CYBERPRZESTRZEŃ A PRAWO MIĘDZYNARODOWE

Joanna Worona

Wolters Kluwer

CYBERPRZESTRZEŃ A PRAWO MIĘDZYNARODOWE

Status quo i perspektywy

Joanna Worona

Zamów książkę w księgarni internetowej
profinfo.pl
księgarnia internetowa

Wolters Kluwer

WARSZAWA 2020

SERIA **MONOGRAFIE**

Stan prawny na 7 stycznia 2020 r.

Publikacja została dofinansowana przez Kancelarię
Gardocki i Partnerzy Adwokaci i Radcowie Prawni spółka partnerska
ul. Śmiała 26, 01-523 Warszawa

Recenzent
Dr hab. Maciej Rogalski, prof. Uczelni Łazarskiego w Warszawie

Wydawca
Joanna Dzwonnik

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne i łamanie
Violet Design Wioletta Kowalska

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

prawolubni

SZANUJMY PRAWO I WŁASNOŚĆ
Więcej na **www.legalnakultura.pl**
Polska Izba Książki

© Copyright by
Wolters Kluwer Polska Sp. z o.o., 2020

ISBN 978-83-8187-025-2
ISSN 1897-4392

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

SPIS TREŚCI

WYKAZ SKRÓTÓW 11

WSTĘP 19

CZĘŚĆ I
CYBERPRZESTRZEŃ A JURYSDYKCJA

ROZDZIAŁ 1
CYBERPRZESTRZEŃ – POJĘCIE I GENEZA 27
1.1. Pojęcie cyberprzestrzeni 28
1.2. Geneza i ewolucja cyberprzestrzeni 32
1.2.1. Historia powstania Internetu 33
1.2.1.1. ARPANET 33
1.2.1.2. Komercjalizacja Internetu 38
1.2.1.3. System domen internetowych 39
1.2.2. Internet na początku XXI wieku 40
1.3. Etapy rozwoju społeczeństwa informacyjnego 42
1.4. Zagrożenie w cyberprzestrzeni 49
1.4.1. Zagadnienia ogólne 49
1.4.2. Walka informacyjna 52
Podsumowanie 57

ROZDZIAŁ 2
JURYSDYKCJA PAŃSTWOWA A CYBERPRZESTRZEŃ 58
2.1. Jurysdykcja jako pojęcie prawa – istota 59
2.1.1. Obszary jurysdykcji 63
2.1.2. Jurysdykcja cywilna 64
2.1.2.1. Zasady jurysdykcji cywilnej 65
2.1.2.2. Regulacje globalne 68
2.1.2.2.1. Konwencja wiedeńska z 1980 r. 69
2.1.2.2.2. Konwencja lugańska z 2007 r. 69
2.1.2.3. Regulacje regionalne na przykładzie Unii Europejskiej 73
2.1.2.3.1. Rozporządzenie Rzym I 73
2.1.2.3.2. Rozporządzenie Rzym II 77
2.1.2.3.3. Rozporządzenie nr 1215/2012 78

2.1.2.4. Jurysdykcja cywilna w cyberprzestrzeni w aspekcie prawnoporównawczym ... 82
2.1.2.4.1. Regulacje europejskie ... 83
2.1.2.4.1.1. Francja ... 83
2.1.2.4.1.2. Niemcy ... 89
2.1.2.4.1.3. Polska ... 90
2.1.2.4.1.4. Wielka Brytania ... 93
2.1.2.4.2. Regulacje pozaeuropejskie ... 93
2.1.2.4.2.1. Stany Zjednoczone ... 93
2.1.2.4.2.2. Indie ... 97
2.1.3. Jurysdykcja karna ... 99
2.1.3.1. Zasady jurysdykcji karnej ... 101
2.1.3.1.1. Zasada jurysdykcji terytorialnej ... 101
2.1.3.1.2. Zasada jurysdykcji personalnej ... 104
2.1.3.1.2.1. Zasada czynnej jurysdykcji personalnej ... 104
2.1.3.1.2.2. Zasada biernej jurysdykcji personalnej ... 105
2.1.3.1.3. Zasada jurysdykcji ochronnej ... 105
2.1.3.1.4. Zasada jurysdykcji uniwersalnej ... 106
2.1.3.2. Regulacje globalne ... 111
2.1.3.2.1. Jurysdykcja a konwencja o cyberprzestępczości ... 111
2.1.3.3. Regulacje regionalne na przykładzie Unii Europejskiej ... 113
2.1.3.3.1. Decyzja ramowa 2009/948/WSiSW ... 114
2.1.3.3.2. Inne akty prawne Unii Europejskiej ... 116
2.1.3.4. Jurysdykcja karna w cyberprzestrzeni w aspekcie prawnoporównawczym ... 117
2.1.3.4.1. Regulacje europejskie ... 118
2.1.3.4.1.1. Belgia ... 118
2.1.3.4.1.2. Dania ... 120
2.1.3.4.1.3. Niemcy ... 121
2.1.3.4.1.4. Polska ... 124
2.1.3.4.1.5. Wielka Brytania ... 125
2.1.3.4.2. Regulacje pozaeuropejskie ... 127
2.1.3.4.2.1. Australia ... 127
2.1.3.4.2.2. Stany Zjednoczone Ameryki ... 129
2.2. Próba identyfikacji właściwych przedmiotowo norm wobec cyberprzestrzeni ... 130

