przyjęcie jednorodnych środków karnych w ustawodawstwie poszczególnych krajów. Choć polski ustawodawca wydawał się być tego świadomy, przyjęte przez niego rozwiązania zależy uznać za nie w pełni zgodne ze standardami normatywnymi wyrażonymi w Konwencji. Brak spójności wynika z pominięcia niektórych przestępstw konwencyjnych lub też ich nieprawidłowej transpozycji do krajowego porządku prawnego.

Należy jednak pamiętać, że nawet najlepsze przepisy nie będą skuteczne, jeżeli użytkownicy nie będą świadomi zagrożenia, jakie niesie za sobą rozwój nowoczesnych technologii.

SPIS TABEL

BIBLIOGRAFIA

AKTY NORMATYWNE I INNE DOKUMENTY

1. Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (97/66/WE);
2. Dyrektywa Parlamentu i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (2000/31/WE);
3. Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (2011/93/UE);
4. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW;
5. EU Commision: Ensuring security and trust in electronic communication. Towards a European framework for digital signatures and encryption. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions (COM (97) 503 final);
6. EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace [Online], dostęp: 4.05.2015, http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf;
7. Glosa do wyroku SN z dnia 4 września 2008 r., V KK 171/08;
8. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee Of The Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN/2013/0001);
9. Komisja Europejska - Komunikat Prasowy: Unijne centrum ds. walki z cyberprzestępczością będzie zwalczać przestępstwa internetowe i chronić e-konsumentów [on-line], dostęp: 5.05.2015, http://europa.eu/rapid/press-release_IP-12-317_pl.htm;
10. Komisja Europejska - Komunikat Prasowy: Europejskie Centrum ds. Walki z Cyberprzestępczością - pierwszy rok działalności [on-line], dostęp: 5.05.215, http://europa.eu/rapid/press-release_IP-14-129_pl.htm;

11. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. (Dz.U. 1993 nr 61, poz. 284);
12. Ministerstwo Gospodarki - ePolska. Plan działania na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 - 2006;
13. OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, Report DSTI-ICCP 84.22 of 18 April 1986;
14. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [on-line], C(2002)131/FINAL, 29 July 2002, dostęp: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C%282002%2913 l/FINAL&docLanguage=En;
15. OECD, Computer Viruses and Other Malicious Software: A Threat to the Internet Economy [on-line], dostęp: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other- malicious-software_9789264056510-en#pagel;
16. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej [on-line], Warszawa 2013, dostęp: 29.04.2015, http://www.cert.gov.pl/cer/publikacj e/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej .html;
17. Protocol (No 36) on transitional provisions (EUR-Lex, nr 12008M/PRO/36);
18. Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer-related crime and final Report of the European Committee on Crime Problems;
19. Report on Europę and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council, Bulletin of the European Union, Supplement No. 2/94;
20. Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 - założenia [on-line], Warszawa 2009, dostęp: 29.04.2015, https://www.msz.gov.pl/resource/93ele4c7-el29-41c7-8365- 39dbad8blc54:JCR;
21. Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 [on-line], dostęp: 29.04.2015, http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html;
22. Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający

Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r., Dz.U. 2009 nr 203, poz. 1569;

23. Traktat o funkcjonowaniu Unii Europejskiej, Dz.Urz. UE 2012, C 326/47;
24. United States Government Accountability Office: Report to Congressional Committees, *Intellectual Property: Observations on Efforts to Quantijy the Economic Effects of Counterfeit and Pirated Goods*, GAO-10-423, April 2010;
25. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24, poz. 83);
26. Ustawa z dnia 6 czerwca 1997 r. - Kodeks kamy (Dz.U. 1997 nr 88, poz. 553);
27. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133, poz. 883);
28. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144, poz. 1204);
29. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2002 r. nr 156, poz. 1301);
30. Ustawa z dnia 18 marca 2004 r. o zmianie ustawy - Kodeks kamy, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń (Dz.U. 2004 nr 69, poz. 626);
31. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 r. nr 64, poz. 565);
32. Ustawa z dnia 24 października 2008 r. o zmianie ustawy - Kodeks kamy oraz niektórych innych ustaw (Dz.U. 2008 nr 214, poz. 1344);
33. Uzasadnienie projektu ustawy o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.;
34. World Summit on the Information Society Geneva 2003 - Tunis 2005, WSIS-03/GENEVA/DOC/5-E, 12 December 2003;
35. World Summit on the Information Society Geneva 2003 - Tunis 2005, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2015;
36. Wyrok SN z dnia 17.03.2015 r., IKZP 2/05, OSNKW 2005, nr 3, poz. 25;

