ODPOWIEDZIALNOŚĆ KARNA ZA HACKING

I INNE PRZESTĘPSTWA PRZECIWKO DANYM KOMPUTEROWYM I SYSTEMOM INFORMATYCZNYM

Filip Radoniewicz

MONOGRAFIE

Wolters Kluwer

ODPOWIEDZIALNOŚĆ KARNA ZA HACKING

I INNE PRZESTĘPSTWA PRZECIWKO DANYM KOMPUTEROWYM I SYSTEMOM INFORMATYCZNYM

Filip Radoniewicz

MONOGRAFIE

Wolters Kluwer

WARSZAWA 2016

Stan prawny na 15 listopada 2015 r.

Recenzent
Dr hab. Andrzej Adamski, prof. UMK

Wydawca
Monika Pawłowska

Redaktor prowadzący
Adam Choiński

Opracowanie redakcyjne
Katarzyna Paterak-Kondek

Łamanie
Wolters Kluwer

ISBN 978-83-264-9467-3
ISSN 1897-4392
ISBN PDF-a: 978-83-8092-212-9

Wydane przez:
Wolters Kluwer SA

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

Książkę poświęcam żonie Monice,
z podziękowaniem za wsparcie i wyrozumiałość

Spis treści

Wykaz skrótów

Źródła prawa

ACTA	–	Anti-Counterfeiting Trade Agreement (Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi)
CMA	–	Computer Misuse Act 1990 (brytyjska ustawa o nadużyciach komputerowych z 1990 r.)
Code Pénal	–	francuski kodeks karny z 1992 r.
d. TUE	–	Traktat o Unii Europejskiej podpisany w Maastricht dnia 7 lutego 1992 r., w brzmieniu sprzed wejścia w życie Traktatu z Lizbony (wersja skonsolidowana uwzględniająca traktaty akcesyjne, które weszły w życie w dniu 1 maja 2004 r. i 1 stycznia 2007 r.: Dz. Urz. UE C 321E z 29.12.2006 r., s. 5)
decyzja ramowa 2002/584 w sprawie ENA	–	decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (Dz. Urz. WE L 190 z 18.07.2002 r., s. 1)
decyzja ramowa 2005/222	–	decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE L 69 z 16.03.2005 r., s. 67)
decyzja ramowa 2008/841	–	decyzja ramowa Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej (Dz. Urz. UE L 300 z 11.11.2008 r., s. 42)

dyrektywa 2013/40	–	dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastepująca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218 z 14.08.2013 r., s. 8)
dyrektywa o handlu elektronicznym	–	dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz. Urz. WE L 178 z 17.07.2000 r., s. 1)
dyrektywa o prywatności i łączności elektronicznej	–	dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. WE L 201 z 31.07.2002 r., s. 37)
dyrektywa ramowa	–	dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz. Urz. WE L 108 z 24.04.2002 r., s. 33)
EKPCz	–	Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.)
k.c.	–	ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn.: Dz. U. z 2014 r. poz. 121 z późn. zm.)
k.k.	–	ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.)
Konwencja o cyberprzestępczości	–	Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728)

k.p.k.	–	ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.)
k.w.	–	ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (tekst jedn.: Dz. U. z 2015 r. poz. 1094 z późn. zm.)
MPPOiP	–	Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167)
nowelizacja z 2004 r.	–	ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. Nr 69, poz. 626)
nowelizacja z 2008 r.	–	ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344)
pr. tel.	–	ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tekst jedn.: Dz. U. z 2014 r. poz. 243 z późn. zm.)
Protokół dodatkowy do Konwencji o cyberprzestępczości	–	Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu dnia 28 stycznia 2003 r. (Dz. U. z 2015 r. poz. 730)
RIPA	–	Regulation of Investigatory Powers Act 2000 (brytyjska ustawa o uregulowaniu środków śledczych z 2000 r.)
rozporządzenie 460/2004	–	rozporządzenie (WE) nr 460/2004/WE Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz. Urz. UE L 77 z 13.03.2004 r., s. 1.)
r.z.t.p.	–	rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. Nr 100, poz. 908 z późn. zm.)
StGB	–	niemiecki kodeks karny (Strafgesetzbuch) z 1871 r. w wersji opublikowanej w dniu 13 listopada 1998 r. (BGBl. I S. 3322)

TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 326 z 26.10.2012 r., s. 47, z późn. zm.)
Traktat Konstytucyjny	–	Traktat ustanawiający Konstytucję dla Europy (Wspólnoty Europejskiej) podpisany w Rzymie dnia 29 października 2004 r. (Dz. Urz. UE C 310 z 16.12.2004 r., s. 1)
Traktat z Amsterdamu	–	Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie oraz niektóre związane z nimi akty podpisany w Amsterdamie dnia 2 października 1997 r. (Dz. Urz. WE C 340 z 10.11.1997 r., s. 1)
Traktat z Lizbony	–	Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie dnia 13 grudnia 2007 r. (Dz. Urz. UE C 306 z 17.12.2007 r., s. 1)
Traktat z Maastricht	–	Traktat o Unii Europejskiej podpisany w Maastricht dnia 7 lutego 1992 r. (w brzmieniu pierwotnym) (Dz. Urz. WE C 191 z 29.07.1992 r., s. 1)
Traktat z Nicei	–	Traktat z Nicei zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie oraz niektóre związane z nimi akty prawne podpisany w Nicei dnia 26 lutego 2001 r. (Dz. Urz. WE C 80 z 10.3.2001 r., s. 1)
TUE	–	Traktat o Unii Europejskiej podpisany w Maastricht dnia 7 lutego 1992 r. (wersja skonsolidowana Dz. Urz. UE C 326 z 26.10.2012 r., s. 13, z późn. zm.)
TWE	–	Traktat ustanawiający Wspólnotę Europejską z 25 marca 1957 r. (w brzmieniu bezpośrednio sprzed wejścia w życie Traktatu z Lizbony) (wersja skonsolidowana uwzględniająca traktaty akcesyjne, które weszły w życie w dniu 1 maja 2004 r. i 1 stycznia 2007 r., Dz. Urz. UE C 321E z 29.12.2006 r., s. 37)
u.i.d.p.p.	–	ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn.: Dz. U. z 2014 r. poz. 1114)

u.o.d.o.	–	ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2015 r. poz. 1309 z późn. zm.)
USC	–	The Code of Laws of the United States of America (United States Code) (skodyfikowany zbiór prawa federalnego obowiązującego w Stanach Zjednoczonych Ameryki)
u.ś.u.d.e.	–	ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn.: Dz. U. z 2013 r. poz. 1422 z późn. zm.)
u.z.n.k.	–	ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jedn.: Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.)
zalecenie (89) 9	–	zalecenie Komitetu Ministrów Rady Europy nr R (89) 9 z dnia 13 września 1989 r. w sprawie przestępstw komputerowych
zalecenie (92) 188	–	zalecenie Rady OECD C (92) 188 z dnia 26 listopada 1992 r. dotyczące wytycznych w zakresie bezpieczeństwa systemów informatycznych
zalecenie (2002) 131	–	zalecenie Rady OECD C (2002) 131 z dnia 25 lipca 2002 r. w sprawie wytycznych w zakresie bezpieczeństwa systemów i sieci informatycznych: w kierunku kultury bezpieczeństwa

Publikatory, czasopisma, zbiory orzecznictwa

BGBl.	–	Dziennik Urzędowy Republiki Federalnej Niemiec
CzPKiNP	–	Czasopismo Prawa Karnego i Nauk Penalnych
Dz. U.	–	Dziennik Ustaw
Dz. Urz. UE	–	Dziennik Urzędowy Unii Europejskiej
Dz. Urz. WE	–	Dziennik Urzędowy Wspólnot Europejskich
e-Biuletyn CBKE	–	e-Biuletyn Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Wydział Prawa, Administracji i Ekonomii, Uniwersytet Wrocławski
EP	–	Edukacja Prawnicza

EPS	–	Europejski Przegląd Sądowy
M. Praw.	–	Monitor Prawniczy
OSNKW	–	Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSNwSK	–	Orzecznictwo Sądu Najwyższego w Sprawach Karnych
OSP	–	Orzecznictwo Sądów Polskich
OTK	–	Orzecznictwo Trybunału Konstytucyjnego
OTK-A	–	Orzecznictwo Trybunału Konstytucyjnego, Zbiór Urzędowy, seria A
PiP	–	Państwo i Prawo
Prok. i Pr.	–	Prokuratura i Prawo
PS	–	Przegląd Sądowy
St. Praw.	–	Studia Prawnicze
WPP	–	Wojskowy Przegląd Prawniczy

Organizacje, instytucje, sądy i trybunały

AIDP/AIPL	–	Międzynarodowe Stowarzyszenie Prawa Karnego
ARPA	–	Agencja Zaawansowanych Projektów Badawczych (Advanced Research Project Agency)
CDPC	–	Europejski Komitet ds. Przestępczości (European Committee on Crime Problems)
CERN	–	Europejska Organizacja Badań Jądrowych
DARPA	–	Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (Defence Advanced Research Project Agency)
ECOSOC	–	Rada Gospodarcza i Społeczna ONZ
EFF	–	Electronic Frontier Foundation
EKES	–	Europejski Komitet Ekonomiczno-Społeczny
ETPCz	–	Europejski Trybunał Praw Człowieka
ETS	–	Europejski Trybunał Sprawiedliwości (od 1 grudnia 2009 r. Trybunał Sprawiedliwości Unii Europejskiej)
Eurojust	–	Europejska Sieć Sądowa
Europol	–	Europejski Urząd Policji
EWG	–	Europejska Wspólnota Gospodarcza