CZĘŚĆ II
PRAWNOMIĘDZYNARODOWY WYMIAR CYBERPRZESTRZENI – *STATUS QUO*

ROZDZIAŁ 1
IDENTYFIKACJA REGULACJI PRAWNYCH CYBERPRZESTRZENI Z PERSPEKTYWY MIĘDZYNARODOWEJ ... 137
1.1. Prawnomiędzynarodowe regulacje cyberprzestrzeni ... 138
1.1.1. Regulacje wypracowane w systemie Organizacji Narodów Zjednoczonych ... 139
1.1.1.1. Dorobek Organizacji Narodów Zjednoczonych ... 139
1.1.1.2. Dorobek Biura Narodów Zjednoczonych do spraw Narkotyków i Przestępczości ... 143

1.1.1.3. Dorobek Komisji Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego ... 146
1.1.1.3.1. Ustawa modelowa UNCITRAL z 16.12.1996 r. w sprawie handlu elektronicznego ... 147
1.1.1.3.2. Ustawa modelowa UNCITRAL o podpisach elektronicznych z 12.12.2001 r. ... 148
1.1.1.3.3. Konwencja Organizacji Narodów Zjednoczonych z 23.11.2005 r. o korzystaniu z komunikacji elektronicznej w kontraktach międzynarodowych ... 151
1.1.1.4. Dorobek Forum Zarządzania Internetem ... 154
1.1.1.5. Dorobek Światowej Organizacji Własności Intelektualnej ... 156
1.1.1.5.1. Traktat WIPO o prawie autorskim ... 157
1.1.1.5.2. Traktat WIPO o artystycznych wykonaniach i fonogramach ... 158
1.1.1.6. Dorobek Międzynarodowego Związku Telekomunikacyjnego ... 159
1.1.2. Regulacje wypracowane w systemach organizacji regionalnych ... 161
1.1.2.1. Dorobek Rady Europy ... 161
1.1.2.1.1. Konwencja o cyberprzestępczości ... 163
1.1.2.1.2. Protokół dodatkowy do konwencji o cyberprzestępczości ... 172
1.1.2.1.3. Konwencja o ochronie dzieci przed wykorzystaniem seksualnym i niegodziwym traktowaniem w celach seksualnych ... 173
1.1.2.1.4. Inne regulacje Rady Europy ... 175
1.1.2.2. Dorobek Unii Europejskiej ... 177
1.1.2.2.1. Regulacje bezpośrednio odnoszące się do cyberprzestrzeni ... 178
1.1.2.2.1.1. Akty prawne dotyczące bezpieczeństwa sieci ... 178
1.1.2.2.2. Regulacje pośrednio odnoszące się do cyberprzestrzeni ... 186
1.1.2.2.2.1. Akty prawne dotyczące cyberprzestępczości ... 186
1.1.2.2.2.2. Akty prawne dotyczące danych osobowych ... 192
1.1.2.2.2.3. Akty prawne dotyczące obrotu gospodarczego ... 193
1.1.2.2.2.4. Akty prawne dotyczące własności intelektualnej ... 199
1.1.3. Regulacje organizacji wyspecjalizowanych ... 203
1.1.3.1. Dorobek Sojuszu Północnoatlantyckiego ... 203
1.1.3.2. Dorobek Europejskiej Agencji Bezpieczeństwa Sieci i Informacji ... 207
1.1.3.3. Dorobek Organizacji Współpracy Gospodarczej i Rozwoju ... 209
1.1.3.4. Dorobek Światowej Organizacji Handlu ... 213
1.1.4. Regulacje organizacji zwalczających cyberprzestępczość ... 215
1.1.4.1. Dorobek Interpolu ... 215
1.1.4.2. Dorobek Europolu ... 218
1.1.4.3. Dorobek Europejskiego Centrum do spraw Walki z Cyberprzestępczością ... 220
1.1.5. Inne regulacje ... 222
1.1.5.1. Dorobek Grupy G8 ... 222
1.1.5.2. Dorobek Brytyjskiej Wspólnoty Narodów ... 223
1.1.5.3. Dorobek CERT ... 223
1.2. Regulacje krajowe cyberprzestrzeni mające wpływ na tworzenie prawa międzynarodowego ... 224
1.2.1. Porządki prawne krajów ofiar cyberataków ... 226

1.2.1.1. Estonia a cyberprzestrzeń ... 226
1.2.1.2. Gruzja a cyberprzestrzeń ... 229
1.2.1.3. Polska a cyberprzestrzeń ... 232
1.2.2. Porządki prawne cybermocarstw ... 238
1.2.2.1. Stany Zjednoczone a cyberprzestrzeń ... 238
1.2.2.2. Rosja a cyberprzestrzeń ... 246
1.2.2.3. Chiny a cyberprzestrzeń ... 250
1.2.3. Porządki prawne krajów determinowane postępem technologicznym ... 253
1.2.3.1. Japonia a cyberprzestrzeń ... 253
1.2.3.2. Kanada a cyberprzestrzeń ... 256
Podsumowanie ... 258