MONOGRAFIE

1. Adamski A., *Crimes Related to Computer NetWork. Threats and Opportunities: A Criminological Perspective*, [w:] M. Joutsen (red.), *Five Issues in European Criminal Justice: Corruption, Women in the Criminal Justice System, Criminal Policy*

Indicators, Community Crime Prevention and Computer Crime, HEUNI, Publication Series No. 34, Helsinki 1999;
2. Adamski A., *Prawo karne komputerowe*, Wydawnictwo C.H. Beck, Warszawa 2000;
3. Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Wydawnictwo „Dom Organizatora", Toruń 2001;
4. Ariwa E., El-Qawasmeh E., Sedoyeka E, Yonazi J. J. (red.), *e-Technologies and Networks for Development,* Springer-Verlag, Berlin 2011;
5. Barta J., Markiewicz R. (wstęp), *Prawo autorskie i prawa pokrewne,* Wolters Kluwer Polska, Warszawa 2007;
6. Bębas S., Plis J., Bednarek J. (red.), *Patologie w cyberświecie*, Wyższa Szkoła Handlowa, Radom 2012;
7. Białogórksi R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku: zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011;
8. Bienias T., *Internet*, Wydawnictwo Znak, Kraków 1998;
9. Bojarski T. (red.), *Kodeks karny. Komentarz,* LexisNexis, Warszawa 2013;
10. Brenner S., *Cybercrime: Criminal Threats from Cyberspace,* USA: ABC-CLIO, Santa Barbara, 2010, s. 9-10;
11. Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania* [on-line], Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, dostęp: 21.02.2015: http://informacjacyfrowa.wsb.edu.pl/pdfs/SpoleczenstwoInformacyjne.pdf;
12. Golat R., *Prawo Internetu dla praktyków*, Ośrodek Doradztwa i Doskonalenia Kadr Sp. z o.o., Gdańsk 2009;
13. Grześkowiak A., Wiak K. (red.), *Kodeks karny - komentarz,* Wydawnictwo C.H. Beck, Warszawa 2015;
14. Hofmolk J., *Internet jako nowe dobro wspólne*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2009;
15. B. Hołyst, *Kryminologia,* LexisNexis Polska, Warszawa 2009;
16. Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Difin SA, Warszawa 2014;
17. Kosiński J., *Pradygmaty cyberprzetępczości*, Difin SA, Warszawa 2015;
18. Kulesza J., *Międzynarodowe Prawo Internetu,* Ars boni et aeąui, Poznań 2010;
19. Kunicka-Michalska B., *Przestępstwa przeciwko ochronie informacji i*

wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz, Wydawnictwo C.H. Beck, Warszawa 2010;

20. Lubacz J. (red.), *W drodze do społeczeństwa informacyjnego*, Drukarnia Oficyny Wydawniczej Politechniki Warszawskiej, Warszawa 1999;
21. Marek A., *Kodeks karny. Komentarz*, Wolters Kluwer Polska, Warszawa 2010;
22. Misiuk A., Ciszek P., Kosiński J., Przestępczość teleinformatyczna: VI seminarium naukowe, Wyższa Szkoła Policji, Szczytno 2003;
23. Mozgawa M. (red.), Kodeks karny. Komentarz, LexisNexis Polska, Warszawa 2013;
24. Porębski L., *Elektroniczne oblicze polityki: demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Uczelniane Wydawnictwo Naukowo-Dydaktyczne AGH, Kraków 2001;
25. Szewczyk A. (red.), *Dylematy cywilizacji informatycznej*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2004;
26. Rosenne S., *The perplexities of modern international law, General Course on Public International Law,* RCADI 2003;
27. Shinder D., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Wydawnictwo HELION, Gliwice 2004;
28. Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne,* Wolters Kluwer Polska, Warszawa 2011;
29. Siwicki M., *Cyberprzetępczość*, Wydawnictwo C.H. Beck, Warszawa 2013;
30. Sobol E. (red.), *Słownik Języka Polskiego,* Wydawnictwo Naukowe PWN, Warszawa 1994;
31. Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzem,* Wolters Kluwer Polska, Warszawa 2010;
32. Szpor G. (red.), *Internet. Ochrona wolności, własności i bezpieczeństwa*, Wydawnictwo C.H. Beck, Warszawa 2011;
33. Kosiński J., *Pradygmaty cyberprzstępczości,* Difin SA, Warszawa 2015;
34. Wąsek A., Zawłocki R. (red.), *Kodeks karny. Część szczególna. Komentarz do artykułów 222-316,* Wydawnictwo C.H. Beck, Warszawa 2010
35. Zoll A. (red.) *Kodeks karny. Część szczególna. Komentarz do artykułów 117- 277 k.k.*, Wolters Kluwer Polska, Warszawa 2013;