EWI	–	EastWest Institute
ICCP	–	Komitet ds. Polityki Informatyzacji, Komputeryzacji i Telekomunikacji (Committee on Information, Communications and Computer Policy – ICCP Committee)
Interpol	–	Międzynarodowa Organizacja Policji Kryminalnych
ISO	–	Międzynarodowa Organizacja Standaryzacyjna (ang. International Organization for Standarization, fr. Organisation internationale de normalisation)
ITU	–	Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union)
NSA	–	Naczelny Sąd Administracyjny
OECD	–	Organizacja Współpracy Gospodarczej i Rozwoju (ang. Organization for Economic Co-operation and Development)
SA	–	Sąd Apelacyjny
SN	–	Sąd Najwyższy
TK	–	Trybunał Konstytucyjny
UE	–	Unia Europejska
WE	–	Wspólnota Europejska

Inne

AS	–	system autonomiczny (Autonomous System)
CERT	–	zespół ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego (Computer Emergency Response Team)
DDoS	–	rozproszona odmowa usługi (distributed denial of service)
DoS	–	odmowa usługi (denial of service)
Explanatory Report	–	Komentarz do Konwencji o cyberprzestępczości (Explanatory Report to Convention on Cybercrime)
GCA	–	Global Cybersecurity Agenda (Globalna Agenda na rzecz Cyberbezpieczeństwa)

HLEG	–	High-level expert group (grupa ekspertów wysokiego szczebla ds. spraw cyberbezpieczeństwa, powołana w ramach ITU)
INGOs	–	międzynarodowe organizacje pozarządowe (International Non-Governmental Organizatons)
ITU Toolkit	–	ITU Toolkit for Cybercrime Legislation
LEX	–	system informacji prawnej LEX
p2p	–	sieci peer-to-peer
PWBiS	–	Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości
Raport OECD	–	Computer-Related Crime. Analysis of legal policy in the OECD Area, ICCP Series nr 10, OECD, Paris 1986
WAP	–	Wireless Application Protocol
WPZiB	–	Wspólna Polityka Zagraniczna i Bezpieczeństwa
WSiSW	–	Wymiar Sprawiedliwości i Sprawy Wewnętrzne

Wstęp

Od początku ubiegłego wieku mamy do czynienia z rozwojem techniki na niespotykaną wcześniej skalę. Jej gałęzią, która ostatnimi czasy rozwija się najprężniej, jest wkraczająca we wszystkie dziedziny życia szeroko rozumiana technologia informatyczna, a w szczególności teleinformatyka. Dzieje się tak przede wszystkim w związku z postępującą w ostatnich latach konwergencją informatyki i telekomunikacji, będącą następstwem rozwoju sieci komputerowych oraz Internetu, wymuszającego konieczność zapewnienia szybkiego i efektywnego przetwarzania oraz przekazywania informacji, której rola niepomiernie wzrosła. Stała się ona nie tylko towarem, zyskując ogromne znaczenie ekonomiczne, ale także istotnym instrumentem w dziedzinie polityki i sprawowania władzy. Coraz częściej w związku z tym można spotkać się ze stwierdzeniem, że żyjemy w społeczeństwie „rewolucji informacyjnej", „informacyjnym", a nawet „informatycznym"[1].

Oczywiście, proces ten, poza niewątpliwymi korzyściami, niesie za sobą także zagrożenia. Janusz Barta i Ryszard Markiewicz porównują Internet do Dzikiego Zachodu, jako terenu, „gdzie prawa nie ma lub trudno je egzekwować"[2]. Nie ulega wątpliwości, że skonstruowanie regulacji zapewniającej bezpieczeństwo przepływu informacji stanowi nie lada wyzwanie dla tworzących prawo. Wyzwanie, co należy podkreślić, któremu ustawodawcom niełatwo podołać.

Tematem niniejszego opracowania jest odpowiedzialność karna za przestępstwo hackingu. Już na samym wstępie należy poczynić istotną

[1] Zob. P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, CzPKiNP 2000, nr 1, s. 25–30; R. Skubisz, *Internet – ku społeczeństwu przyszłości* (w:) *Internet 2000. Prawo – ekonomia – kultura*, Lublin 1999, s. 9–12.