ROZDZIAŁ 2
IDENTYFIKACJA KLUCZOWYCH ZAGADNIEŃ PRZEDMIOTOWYCH PRAWNOMIĘDZYNARODOWEJ REGULACJI CYBERPRZESTRZENI ... 262
2.1. Zwalczanie cyberprzestępczości a prawo międzynarodowe ... 263
2.1.1. Cyberprzestępstwa przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji ... 272
2.1.1.1. Nielegalny dostęp do systemu komputerowego (*hacking*) ... 272
2.1.1.2. *Social engineering* ... 273
2.1.1.3. Nielegalny podsłuch komputerowy ... 274
2.1.1.4. *Sniffing* ... 275
2.1.2. Naruszenie integralności danych komputerowych i systemu komputerowego ... 277
2.1.2.1. Sabotaż komputerowy. Systemy teleinformatyczne jako infrastruktura krytyczna ... 277
2.1.2.2. Niszczenie danych lub programów komputerowych ... 279
2.1.3. Cyberprzestępstwa przeciwko mieniu ... 281
2.1.3.1. Oszustwo komputerowe ... 281
2.1.3.2. Fałszerstwo komputerowe ... 284
2.1.3.3. *Phishing* ... 285
2.1.3.4. *Pharming* ... 287
2.1.4. Cyberprzestępstwa związane z treścią informacji ... 288
2.1.4.1. *Cyberstalking* ... 288
2.1.4.2. Wolność słowa a mowa nienawiści w cyberprzestrzeni ... 293
2.1.4.3. Pornografia dziecięca w Internecie ... 295
2.1.5. Kradzież tożsamości w cyberprzestrzeni ... 302
2.1.6. Cyberterroryzm ... 306
2.2. Obrót gospodarczy w cyberprzestrzeni a prawo międzynarodowe ... 313
2.2.1. Zawieranie umów w cyberprzestrzeni ... 316
2.2.1.1. Umowa – rodzaje, cechy ... 318
2.2.1.2. Zawarcie umowy ... 322
2.2.1.3. Oferta i jej przyjęcie ... 325
2.2.1.4. Negocjacje ... 329
2.2.1.5. Przetarg i aukcja ... 332
2.2.1.6. Czas i miejsce zawarcia umowy ... 337
2.2.1.7. Wykonanie umowy ... 339
2.2.1.8. Podpis elektroniczny ... 340

2.2.2. Elektroniczne środki płatnicze ... 347
2.2.2.1. Pieniądz elektroniczny ... 348
2.2.2.2. Pieniądz wirtualny ... 355
2.3. Własność intelektualna w cyberprzestrzeni a prawo międzynarodowe ... 363
2.3.1. Przedmiot ochrony ... 364
2.3.2. Naruszenie praw autorskich – piractwo komputerowe ... 366
2.3.3. Programy komputerowe ... 369
2.3.4. Bazy danych ... 371
2.3.5. Usługi *peer-to-peer* ... 373
2.3.6. Strona internetowa a prawo własności intelektualnej ... 374
2.3.7. Chmura obliczeniowa a własność intelektualna ... 376
2.4. Inne obszary cyberprzestrzeni ... 379
2.4.1. Cyberprzestrzeń a prawa człowieka ... 379
2.4.1.1. Prawo do Internetu a prawa człowieka ... 381
2.4.1.2. Wolność wypowiedzi ... 384
2.4.1.3. Prawo do prywatności ... 388
2.4.1.4. Ochrona korespondencji ... 389
2.4.2. Cyberprzestrzeń a ochrona danych osobowych ... 390
2.4.3. Adekwatność dotychczasowych rozwiązań prawnych wobec problemów przedmiotowych cyberprzestrzeni – próba oceny ... 394

CZĘŚĆ III
KONCEPCJA REKONSTRUKCJI STATUSU PRAWNEGO CYBERPRZESTRZENI (Z WYKORZYSTANIEM PRAWA MIĘDZYNARODOWEGO)

ROZDZIAŁ 1
POSTULATY I PROPOZYCJE ROZWIĄZAŃ PRAWNYCH DLA CYBERPRZESTRZENI ... 401
1.1. Koncepcje samoregulacji cyberprzestrzeni ... 402
1.1.1. Autonomiczne prawo cyberprzestrzeni ... 403
1.1.2. *Lex informatica* ... 408
1.1.3. Inicjatywa *Creative Commons* ... 415
1.1.4. Cyberprzestrzeń jako czwarta przestrzeń międzynarodowa ... 417
1.2. Koncepcja nowego ładu cyberprzestrzeni ... 424
1.2.1. Rekonstrukcja pojęcia prawa cyberprzestrzeni ... 425
1.2.2. Aspekt podmiotowy nowego ładu cyberprzestrzeni ... 428
1.2.3. Aspekt przedmiotowy nowego ładu cyberprzestrzeni ... 433
1.2.4. Aspekt proceduralny nowego ładu cyberprzestrzeni ... 437
1.3. Rekonstrukcja prawa cyberprzestrzeni ... 443