ARTYKUŁY

1. Adamski A., *Cyberprzestępczość - aspekty prawne i kryminologiczne* [w:] „Studia

Prawnicze", Zeszyt 4(166) 2005, Wydawnictwo Naukowe Scholar, Warszawa 2006;
2. Gienias K., *Zwalczanie cyberprzestępczości w świetle ort. 296b Kodeksu karnego - problem tzw. hacking tools,* „Prawnik na łączach" 2006, nr 4;
3. Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski - zarys problemu* [w:] „Bezpieczeństwo Narodowe" 2012, nr 22;
4. Gruew G., Kompetencja instytucji Unii Europejskiej do ustanawiania i kształtowania norm prawa karnego, „Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza" 2012, nr 1;
5. Jakubski K. J., *Przestępczość komputerowa - zarys problematyki, „* Prokuratura i prawo" 1996, nr 12;
6. Jaroszewska I. A., *Dostęp do informacji za pośrednictwem Internetu przez osoby nieuprawnione. Studium prawnokarne,* XLIV Międzynarodowe Seminarium Kół Naukowych "Koła Naukowe szkoła twórczego działania", Olsztyn 2015;
7. Karatysz M., *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski* [on-line], „Refleksje. Pismo naukowe studentów i doktorantów WNPiD UAM", nr 7, dostęp: 5.05.2015, http://hdl.handle.net/10593/10524;
8. Kardas P., *Oszustwo komputerowe w kodeksie karnym,* „Przegląd Sądowy" 2000, nr 11-12.
9. Kerr O. S., *The Problem of perspective in Internet law* [on-line], Georgetown Law Journal 2003, Vol. 91, February 2003, dostęp: 19.05.2015, http://papers.ssm.com/sol3/papers.cfm?abstract_id=310020;
10. Kisiel A., *Społeczeństwo Informacyjne - wybrane przykłady szans i zagrożeń,* „Polskie Stowarzyszenie Zarządzania Wiedzą, Seria: Studia i Materiały" 2011, nr 51;
11. Kozłowska P., Kucharska M., *Prawnokarne aspekty pornografii,* „Prokuratura i Prawo" 1999, nr 4;
12. Wójcik J. W., *Cyberprzestępczość. Wybrane zagadnienia kryminologiczne i* prawne, „Problemy Prawa i Administracji" 2011, nr 1, s. 155.
13. Peterson J. H., Segal L., Eonas A., *Global Cyber Intermediary Liability: A Legal & Cultural Strategy,* 34 Pace L. Rev. 586 2014;
14. Sowa M., *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo 2002" nr 4;
15. Wasilewski J., *Zarys definicyjny cyberprzestrzeni* [w:] „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5) [on-line], dostęp: 18.03.2015,

http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa/987,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-9-5- 2013.html;
16. Wrześniewski M., *Krytycznie o przestępstwach pornograficznych*, „Prokuratura i Prawo" 2011, nr 11;