[2] J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 9.

uwagę natury terminologicznej, dotyczącą rozumienia tego pojęcia. Kwestia ta zostanie omówiona obszerniej w rozdziale pierwszym, stanowiącym wprowadzenie do problematyki przestępczości komputerowej. W tym miejscu zasygnalizować jedynie należy, że obecnie termin ten rozumiany jest nieco szerzej, niż pierwotnie. Początkowo pojmowany był jako uzyskiwanie nielegalnego dostępu do zasobów komputerów lub sieci komputerowych. „Współczesne" rozumienie tego terminu jest szersze, obejmuje wszelkie działania mające na celu zakłócenie funkcjonowania sieci, a więc zachowania stanowiące przestępstwa przeciwko bezpieczeństwu informacji we wszystkich jego aspektach (integralności, poufności i dostępności)[3].

Problematyka przestępstw komputerowych przeciwko bezpieczeństwu informacji, mimo swojego wzrastającego znaczenia, nie cieszy się należytym zainteresowaniem doktryny. Zjawisko to w zasadzie nie doczekało się również badań empirycznych[4], stąd jego rzeczywista skala w Polsce nie była znana. Nawet analiza danych pochodzących z oficjalnych statystyk przestępczości ujawnionej (statystyka policyjna), których przedmiotem były przestępstwa stypizowane w art. 267–269b ustawy z dnia

[3] Na marginesie warto zauważyć, iż zwykle w piśmiennictwie dla określenia sprawców przestępstw komputerowych, godzących w funkcjonowanie sieci komputerowych, używa się pojęcia „hackerzy". Postępują tak nawet ci autorzy, którzy starają się przestrzegać wskazanej wyżej konwencji językowej i pod pojęciem hackingu rozumieją jedynie uzyskanie nielegalnego dostępu do systemu komputerowego (czy sieci komputerowej) lub danych komputerowych (zob. S.W. Brenner (w:) R.D. Clifford (red.), *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime,* Durham 2011, s. 18; J. Erickson, *Hacking. Sztuka penetracji*, Gliwice 2004, s. 9–13; D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci,* Gliwice 2005, s. 301; U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, Przegląd Policyjny 1995, nr 3, s. 12; M. Siwicki, *Cyberprzestępczość*, Warszawa 2013. s. 158).

[4] Badania z tego zakresu przeprowadzili A. Adamski (*Nadużycia komputerowe w Polsce w świetle wstępnych wyników badań wiktymizacyjnych* (w:) A. Adamski (red.), *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej, Poznań, 20–22 IV 1994*, Toruń 1994, s. 33–52) oraz R.A. Stefański (*Przestępstwa internetowe w Polsce. Analiza praktyki*, St. Praw. 2005, z. 4, s. 121–128). Jednak przedmiotem badań A. Adamskiego była wiktymizacja (opierały się na analizie ankiet wypełnionych przez pokrzywdzonych) i przeprowadzone zostały w pierwszej połowie lat 90., a więc w okresie, gdy technologia informatyczna, a w związku z tym przestępczość komputerowa, jeszcze „raczkowały". Natomiast badania przeprowadzone przez R.A. Stefańskiego opierały się na analizie 619 wyselekcjonowanych akt spraw zarejestrowanych w latach 2001–2002, których przedmiotem była bardzo zróżnicowana grupa przestępstw („przestępstwa internetowe"), a co za tym idzie – przestępstwa przeciwko bezpieczeństwu danych komputerowych oraz systemów informatycznych stanowiły znikomy ich odsetek (23 sprawy, tj. niespełna 4%).

6 czerwca 1997 r. – Kodeks karny[5], okazała się mało miarodajna (zob. rozdział siódmy).

W związku z powyższym celem niniejszego opracowania była w pierwszej kolejności analiza przepisów art. 267–269b k.k., w których dokonano kryminalizacji przestępstw komputerowych przeciwko bezpieczeństwu informacji, z uwzględnieniem regulacji międzynarodowych i unijnych oraz rozwiązań obowiązujących w wybranych krajach europejskich. Jednocześnie stanowi ono próbę skonfrontowania polskich rozwiązań z wynikami badań empirycznych o zasięgu ogólnokrajowym, których przedmiotem była problematyka odpowiedzialności karnej za przestępstwo hackingu.

Niniejsza monografia składa się ze wstępu, siedmiu rozdziałów i zakończenia. Dwa pierwsze rozdziały mają charakter wprowadzający do omawianej problematyki, rozdział pierwszy jest ogólnym wprowadzeniem do tematyki hackingu, następne pięć ma charakter dogmatyczny, natomiast rozdział ostatni prezentuje wyniki badań empirycznych.

Rozdział pierwszy, poza krótkim przedstawieniem historii sieci komputerowych oraz Internetu i jego ogólnej charakterystyki, zawiera podstawowe informacje mające przybliżyć zasady funkcjonowania sieci komputerowych, jak również zwięzłe omówienie technicznej strony przestępczości komputerowej, czyli metod stosowanych przez przestępców, zwanych potocznie hackerami.

