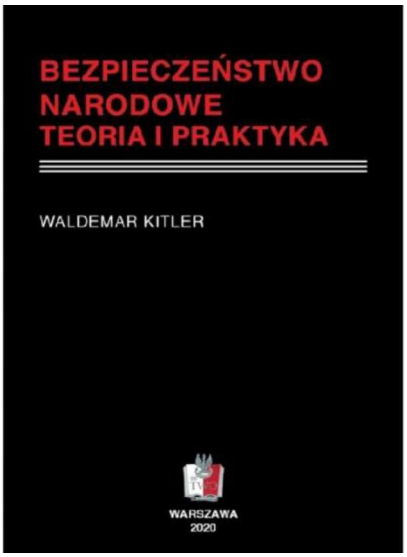
CYBERBEZPIECZEŃSTWO

JAKO FILAR BEZPIECZEŃSTWA NARODOWEGO

Pakiet 3 książki

ISBN 978-83-68170-83-2 (PDF)



MODELE ROZWIĄZAŃ PRAWNYCH

W SYSTEMIE CYBERBEZPIECZEŃSTWA RP

REKOMENDACJE

Publikacja powstała w ramach Grantu Badawczego MON
„System cyberbezpieczeństwa RP – model rozwiązań prawnych".
Umowa MON nr GB/4/2018/208/2018/DA. Zadanie nr 62.

WARSZAWA
2021

Redakcja naukowa:
Katarzyna Chałubińska-Jentkiewicz
Agnieszka Brzostek

Recenzenci:
Prof. dr hab. Waldemar Kitler, ASZWOJ
dr hab. Jarosław Kostrubiec, prof. UMCS

Redakcja merytoryczna:
dr Zbigniew Moszumański

Opracowanie graficzne i projekt okładki:
IDEAPRESS Sp. z o.o. Anna Skowrońska

ISBN 978-83-960228-1-3 (miękka oprawa)
ISBN 978-83-68170-37-5 (pdf)
ISBN 978-83-68170-38-2 (epub)
ISBN 978-83-68170-39-9 (mobi)

Wydanie I

Publikacja jest finansowana przez
Akademickie Centrum Polityki Cyberbezpieczeństwa
Akademia Sztuki Wojennej

Wydawca:
Wydawnictwo Towarzystwa Wiedzy Obronnej
ul. 11 Listopada 17/19, 03-446 Warszawa
www.two.edu.pl
e-mail: kontakt@two.edu.pl

Wydawnictwo Towarzystwa Wiedzy Obronnej znajduje się w wykazie
wydawnictw publikujących recenzowane monografie naukowe,
sporządzonym przez MNiSzW: poz. 652, poziom I – 80 punktów.

Skład:
IDEAPRESS Sp. z o.o. Katarzyna Pogrzebska
Przygotowanie do druku:
IDEAPRESS Sp. z o.o.
ul. Konstantego Ildefonsa Gałczyńskiego 4 /901, 00-362 Warszawa
www.ideapress.pl

Spis treści | Contents

Wstęp
Introduction

Cyberprzestrzeń może wydawać się bardzo oddalona od sfery obronności i bezpieczeństwa narodowego. W ciągu ostatnich 20 lat technologie cyfrowe połączyły nasze życie osobiste i zawodowe, podniosły konkurencyjność firm na niespotykany dotąd poziom, a także zbliżyły administrację do użytkowników. Każdy bowiem korzysta z połączonych sieci z zaawansowanymi programami cyberobrony. Na poziomie indywidualnym atak może być przeprowadzony wielopłaszczyznowo i przynieść rozległe szkody, tj. kradzież tożsamości, próby wyłudzenia czy utrata danych osobowych, włamania do sieci osobistych oraz kradzież rodzinnych pamiątek. Cyberprzestrzeń stała się miejscem konfrontacji, zawłaszczania danych osobowych, szpiegowania naukowego, gospodarczego i handlowego dziedzictwa firm będących ofiarami konkurencji lub obcych mocarstw czy też wstrzymywania usług niezbędnych do prawidłowego funkcjonowania gospodarki lub życia codziennego, narażenia utraty suwerenności, a nawet – w pewnych okolicznościach – pozbawienia życia ludzkiego.

Współcześnie cyberprzestrzeń nie jest już traktowana jako odrębna kategoria polityki czy działalności oddzielonej od innych elementów władzy krajowej. Cyberprzestrzeń i jej ochrona stały się bowiem stałym elementem systemu ochrony bezpieczeństwa państwa i obronności. Na poziomie ogólnopaństwowym takie ataki mogą przynieść długotrwale odczuwalne skutki finansowe, ekonomiczne i społeczne. Szczelny, ofensywny, sprawnie współpracujący