PODSUMOWANIE ... 447

BIBLIOGRAFIA ... 457

SPIS RYSUNKÓW ... 483

SPIS TABEL ... 485

WSTĘP

Cyberprzestrzeń, nazywana również Internetem, przestrzenią cyfrową lub wirtualną, jest swoistym medium, które bez wątpienia zrewolucjonizowało współczesny świat. Mimo że geneza cyberprzestrzeni sięga lat 60. XX wieku, to momentem przełomowym dla globalnej sieci były lata 90. przypadające na okres komercjalizacji Internetu, ale przede wszystkim upowszechnienia komputerów osobistych. Liczba użytkowników Internetu wynosiła wówczas kilkanaście milionów[1]. Według danych witryny Internet World Stats w czerwcu 2019 r. liczba internautów przekroczyła 4,5 mld[2]. Oznacza to, że ponad połowa światowej populacji jest częścią globalnej wioski, położonej w nowej przestrzeni, o wirtualnym, transgranicznym, aterytorialnym i ponadnarodowym charakterze. Jeszcze nigdy w historii naszego globu nie było możliwości tak łatwego, taniego i szybkiego przesyłania danych czy komunikowania się na odległość.

Intensywny rozwój systemów informacyjnych i telekomunikacyjnych w ostatnich trzech dekadach sprawił, że cyberprzestrzeń stała się ważnym czynnikiem wspomagającym i stymulującym rozwój gospodarczy państw, w szczególności krajów wysoko rozwiniętych. Wysoki poziom komputeryzacji przyczynił się jednakże do wzrostu uzależnienia krajów od ich poprawnego i niezakłóconego działania. Ewolucja i postępująca ekspansja cyberprzestrzeni zdeterminowały nieznane dotąd zagrożenia, takie jak cyberprzestępczość czy cyberterroryzm. W państwie informacyjnym, którego wszelkie dziedziny życia oparte są na skoncentrowanych w systemach komputerowych źródłach informacji, zakłócenie ich funkcjonowania oznacza dezorganizację życia państwa i społeczeństwa. Konsekwentny i coraz silniejszy rozkwit koniunktury wirtualnej na przestrzeni ostatnich lat spowodował, że przestrzeń cyfrowa ma coraz silniejszy wpływ na takie dziedziny życia, jak produkcja, handel czy też edukacja i prawo.

Ogromna liczba użytkowników sieci oraz nieograniczony narodowo charakter Internetu powodują, że stroną ulokowanego tu stosunku prawnego może być niemal co drugi mieszkaniec Ziemi. Ustawodawcy krajowi mimo podejmowanych prób nie są

---

[1] K.B. Wydro, *Internet dziś – stan i wykorzystanie* [w:] *Fenomen Internetu*, red. A. Szewczyk, E. Krok, t. 1, Szczecin 2008, s. 51.

[2] http://www.internetworldstats.com/stats.htm (dostęp: 16.12.2019 r.).

w stanie nadążyć za szybkimi zmianami technologicznymi, brakuje jednolitych reguł postępowania oraz unormowań podstawowych kwestii, takich jak jurysdykcja czy sposób zarządzania cyberprzestrzenią. Omawiane medium nie ma granic, fizycznego podziału, narodowości ani jednego prawa właściwego, dlatego też stanowi wyzwanie dla teoretyków i praktyków prawa. Szczególne znaczenie w procesie regulacji statusu cyberprzestrzeni mają prace organizacji międzynarodowych, które podejmują działania w kierunku harmonizacji przepisów dotyczących działalności człowieka w przestrzeni wirtualnej. Podjęta problematyka, mimo globalnego wymiaru, ma bezpośrednie i praktyczne przełożenie na codzienną rzeczywistość milionów ludzi żyjących w różnych regionach świata. Powoduje to, że wybór tematu ma tu uzasadnienie zarówno obiektywne, jak i subiektywne. Przygotowana publikacja ma charakter interdyscyplinarny, gdyż tylko takie podejście pozwoli na gruntowne zbadanie tematu. Omówione w książce zagadnienia mogą stać się przyczynkiem do dalszej dyskusji o roli prawa międzynarodowego w cyberprzestrzeni.

Niniejsza książka stanowi uzupełnioną wersję rozprawy o doktorskiej o tożsamym tytule. Celem niniejszych rozważań jest weryfikacja aktualnego statusu cyberprzestrzeni w kierunku jej optymalnego uregulowania z wykorzystaniem prawa międzynarodowego. Zostanie również dokonana identyfikacja obszarów, w których istnieje konieczność unifikacji przepisów odnoszących się do cyberprzestrzeni.