O ile celem rozdziału pierwszego jest ogólne wprowadzenie do tematyki hackingu poprzez przedstawienie podstawowych informacji na temat tego zjawiska oraz omówienie jego technicznych aspektów, o tyle rozdział drugi stanowi niejako właściwy wstęp do niniejszego opracowania. Przedstawione w nim zostały próby zdefiniowania przestępstw komputerowych i ich klasyfikacji, historia kryminalizacji tego zjawiska wraz z wiążącymi się z tym trudnościami oraz wyjaśnienie podstawowych pojęć: informacji, danych komputerowych oraz programu komputerowego.

W rozdziale trzecim omówione zostały najistotniejsze inicjatywy międzynarodowe, których przedmiotem jest przestępczość komputerowa. Ich cechą charakterystyczną jest to, że mają charakter niewiążący. Wyjątek stanowi Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.[6], na którą został położony w związ-

[5] Dz. U. Nr 88, poz. 553 z późn. zm.
[6] Dz. U. z 2015 r. poz. 728.

ku z tym szczególny nacisk. Poza tym aktem zostały zaprezentowane inne dokumenty oraz inicjatywy podejmowane przez organizacje międzynarodowe, zarówno rządowe (Organizacja Narodów Zjednoczonych, Międzynarodowy Związek Telekomunikacyjny, Organizacja Współpracy Gospodarczej i Rozwoju, Rada Europy, Grupa G7/G8), jak i pozarządowe (Międzynarodowa Organizacja Policji Kryminalnych, Międzynarodowe Stowarzyszenie Prawa Karnego, EastWest Institute).

Działaniom Unii Europejskiej w zakresie zwalczania hackingu poświęcony został rozdział czwarty. Rozwiązanie takie było podyktowane odrębnością porządku prawnego Unii Europejskiej od prawa międzynarodowego oraz krajowego[7]. Omówione zostały przede wszystkim decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[8] oraz – zastępująca ją – dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW[9].

Rozdział piąty poświęcony jest polskiej regulacji karnej i zawiera omówienie znamion przestępstw komputerowych zawartych w rozdziale XXXIII kodeksu karnego:

1) uzyskania nieuprawnionego dostępu do informacji (art. 267 § 1 k.k.);
2) uzyskania nieuprawnionego dostępu do całości systemu informatycznego lub jego części (art. 267 § 2 k.k.);
3) nielegalnego podsłuchu i inwigilacji za pomocą urządzeń technicznych i programów komputerowych (art. 267 § 3 k.k.);
4) ujawnienia informacji uzyskanej nielegalnie (art. 267 § 4 k.k.);
5) naruszenia integralności zapisu informacji (art. 268 § 2 i 3 k.k.);
6) naruszenia integralności danych informatycznych, utrudniania dostępu do nich oraz zakłócania ich przetwarzania (art. 268a § 1 i 2 k.k.);
7) sabotażu informatycznego (art. 269 § 1 k.k.);

[7] Wyroki ETS z dnia: 5 lutego 1963 r. w sprawie *NV Algemene Transport en Expeditie Onderneming van Gend and Loos przeciwko Holenderskiej administracji celnej* (26/62) oraz 15 lipca 1964 r. w sprawie *Flaminio Costa przeciwko E.N.E.L.* (6/64). Zob. szerzej np. J. Barcz, *Charakter prawny i struktura Unii Europejskiej. Pojęcie prawa UE* (w:) J. Barcz (red.), *Prawo Unii Europejskiej. Zagadnienia systemowe*, Warszawa 2006, s. 28; S. Biernat, *Prawo Unii Europejskiej a prawo państw członkowskich* (w:) J. Barcz (red.), *Prawo Unii...*, s. 253–254; A. Zawidzka-Łojek, *Prawo Unii Europejskiej a prawo krajowe państw członkowskich* (w:) J. Barcz (red.), *Źródła prawa Unii Europejskiej*, Warszawa 2012, s. 146–147.

[8] Dz. Urz. UE L 69 z 16.03.2005 r., s. 67.

[9] Dz. Urz. UE L 218 z 14.08.2013 r., s. 8.

8) zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej (art. 269a k.k.);
9) tzw. bezprawnego wykorzystania urządzeń, programów i danych (art. 269b § 1 k.k.).