ŹRÓDŁA INTERENTOWE

1. Borkowski P., *Perspektywy cyberbezpieczeństwa Unii Europejskiej* [on-line], Portal Spraw Zagranicznych 2009, dostęp: 4.05.2015, http://www.psz.pl/127-unia-europejska/piotr-borkowski-perspektywy-cyber-bezpieczenstwa-unii- europejskiej;
2. Business Software Alliance, *Czym jest piractwo komputerowe?* [on-line], dostęp: 12.05.2015, http://ww2.bsa.org/country/Anti-Piracy/What-is-Software-Piracyaspx?sc_l ang=pl -PL;
3. CERT.PL, dostęp: 12.05.2015, http://www.cert.pl/o-nas;
4. Cyber [w:] Słownik języka polskiego PWN [on-line], dostęp: 29.04.2015, http://sjp.pwn.pl/szukaj/cyb er. html;
5. Delvy P., *Deuxieme Deluąe* [on-line], „Magazyn Sztuki" 1997, nr 13, dostęp, http://magazynsztuki.eu/old/n_technologia/drugi%20potop.htm;
6. European CyberSecurity Dashboard and 28 Country Reports Launched - 3 March2015 [on-line], dostęp: 4.05.2015, http://www.galexia.com/public/about/news/about_news-id300.html;
7. Fitzgerald B., *Software Piracy: Study Claims 57Percent Of The World Pirates Software* [w:] The Huffington Post [on-line], dostęp: 13.05.2015, http://www.huffingtonpost.com/2012/06/01/software-piracy-study-bsa_n_1563006.html;
8. Gercke M., *Understanding cybercrime: phenomena, challenges and legal response* [on-line], ITU 2012, dostęp: 3.05. 2015, http://www.itu.int/TTU-D/cyb/cybersecurity/docs/Cybercrime%201egislation%20EV6.pdf;
9. GO-Gulf: Cyber Crime Statistic and Trends [Infographic] [on-line], dostęp: 11.05.2015, http://www.go-gulf.com/blog/cyber-crime/;
10. International Federation of the Phonographic Industry: Global Statistics [on- line], dostęp: 12.05.2015, http://www.ifpi.org/global-statistics.php;
11. International Telecommunication Union [on-line], dostęp: 1.05.2015, http://www.itu.int/en/about/Pages/overview.aspx;
12. International Telecommunication Union [on-line], dostęp: 3.05.2015,

http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx;
13. Interpol, *Cybercrime* [online], dostęp: 17.04.2015, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime;
14. Kuczerawy A., *Odpowiedzialność dostawcy usług internetowych* [on-line], Biblioteka Cyfrowa Uniwersytetu Wrocławskiego, dostęp: 6.05.2015, http://www.bibliotekacyfrowa.pl/Content/23625/Odpowiedzialnosci_dostawcy_uslug_intemetowych.pdf;
15. Łydziński D., *Kryptograficzne metody ochrony informacji* [on-line], dostęp: 9.05.2015, http://www.4itsecurity.pl/index.php/kategorie/hacking/62-kryptograficzne-metody-ochrony-informacji;
16. Norton, *Boty i sieci typu „bot" - rosnące zagrożenie* [on-line], dostęp: http://pl.norton.com/botnet;
17. Nowak M., *Cybernetyczne przestępstwa - definicje i przepisy prawne* [on-line], „Biuletyn EBIB" 2010, nr 4, dostęp: 3.02.2015, http://www.ebib.p1/2010/113/a.php7nowak;
18. OECD.org [on-line], dostęp: 4.05.2015, http://www.oecd.org/about/;
19. PINGDOM, *Internet 2012 in numbers* [online], dostęp: 10.04.2015, http//royal.pingdom.com/2013/01/16/intemet-2012-in-number/;
20. F. Randoniewicz, *Odpowiedzialność karana za przestępstwo hackingu* [on- line], dostęp: 21.05.2015, http://www.iws.org.pl/pliki/files/IWS_Radoniewicz_Odp%20za%20przest%20hackingu.pdf;
21. RSA Cybercrime Report: The Current State of Cybercrime 2014. An Inside Look at the Changing Threat Landscape [on-line], dostęp: 5.05.2015, http://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf;
22. Securelist - Information about Viruses, Hackers and Spam, *Oszustwa wykorzystujące portale społecznościowe* [on-line], dostęp: 12.05.2015, http://securelist.pl/analysis/7280,oszustwa_wykorzystujace_portale_spolecznosciowe.html;
23. Symantec: Internet Security Threat Report 2014 [on-line], Volume 19, dostęp: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_intemet_theeat_report_ITU2014pdf;
24. Symantec: Internet Security Threat Report [on-line], Volume 20, April 2015, dostęp: 11.05.2015:

https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-intemet-security-threat-report-volume-20-2015-social_v2.pdf;

25. Worldmapper, *Internet Users 1990, Map No.335* [online], dostęp: 10.04.2015, http://www.worldmapper.org/display.php?selected=335;
26. 2013 Norton Report [on-line], dostęp: 11.05.2015, http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-infographic.en-us.pdf;