Głównym celem niniejszej publikacji jest ustalenie, czy prawo międzynarodowe może udoskonalić rekonstrukcyjnie aktualny status cyberprzestrzeni. Niniejsza monografia odpowiada na pytania dotyczące reguł jurysdykcyjnych stosowanych w cyberprzestrzeni, zakresu, w jakim państwa, organizacje międzynarodowe i inne podmioty podejmują próbę regulacji cyberprzestrzeni. Przedstawione zostaną rozważania na temat płaszczyzn, w których prawo międzynarodowe może mieć zastosowanie w stosunku do cyberprzestrzeni, oraz obszarów, w których prawo międzynarodowe przyczynia się do unifikacji problematycznych kwestii związanych przestrzenią wirtualną. Wreszcie w publikacji podjęto próbę przedstawienia adekwatnych postulatów i propozycji rozwiązań prawnych regulacji cyberprzestrzeni. W monografii postawiono tezę, wedle której prawo międzynarodowe jest najbardziej predysponowane do racjonalnego i użytecznego modelowania oraz harmonizacji regulacji krajowych cyberprzestrzeni.

Badania przedstawione w niniejszej publikacji zostały oparte na metodologii dogmatycznej, polegającej na analizie wielostronnych umów międzynarodowych, aktów prawnych uniwersalnych i regionalnych organizacji międzynarodowych oraz dokumentów tworzonych przez podmioty zajmujące się problematycznymi zagadnieniami występującymi w cyberprzestrzeni, jak np. cyberprzestępczością. Zastosowanie tej metody pozwoliło na określenie norm prawnych stosowanych w przestrzeni wirtualnej oraz identyfikację przedmiotowych obszarów, w których istnieje potrzeba regulacji i harmonizacji. Nie mniej istotna okazała się analiza prawnoporównawcza

wybranych państw oraz analiza orzecznictwa i doktryny, która pozwoliła na porównanie judykatury i określenie, w jaki sposób kształtuje się praktyka sądowa w wybranych państwach oraz jak cyberprzestrzeń winna być regulowana według znawców prawa.

Przygotowana publikacja jest obszerna, dlatego została podzielona na trzy części. Część pierwsza „Cyberprzestrzeń a jurysdykcja" składa się z dwóch rozdziałów. W pierwszym, zatytułowanym „Cyberprzestrzeń – pojęcie i geneza", omówiono pojęcie, genezę i ewolucję historyczną cyberprzestrzeni oraz etapy rozwoju społeczeństwa informacyjnego. Opisano także kluczowe koncepcje i poglądy doktryny krajowej oraz zagranicznej na temat cyberprzestrzeni. Ukazano statystyki odnoszące się do liczby użytkowników sieci oraz etapów rozwoju sieci wirtualnej. Zasygnalizowano również zagrożenia związane z funkcjonowaniem cyberprzestrzeni. W rozdziale drugim, „Jurysdykcja państwowa a cyberprzestrzeń", ujęto rozważania wskazujące prawo właściwe do zobowiązań umownych zawieranych za pośrednictwem Internetu, deliktów elektronicznych oraz jurysdykcji w sprawach cywilnych i handlowych. Wskazano międzynarodowe oraz regionalne akty prawne, które mogą mieć zastosowanie do umów zawieranych w przestrzeni cyfrowej. Opisano również rozwiązania prawne wybranych krajów oraz orzecznictwo poruszające kwestię prawa właściwego w stosunkach cywilno-gospodarczych w przestrzeni wirtualnej. Przedstawiono zagadnienie jurysdykcji karnej w odniesieniu do czynów przestępczych popełnionych w cyberprzestrzeni. Ponadto ukazano model władztwa jurysdykcyjnego przyjęty w Konwencji Rady Europy o cyberprzestępczości z 23.11.2001 r. oraz w decyzji ramowej Rady 2009/948/WSiSW z 30.11.2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów. Szczegółowo omówiono również kwestię jurysdykcji karnej w cyberprzestrzeni w ujęciu prawnoporównawczym wybranych państw. Podjęto też rozważania na temat teoretycznego ujęcia zasad jurysdykcji oraz możliwości ich zastosowania w cyberprzestrzeni.

Część druga publikacji „Prawnomiędzynarodowy wymiar cyberprzestrzeni – *status quo*" także składa się z dwóch rozdziałów. Rozdział pierwszy części drugiej, zatytułowany „Identyfikacja regulacji prawnych cyberprzestrzeni z perspektywy międzynarodowej", poświęcono wnikliwej analizie norm prawnych dotyczących cyberprzestrzeni ustanowionych przez powszechne i regionalne organizacje międzynarodowe, w tym międzynarodowe organy ścigania oraz inne instytucje zainteresowane regulacją statusu przestrzeni wirtualnej. Ponadto ukazano, jakie regulacje prawne w odniesieniu do cyberprzestrzeni zostały przyjęte w cybermocarstwach, krajach determinowanych postępem technologicznym oraz państwach, które stały się ofiarami cyberataków. W drugim rozdziale „Identyfikacja kluczowych zagadnień przedmiotowych prawnej regulacji cyberprzestrzeni" poruszono problem zwalczania cyberprzestępczości, obrotu gospodarczego, własności intelektualnej i innych obszarów, w których prawo międzynarodowe może mieć zastosowanie. Druga część książki jest najobszerniejsza,

między innymi ze względu na złożoność przedstawionej problematyki. Brak jednej, uniwersalnej instytucji międzynarodowej regulującej działalność człowieka w cyberprzestrzeni powoduje fragmentację oraz rozproszenie przyjętych rozwiązań. Tym bardziej była potrzebna identyfikacja kluczowych zagadnień podlegających regulacji w przestrzeni cyfrowej.