z podmiotami zewnętrznymi, prowadzący ciągły monitoring i wyposażony w specjalistów w odpowiednich dziedzinach system bezpieczeństwa cybernetycznego może zmniejszać skutki tych ataków, a nawet je uniemożliwić. Dotyczy przede wszystkim najważniejszych systemów cybernetycznych, takich jak: sieci energetyczne, sieci komunikacyjne lub instytucje finansowe, które są tak ważne, że każde zakłócenie może mieć poważne konsekwencje dla bezpieczeństwa publicznego i bezpieczeństwa narodowego. Nie sposób nie docenić wysiłków organów ścigania, które mają na celu zwalczanie cyberprzestępczości przy jednoczesnej ochronie prywatności w cyberprzestrzeni. Powszechnie uznaje się, że cyberbezpieczeństwo służy ochronie danych osobowych, a co za tym idzie – prywatności. Na przykład, Kanadyjczycy wspierają wysiłki na rzecz ochrony swojej prywatności w Internecie oraz przyznają, że organy ścigania stoją przed wyzwaniami związanymi z cyberprzestępczością, i są zaniepokojeni rosnącym zagrożeniem cyberprzestępczością osób fizycznych, organizacji sektora prywatnego i publicznego oraz rządów.

Niniejsza monografia powstała w wyniku realizacji przez Akademię Sztuki Wojennej grantu badawczego na temat: „System cyberbezpieczeństwa RP – model rozwiązań prawnych" – jako projektu w zakresie obronności i bezpieczeństwa państwa, finansowanego ze środków Ministerstwa Obrony Narodowej[1]. Cyberbezpieczeństwo jako zjawisko interdyscyplinarne stało się przedmiotem rozważań Autorów. Badaniom poddano działalność państw jako podmiotów prawa międzynarodowego, skupiając się na wskazaniu prawnych i organizacyjnych rozwiązań przyjętych zarówno w wymiarze indywidualnym, jak i w sposób zorganizowany, aby efektywne przeciwdziałać oraz zwalczać niepożądane i przestępcze zachowania w cyberprzestrzeni. Wyodrębnieniu uległy także relacje pomiędzy

[1] „System cyberbezpieczeństwa RP – model rozwiązań prawnych" – projekt w zakresie obronności i bezpieczeństwa państwa, objęty kodem A.I.1.2.0 i numerem Kwestury 62, finansowany ze środków Ministerstwa Obrony Narodowej na podstawie decyzji nr 5/2018/GB z dnia 7 listopada 2018 r. [umowa MON GB/4/2018/208/2018/DA]. Kierownik projektu: dr hab. Katarzyna Chałubińska-Jentkiewicz, profesor ASzWoj. Zadanie badawcze nr 3: *Diagnoza formalno-prawnych podstaw i stanu organizacji bezpieczeństwa personalnego w aspekcie prywatności i tożsamości w ramach jednolitego i zintegrowanego systemu cyberbezpieczeństwa RP.*

systemem cyberbezpieczeństwa a systemem prawa i związanym z tym działaniem organów władzy publicznej. Odrębna kwestię stanowi analiza prawno-administracyjnych uregulowań w zakresie ochrony danych osobowych jako ochrony prawa do prywatności oraz ochrony informacji w cyberprzestrzeni, a także odpowiedzialności karnej za naruszenie dóbr podlegających ochronie.

Redaktorzy

I

Cyberbezpieczeństwo jako przedmiot prawa międzynarodowego – kierunki zmian

Cybersecurity as Subject of International Law – Directions of Changes

Piotr Milik[1]

Uwarunkowania globalne cyberbezpieczeństwa

Global Conditions of Cybersecurity

Streszczenie: W niniejszym opracowaniu zostały poddane analizie aktualne wysiłki państw zmierzające do ustanowienia prawnych ram współpracy w celu skutecznego przeciwdziałania oraz zwalczania niepożądanych i przestępczych zachowań w cyberprzestrzeni. Najpierw zostaną wymienione instrumenty rangi międzynarodowej o charakterze prawnie wiążącym, czyli umowy międzynarodowe wielostronne i dwustronne, których celem jest zdefiniowanie zagrożeń występujących w cyberprzestrzeni i skonstruowanie mechanizmów współpracy pozwalających na ich skuteczne zwalczanie. Następnie zostaną przeanalizowane aktualne wysiłki i inicjatywy nowych rozwiązań proponowanych na forum międzynarodowym, zwłaszcza inicjatywa Zgromadzenia Ogólnego ONZ z grudnia 2019 r. zmierzająca do przyjęcia nowej umowy międzynarodowej o globalnym, powszechnym zasięgu regulującej kwestie bezpieczeństwa w cyberprzestrzeni.
Słowa kluczowe: cyberprzestrzeń, zwalczanie przestępczości, zapobieganie przestępczości, umowy międzynarodowe wielostronne i dwustronne.

[1] Doktor habilitowany, Katedra Prawa Bezpieczeństwa Instytutu Prawa Akademii Sztuki Wojennej w Warszawie, adwokat.

*

Summary: This study will analyze the current efforts of states to establish a legal framework for cooperation to effectively prevent and combat undesirable and criminal behavior in cyberspace. First of all, the instruments of international rank of legally binding nature will be mentioned, i.e. multilateral and bilateral international agreements, the purpose of which is to define threats occurring in cyberspace and construct cooperation mechanisms allowing for effective counteraction. Next, the current efforts and initiatives of new solutions proposed on the international forum will be analyzed, in particular the initiative of December 2019 of the UN General Assembly aimed at adopting a new international agreement of global scope regulating the issues of security in cyberspace.
Keywords: cyberspace, fighting crime, crime prevention, bilateral and multilateral international agreements.