Analiza obejmuje kolejno znamiona przedmiotu ochrony, strony przedmiotowej, podmiotu, strony podmiotowej każdego z nich. Przyjęcie takiego układu treści (niejako komentarzowego) podyktowane zostało potrzebą zachowania odpowiedniej przejrzystości. Ta ostatnia uwaga odnosi się również do sposobu zaprezentowania problematyki zbiegu przepisów, zbiegu przestępstw, wymiaru kary oraz trybu ścigania omówionych w odrębnych podrozdziałach, wspólnych dla wszystkich analizowanych przestępstw.

W rozdziale szóstym zaprezentowano unormowania dotyczące przestępstw komputerowych obowiązujące w wybranych państwach europejskich. Celem opracowania było wyróżnienie pewnych modeli kryminalizacji tego zjawiska oraz przedstawienie wybranych krajowych unormowań, które z jednej strony byłyby typowe dla tychże modeli, a z drugiej – zawierałyby pewne odmienności czy oryginalne rozwiązania. Umieszczenie tego rozdziału w tym właśnie miejscu, a więc po rozdziale poświęconym polskiej regulacji, powinno dać czytelnikowi maksymalnie przejrzysty obraz omawianego tematu.

W ostatnim rozdziale zaprezentowano wyniki badań empirycznych opartych na analizie akt 1163 postępowań przygotowawczych zarejestrowanych w jednostkach organizacyjnych prokuratury całego kraju w latach 2009–2010. Celem badań było dokonanie oceny skali zjawiska hackingu w Polsce, jak również przyjmowanych kwalifikacji prawnych, sposobów zakończenia wszczętych postępowań oraz przyczyn odmowy ich wszczęcia, a także rodzaju i wysokości orzekanych kar i środków karnych.

Niniejsza monografia stanowi zmodyfikowaną i uaktualnioną wersję rozprawy doktorskiej obronionej przeze mnie w dniu 9 grudnia 2014 r. na Wydziale Prawa i Administracji Uniwersytetu Marii Curie-Skłodowskiej w Lublinie. Wybór jej tematu podyktowany był przede wszystkim moimi zainteresowaniami. Wyzwanie stanowiła także stosunkowa nowość problematyki przestępstw komputerowych, ograniczona liczba publikacji po-

święconych omawianym zagadnieniom, a wreszcie brak badań empirycznych, a nawet opracowań statystycznych[10].

W tym miejscu pragnę podziękować osobom, które miały niewątpliwy wpływ na ostateczny kształt pracy. Przede wszystkim Promotorowi – Panu prof. dr. hab. Markowi Mozgawie za sprawowaną opiekę merytoryczną oraz Recenzentom – Panu prof. dr. hab. Piotrowi Kardasowi oraz Panu prof. dr. hab. Jackowi Sobczakowi za cenne uwagi, a także Panu prof. dr. hab. Andrzejowi Siemaszce, wieloletniemu Dyrektorowi Instytutu Wymiaru Sprawiedliwości, który umożliwił mi przeprowadzenie badań empirycznych stanowiących niezwykle istotny element niniejszego opracowania.

Dziękuję również za przekazane uwagi i słowa zachęty autorowi recenzji wydawniczej Panu prof. dr. hab. Andrzejowi Adamskiemu.

[10] Z danych zgromadzonych przez organy Policji, umieszczonych na stronie Komendy Głównej Policji, trudno wyciągnąć miarodajne wnioski (zob. uwagi na ten temat w rozdziale ostatnim).

Rozdział 1
Hacking – zagadnienia ogólne

1.1. Uwagi wstępne

1.1.1. Zarys historii komputerów i sieci komputerowych

Gwałtowny rozwój sieci komputerowych, którego jednym z najważniejszych aspektów jest powstanie Internetu, miał miejsce w ciągu ostatnich 30 lat. Początkowo trudno było bowiem sobie wyobrazić, że postęp techniczny stanie się aż tak intensywny. Pierwszy komputer powstał już w latach 40. ubiegłego wieku w Stanach Zjednoczonych. Zajmował on 139 m^2, używał 17 tysięcy lamp próżniowych i wykonywał 1000 obliczeń na sekundę (dla porównania – obecnie przeciętny komputer osobisty wykonuje w ciągu sekundy kilkaset milionów operacji). Pierwszym „komercyjnym komputerem" był UNIVAC (*Universal Automatic Computer*) skonstruowany w 1951 r.[11] Na zakup komputerów produkowanych w latach 50. i 60. mogły sobie pozwolić instytucje rządowe oraz uczelnie. Przełom nastąpił w latach 70., kiedy na rynku pojawił się Altair 8800 dostępny dla przeciętnego obywatela w Stanach Zjednoczonych[12]. Następnie pojawiły się Atari, Commodore 64 i IBM PC. W latach 70. powstały też pierwsze sieci. Składały się one z głównego komputera (ang. *mainframe*) oraz połączonych z nim terminali, które korzystały z plików, programów i mocy obliczeniowej komputera *mainframe*. Bez niego były bezużyteczne. Wraz z pojawieniem się stosunkowo tanich komputerów osobistych zaistniała

[11] Szerzej B. Gates, *Droga ku przyszłości*, Warszawa 1997, s. 1–72. Por. R. Skubisz, *Internet – ku społeczeństwu przyszłości* (w:) R. Skubisz (red.), *Internet 2000*, Lublin 1999, s. 7–9; J.W. Wójcik, *Przestępstwa komputerowe*, cz. 1, *Fenomen cywilizacji*, Warszawa 1999, s. 12–14.