Trzecią część monografii zatytułowano „Koncepcja rekonstrukcji statusu prawnego cyberprzestrzeni (z wykorzystaniem prawa międzynarodowego)". W części tej znajduje się ostatni rozdział „Postulaty i propozycje rozwiązań dla cyberprzestrzeni", w którym przedstawiono postulaty i koncepcje zmian zarządzania i regulacji cyberprzestrzeni. W pierwszej kolejności zaprezentowano koncepcje samoregulacji przestrzeni. Następnie zaproponowano koncepcję nowego ładu cyberprzestrzeni w aspekcie podmiotowym, przedmiotowym oraz proceduralnym, a także przeprowadzono rekonstrukcję prawa cyberprzestrzeni oraz podjęto próbę jego definicji.

Niniejsza publikacja nie wyczerpuje wszystkich aspektów działalności człowieka w cyberprzestrzeni w świetle prawa międzynarodowego, tworząc jedynie zarys problematyki, który (być może) będzie przyczynkiem do dalszych rozważań i dyskusji w doktrynie. Problemy, które dotyczą cyberprzestrzeni, takie jak cyberprzestępczość, cyberterroryzm czy transgraniczne zawieranie umów internetowych, coraz częściej są dyskutowane w doktrynie polskiej i zagranicznej. Cyberprzestrzeń stanowi wielkie wyzwanie dla prawa, nie tylko ze względu na swój transgraniczny, niematerialny charakter, ale również ze względu na fakt, że w przestrzeni tej zastosowanie znaleźć może niemal każda dziedzina prawa – prawo karne, cywilne, handlowe, prawo własności intelektualnej czy chociażby prawo bankowe. Bardzo liczne potencjalne możliwości powodują, że autorzy skupiają się zazwyczaj na jednej gałęzi prawa bądź jednym zagadnieniu przedmiotowym. Jedynie nieliczni autorzy podejmują próbę holistycznego opracowania naukowego poruszającego kwestie natury i zasad rządzących cyberprzestrzenią.

Pozycja skierowana jest zarówno do teoretyków, jak i praktyków prawa w zakresie stosowania go w nowej, wirtualnej przestrzeni. Książka podzielona jest według zagadnień tematycznych pochodzących z różnych gałęzi prawa. W publikacji szczegółowo zostały opisane zasady stosowania jurysdykcji karnej i cywilnej w cyberprzestrzeni, kwestie dotyczące cyberprzestępczości, cyberterroryzmu, obrotu gospodarczego w cyberprzestrzeni (w tym kwestie elektronicznych środków płatniczych, tj. pieniądza wirtualnego), własności intelektualnej czy też praw człowieka i ochrony danych osobowych w przestrzeni wirtualnej. Praktycy prawa (adwokaci, radcy prawni, prokuratorzy, sędziowie) znajdą w książce interesujące informacje dotyczące m.in. stosowania prawa właściwego w przypadku wystąpienia „cyberczynnika". Nie mniej istotne jest również szerokie ujęcie tematu obejmujące prawo międzynarodowe, prawo Unii Europejskiej, jak też przedstawienie wybranego orzecznictwa w tym przedmiocie.

Z kolei teoretycy prawa zainteresowani tematyką nowych technologii znajdą w książce obszerny przegląd poglądów doktryny, judykatury oraz analizę wielostronnych umów międzynarodowych, aktów prawnych organizacji międzynarodowych, dokumentów z zakresu *soft law* oraz reprezentatywnych przykładów unormowań z prawa krajowego. W ocenie autorki pozycja taka może być użyteczna dla studentów nie tylko prawa, ale również innych kierunków, takich jak bezpieczeństwo narodowe, wewnętrzne czy też cyberbezpieczeństwo.

Rozdział 2

IDENTYFIKACJA KLUCZOWYCH ZAGADNIEŃ PRZEDMIOTOWYCH PRAWNOMIĘDZYNARODOWEJ REGULACJI CYBERPRZESTRZENI

Użytkownicy korzystają z Internetu w celach prywatnych, służbowych, handlowych czy rozrywkowych. Cyberprzestrzeń jest również ogromnym rynkiem usług, które w jednej sekundzie łączą oddalone od siebie o miliony kilometrów podmioty. W ostatnich latach przestrzeń cyfrowa wzbudza ogromne zainteresowanie państw, głównie w kontekście zagrożeń związanych z działalnością przestępczą oraz terrorystyczną. Kraje coraz śmielej – w sposób bardziej lub mniej jawny – wykorzystują przestrzeń wirtualną do realizacji swoich celów politycznych czy gospodarczych. Cyberprzestrzeń jest wykorzystywana zarówno przez państwa, jak i inne podmioty (pojedynczych hakerów, zorganizowane grupy przestępcze, terrorystów) do prowadzenia wojny informacyjnej. W przyszłości realny wydaje się wybuch cyberwojny – konfliktu, w którym kluczową rolę odgrywać będzie komputer, za pomocą którego prowadzona będzie propaganda, dezinformacja, ale również cybernetyczne ataki na systemy i programy przeciwnika.

Nigdy wcześniej nie mieliśmy do czynienia z obszarem, który z uwagi na swój wirtualny, transgraniczny i transnarodowy charakter skupia w jednym miejscu miliardy rozmaitych podmiotów (państwa, osoby fizyczne i prawne) pochodzących z różnych krajów i porządków prawnych. Powstanie konfliktu jurysdykcyjnego – czy to na poziomie publicznym, prywatnym, karnym, czy cywilnym – wydaje się być tylko kwestią czasu. Przestrzeń wirtualna nie posiada jednego, zunifikowanego i harmonijnego prawa. Prawo cyberprzestrzeni tworzą m.in. akty prawa międzynarodowego, akty stanowione organizacji międzynarodowych oraz prawo krajowe. Należy jednak postawić sobie pytanie, jakie zagadnienia są szczególnie istotne w kontekście międzynarodowej regulacji cyberprzestrzeni i działań w niej podejmowanych.

W niniejszym rozdziale zostaną poruszone kwestie związane z dozwolonym i niedozwolonym wykorzystaniem przestrzeni wirtualnej przez jej użytkowników. Szczególnie palący jest problem cyberprzestępczości, ponieważ szybki rozwój techniki spowodował powstanie zupełnie nowej kategorii przestępstw, które są trudne do wykrycia, ścigania i efektywnego osądzenia m.in. ze względu na trudności w zebraniu dowodów, w tym dowodów cyfrowych. Nie mniej istotnym zagadnieniem – szczególnie ważkim w obliczu zwiększającej się liczby ekstremistów i walki informacyjnej – jest wykorzystanie cyberprzestrzeni przez terrorystów, którzy za pomocą sieci wirtualnej zbierają fundusze, rekrutują nowych członków oraz prowadzą działania propagandowe.

W niniejszej książce zostaną opisane podstawowe zagadnienia związane z kwestią obrotu gospodarczego w przestrzeni cybernetycznej. Internet usprawnił, przyśpieszył i umożliwił wymianę towarów i usług na ogromną skalę. Należy zadać pytania, czym jest obrót gospodarczy w cyberprzestrzeni, w jaki sposób następuje zawarcie umów oraz jakie reguły należy stosować przy zastosowaniu najnowszych elektronicznych form płatności. Inne problemy prawa zobowiązań w cyberprzestrzeni (delikty, odpowiedzialność za produkty niebezpieczne i tym podobne), choć ciekawe, nie będą szczegółowo poruszone w niniejszej pracy. W dalszych rozważaniach zostanie pokrótce opisane stosunkowo nowe zjawisko pieniędzy wirtualnych oraz kwestie związane z najnowszymi problemami własności intelektualnej, ochrony danych osobowych oraz praw człowieka w przestrzeni cyfrowej. Identyfikacja i szczegółowy opis tych obszarów są konieczne do wskazania istniejących uregulowań prawnych, obszarów pozostających poza systemem prawa krajowego i międzynarodowego oraz inicjatyw podjętych w tym przedmiocie.

2.1. Zwalczanie cyberprzestępczości a prawo międzynarodowe

Wojny, terroryzm i przestępczość to problemy, z którymi świat zmaga się od setek lat. Jednakże wejście w nową erę – erę komputerów, telefonów komórkowych, Internetu, GPS-ów oraz satelitów – spowodowało, że stanęliśmy w obliczu zupełnie nowych wyzwań i zagrożeń. Punktem wyjścia do dalszych rozważań będzie wskazanie podstawowych rodzajów zagrożeń w cyberprzestrzeni (tabela 8).

Tabela 8. Podstawowe rodzaje cyberzagrożeń

Zjawisko	Cechy charakterystyczne
Cyberprzemoc	wykorzystanie cyberprzestrzeni w celu wymuszenia odbioru niepożądanych komunikatów zawierających informacje (dane, obrazy, treści), sprzecznych z wartościami adresata
Cyberprzestępstwo	wykorzystanie cyberprzestrzeni w celu dokonania aktów kryminalnych pospolitych i zorganizowanych skierowanych na zasoby osób prywatnych i/lub organizacji (instytucji)
Cyberinwigilacja	wykorzystanie cyberprzestrzeni w celu kontroli i/lub pozyskiwania informacji o zachowaniach i działaniach obywateli (społeczności, społeczeństwa) (efekt „Big Brother")
Cyberterroryzm	wykorzystanie cyberprzestrzeni w celu działań terrorystycznych (państwowych i pozapaństwowych)
Cyberautokratyzm	wykorzystanie cyberprzestrzeni w życiu politycznym państwa niezgodnie z zasadami demokracji liberalnej (przeciwieństwem – cyberdemokracja)
Cyberwojna	wykorzystanie cyberprzestrzeni w celu realizacji działań politycznych realizowanych przez siły zbrojne (*cyberwarriors*) i skierowanych na zasoby i struktury państwa przeciwnika (również w działaniach innych niż wojna)