[12] B. Gates, *Droga...*, s. 17.

możliwość wyposażenia każdego pracownika w taki właśnie sprzęt, a nie tylko terminal. Jednocześnie jednak użytkownicy stracili możliwość korzystania z zasobów komputera głównego, a dane między sobą mogli wymieniać za pomocą fizycznych nośników (tzw. poczta *per pedes*). W celu rozwiązania tego problemu pod koniec lat 70. stworzono standard Ethernet umożliwiający łączenie ze sobą komputerów osobistych w sieć lokalną LAN (ang. *Local Area Network*). Obecnie jest to najpopularniejsza technologia stosowana w sieciach komputerowych[13].

W tym samym czasie zaczęły powstawać tzw. BBS-y[14], czyli sieci powstałe z komputerów połączonych ze sobą przy pomocy modemów i linii telefonicznych; rozwijał się też już ARPANet – „poprzednik" Internetu.

W 1957 r. w Stanach Zjednoczonych, w ramach Departamentu Obrony, powstała Agencja Zaawansowanych Projektów Badawczych (Advanced Research Project Agency)[15]. Pierwotnym celem ARPA była budowa sztucznego satelity. Szybko jednak Agencja zajęła się pracami nad rozwojem nowoczesnych technologii. Jednym z głównych zadań stało się utworzenie sieci komputerowej mającej połączyć uniwersytety i instytucje rządowe. Podstawowym założeniem, jakie przyświecało jej twórcom, było nadanie jej rozproszonego charakteru – skonstruowanie jej bez żadnego centralnego punktu, by nawet w przypadku zniszczenia lub uszkodzenia fragmentu jej struktury, pozostała część mogła funkcjonować. W związku z tym dane nią przekazywane miały być dzielone na pakiety i przesyłane niezależnie,

[13] D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004, s. 70–71.

[14] Najprostszy BBS to po prostu zwykły komputer osobisty, na którym zainstalowano odpowiednie oprogramowanie. Jego użytkownik udostępniał zasoby, umożliwiając korzystanie np. z poczty elektronicznej, grup dyskusyjnych, gier czy wymianę plików. Aby móc skorzystać z danego BBS-u, należało znać jego numer telefonu i po prostu „zadzwonić". Większość BBS-ów posiadała możliwość komunikowania się z innymi BBS-ami, co umożliwiało wymianę poczty i plików w skali świata. Bardzo szybko BBS-y zaczęły być używane do nielegalnych celów – udostępniano sobie programy hackerskie, rozpowszechniano pirackie oprogramowanie (głównie gry) oraz pornografię. Przykładowo – jak podaje A. Walczak-Żochowska – pierwszy serwis poświęcony w całości pornografii dziecięcej powstał już w 1982 r. (A. Walczak-Żochowska, *Internet a seksualne wykorzystywanie dzieci* (w:) P. Girdwoyń (red.), *Prawo wobec nowoczesnych technologii,* Warszawa 2008, s. 110). W czasach największego rozwoju liczba BBS-ów w samych Stanach Zjednoczonych wynosiła ponad 40.000. Obecnie ich znaczenie spadło praktycznie do zera, gdyż dostęp do Internetu stał się znacznie tańszy przy nieporównywalnie większych możliwościach. Por. P. Grabosky, R. Smith, *Crime in the Digital Age*: *Controlling Telecommunications and Cyberspace Illegalities*, Sydney 1998, s. 5–6; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 72.

[15] Od 1972 r. Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (Defence Advanced Research Project Agency).

nawet różnymi trasami, a po dotarciu do celu – składane w oparciu o informacje zawarte w ich nagłówkach (tzw. komutacja pakietów, ang. *packet switching*). Efektem podjętych prac był powstały w 1969 r. ARPANet[16].