Źródło: K. Węderska, *Cybernetyczny Pearl Harbor – mit czy rzeczywistość?* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku*, red. M. Górka, Warszawa 2014, s. 71, na podstawie: *Metody badań nad bezpieczeństwem i obronnością*, red. P. Sienkiewicz, Warszawa 2010.

Pytanie, czym jest cyberprzestępczość i jak ją zdefiniować, budzi szereg wątpliwości. Maciej Siwicki stoi na stanowisku, że dzieje się tak dlatego, że „przestępczość ta ciągle ewaluuje i dostosowuje w sposób elastyczny swoje wielorakie przejawy do zmian technologicznych, często reaguje przy tym z dużą ruchliwością na stosowane wobec niej społeczne środki kontroli"[1]. Krzysztof Gienas uznał, że na specyfikę cyberprzestrzeni składają się dwa elementy: jej eksterytorialny charakter oraz możliwość korzystania z jej zasobów w sposób pozornie anonimowy[2].

Termin „cyberprzestępczość" wywodzi się z anglojęzycznego słowa *cybercrime*, które należy podzielić na dwa człony: *cyber* i *crime*. Drugi ze wskazanych terminów oznacza „zbrodnię, przestępstwo czy występek". Większe trudności nastręcza zdefiniowanie słowa *cyber*, które samo w sobie nie jest oddzielnym terminem, zostało wyodrębnione ze słowa cybernetyka (ang. *cybernetics*). Słowo te pochodzi z greckiego *kybernetes*, które oznacza „sternika, zarządcę", a *kybernán* tłumaczyć należy jako „sterowanie, kontrolowanie". Cybernetyka jest nauką o systemach sterowania oraz związanym z tym przetwarzaniu i przekazywaniu informacji, komunikacji[3].

[1] M. Siwicki, *Cyberprzestępczość…*, s. 15.
[2] K. Gienas, *Cyberprzestępczość*, „Jurysta" 2003/12, s. 9.
[3] M. Siwicki, *Cyberprzestępczość…*, s. 15.

Joanna Worona – doktor nauk prawnych; adwokat, członek Okręgowej Rady Adwokackiej w Białymstoku; specjalizuje się w prawie karnym oraz prawie międzynarodowym; autorka publikacji naukowych z dziedziny prawa w przestrzeni wirtualnej oraz współautorka podręcznika dotyczącego bezpieczeństwa w cyberprzestrzeni.

Publikacja stanowi próbę całościowego zbadania tematu prawa w cyberprzestrzeni z perspektywy prawa międzynarodowego, prawa organizacji międzynarodowych oraz prawodawstwa wybranych państw, w tym Polski. Interdyscyplinarność cyberprzestrzeni powoduje, że doktryna skupia się zazwyczaj tylko na wybranych zagadnieniach przedmiotowych.

W książce omówiono m.in. następujące problemy dotyczące:
– pojęcia, genezy i ewolucji historycznej cyberprzestrzeni,
– jurysdykcji karnej i cywilnej w cyberprzestrzeni,
– analizy norm prawnych dotyczących cyberprzestrzeni ustanowionych przez powszechne i regionalne organizacje międzynarodowe,
– cyberprzestępczości, cyberterroryzmu, pieniądza wirtualnego i umów zawieranych w Internecie,
– postulatów i koncepcji zmian zarządzania cyberprzestrzenią i jej regulacji.

Opracowanie zawiera obszerny przegląd poglądów doktryny, judykatury oraz analizę wielostronnych umów międzynarodowych.

Publikacja będzie wsparciem dla praktyków prawa, pracowników naukowych i studentów, zainteresowanych tematyką nowych technologii.

„Książka porusza ogrom różnorodnych zagadnień wynikających z konfrontacji cyberprzestrzeni z prawem. W konfrontacji tej zawsze przegrywa prawo, które musi podążać za zmianami technologicznymi. Autorka nie tylko przedstawia problemy i pytania, ale także stara się na nie odpowiadać".

Dr hab. Maciej Rogalski, prof. Uczelni Łazarskiego w Warszawie

9788381870252 W01P01

ISSN 1897-4392
ISBN 978-83-8187-025-2

9 788381 870252

ZAMÓWIENIA:
INFOLINIA 801 04 45 45
ZAMOWIENIA@WOLTERSKLUWER.PL
WWW.PROFINFO.PL

CENA 149 ZŁ (W TYM 5% VAT)

GARDOCKI i PARTNERZY
ADWOKACI I RADCOWIE PRAWNI