W latach 70. pojawiła się poczta elektroniczna, pierwowzór dzisiejszego FTP (ang. *File Transfer Protocol* – protokół transferu plików), grupy dyskusyjne oraz gry dla wielu użytkowników. Cały czas jednak ARPANet ograniczał się zasięgiem do uczelni i instytucji rządowych. Na początku lat 80. do ARPANetu było podłączonych 5000 hostów[17], pod koniec dekady natomiast liczba ta wzrosła do 28.000. Niezwykle ważnym wydarzeniem na drodze budowania sieci otwartej (ang. *open-architecture network environment*) i zacierania granic między różnymi sieciami (proces ten nazywano *internetting*[18])[19] było uznanie w 1982 r. opracowanego w latach 70. protokołu TCP/IP[20] za wiodący standard w funkcjonowaniu sieci. W 1983 r. ARPANet został podzielony na dwie części – Milnet (sieć wojskowa) i NSFNet (sieć cywilna), z której wykształcił się dzisiejszy Internet. W 1987 r. powstał DNS (ang. *Domain Name System* – system nazw domen), który jest protokołem, usługą i siecią serwerów służących zamianie mnemonicznych nazw urządzeń sieciowych (zarówno serwerów, jak i pojedynczych komputerów) na adresy IP zrozumiałe dla urządzeń, które tworzą sieć (np. www.sejm.gov.pl na 194.41.12.17).

W 1992 r. zaczęła funkcjonować usługa *World Wide Web* (WWW). Dzięki zastosowaniu tzw. hiperlinków uczyniła ona Internet znacznie dostępniejszym, umożliwiając korzystanie z niego osobom nieposiadającym fachowych umiejętności. Czynnikiem dodatkowo ułatwiającym „surfowanie" było pojawienie się przeglądarek internetowych. Pierwszą był opracowany w 1993 r. Mosaic. Internet liczył wówczas już ponad milion hostów[21].

---

[16] P. Dawidziuk, B. Łącki, M.P. Stolarski, *Sieć Internet – znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa* (w:) M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 42–43; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 74–76.

[17] Termin ten można spotkać w dwóch znaczeniach – komputer nadrzędny, udostępniający swoje zasoby innym (czyli serwer), albo po prostu urządzenie podłączone do sieci, posiadające numer IP (np. pojedynczy komputer).

[18] Słowo „Internet" po raz pierwszy zostało użyte w 1974 r. przez V. Cerfa i B. Kahna w sporządzonym przez nich opracowaniu badawczym *A Protocol for Packet Network Interconnection*, dotyczącym protokołu TCP (D.J. Bem, *Tylko IP* (w:) D.J. Bem (red.), *Internet 2006*, Wrocław 2007, s. 7).

[19] K. Dobrzeniecki, *Lex Informatica*, Toruń 2008, s. 36.

[20] Protokoły sieciowe są to zbiory reguł określających sposoby komunikowania się w sieci. Zob. szerzej pkt 1.2.6.

[21] P. Dawidziuk, B. Łącki, M.P. Stolarski, *Sieć Internet...*, s. 42–43.

Filip Radoniewicz – doktor nauk prawnych, odbył aplikację radcowską zakończoną złożeniem egzaminu zawodowego; absolwent podyplomowych studiów: prawa Unii Europejskiej na Uniwersytecie Jagiellońskim, praw i wolności człowieka, współorganizowanych przez Instytut Nauk Prawnych PAN i Helsińską Fundację Praw Człowieka, oraz administrowania sieciami komputerowymi na Politechnice Lubelskiej; autor lub współautor około trzydziestu publikacji, przede wszystkim z zakresu szeroko rozumianego prawa karnego, prawa nowych technologii oraz praw człowieka.

Monografia, zważywszy na kompleksowe ujęcie omówionych problemów, stanowi pierwsze w polskiej nauce prawa karnego materialnego tak wyczerpujące opracowanie tematyki przestępstw przeciwko systemom informatycznym i danym komputerowym.

Publikacja zawiera:
- przydatną dla praktyki prezentację wyników badań empirycznych, obejmującą m.in. ocenę zapadłych w badanych postępowaniach decyzji procesowych i stosowanej kwalifikacji prawnej,
- analizę przepisów kodeksu karnego, regulacji międzynarodowych i unijnych oraz zagadnień prawnoporównawczych.

Autor uzupełnia rozważania przystępnym wyjaśnieniem podstaw funkcjonowania współczesnych systemów informatycznych oraz technicznych zagadnień związanych z popełnianiem przestępstw komputerowych przeciwko bezpieczeństwu informacji (czyli szeroko rozumianego hackingu).

Książka jest skierowana do przedstawicieli zawodów prawniczych, w szczególności prokuratorów, sędziów, radców prawnych i adwokatów, a także do pracowników organów ścigania. Będzie również przydatna dla osób zajmujących się teorią prawa oraz biorących udział w procesie jego tworzenia.

9788326494673 W01P01

ISSN 1897-4392
ISBN 978-83-264-9467-3
9 788326 494673

CENA 129 ZŁ (W TYM 5% VAT)