***

Na potrzeby niniejszego opracowania możemy zdefiniować pojęcie „cyberprzestrzeń" jako globalną sieć, na którą składają się połączone systemy teleinformatyczne zbudowane z urządzeń umożliwiających tworzenie, przetwarzanie oraz wymianę informacji automatycznie między urządzeniami lub świadomie i celowo między ich użytkownikami. Tak zdefiniowana cyberprzestrzeń, stanowiąca strefę codziennej aktywności państw i ich obywateli, w której są realizowane żywotne dla tych podmiotów interesy, jest stale zagrożona głównie nielegalną działalnością osób i grup przestępczych, w tym terrorystycznych, a także na skutek błędów lub awarii poszczególnych systemów teleinformatycznych.

Pandemia wirusa COVID-19, z którą świat zmierzył się w 2020 r., spowodowała przyspieszenie procesów informatyzacji usług publicznych i prywatnych. Nabrała też tempa rewolucja informacyjna (cyfrowa), którą obserwowaliśmy w ostatnich dziesięcioleciach. Aktywność życiowa i zawodowa rozwiniętych społeczeństw jest związana w znacznej mierze z cyberprzestrzenią. Edukacja powszechna, wykłady akademickie, operacje bankowe, zakupy wszelkiego rodzaju towarów i usług, komunikacja z urzędami przeniosły się niemal z dnia na dzień do Internetu. Rozwinięte społeczeństwa przeszły przyspieszony kurs

korzystania z nowych technologii informacyjnych. Niestety, gwałtowne tempo tych zmian pociągnęło za sobą wzmożoną falę nadużyć. Cyberprzestępczość rozkwitła wraz z intensyfikacją operacji cyfrowych prowadzonych w sieci. Problematyka cyberbezpieczeństwa stała się więc ważna i aktualna, jak jeszcze nigdy dotąd.

W związku z wyżej wskazanymi zagrożeniami – państwa indywidualnie, we współpracy z innymi państwami, w tym w ramach współpracy zinstytucjonalizowanej, próbują przeciwdziałać negatywnym zjawiskom w cyberprzestrzeni, tzn. przy pomocy wyspecjalizowanych narzędzi i służb zwalczać zagrożenia bezpieczeństwa obrotu informacji. Ponieważ charakterystyczną cechą cyberprzestrzeni jest jej eksterytorialność i powszechny, globalny zasięg, w celu skutecznego przeciwdziałania zagrożeniom bezpieczeństwa informatycznego konieczna jest współpraca państw i innych podmiotów działających na arenie międzynarodowej (organizacji międzynarodowych międzyrządowych i pozarządowych).

W niniejszym opracowaniu zostaną poddane analizie aktualne wysiłki państw zmierzające do ustanowienia prawnych ram współpracy mających umożliwić skuteczne przeciwdziałanie i zwalczanie niepożądanych i przestępczych zachowań w cyberprzestrzeni.

Najpierw zostaną wymienione instrumenty rangi międzynarodowej o charakterze prawnie wiążącym, czyli umowy międzynarodowe wielostronne i dwustronne, których celem jest zdefiniowanie zagrożeń występujących w cyberprzestrzeni i skonstruowanie mechanizmów współpracy pozwalających na ich skuteczne zwalczanie. Następnie zostaną przeanalizowane wysiłki i inicjatywy nowych rozwiązań proponowanych na forum międzynarodowym, zwłaszcza inicjatywa Zgromadzenia Ogólnego ONZ z grudnia 2019 r. zmierzająca do przyjęcia nowej umowy międzynarodowej o globalnym, powszechnym zasięgu, regulującej kwestie bezpieczeństwa w cyberprzestrzeni.

Istotny nacisk w niniejszym badaniu zostanie położony w szczególności na działania zmierzające do poprawy bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej. Po pierwsze – Rzeczpospolita Polska, zaliczająca się do cywilizacji zachodniej, dysponującej rozwiniętą siecią urządzeń i połączeń teleinformatycznych, za których pośrednictwem są realizowane codzienne transakcje, obsługiwane są systemy wchodzące w skład infrastruktury krytycznej państwa.

Po drugie – Rzeczpospolita Polska jest pełnoprawnym członkiem wspólnoty zachodnich państw rozwiniętych i członkiem Unii Europejskiej. W związku z tym bliższe spojrzenie na europejskie regulacje regionalne w tej materii dadzą obraz bezpieczeństwa cybernetycznego z polskiej perspektywy.

Działania Unii Europejskiej w walce z cyberprzestępczością obejmują po pierwsze, aktywność regulacyjną (prawodawczą) zarówno w ramach samej Unii, jak i w sferze stosunków międzynarodowych, w relacjach z państwami spoza Unii i spoza kontynentu europejskiego. Po drugie, Unia Europejska podejmuje działalność operacyjną polegającą na realizacji konkretnych projektów mających przyczynić się do ograniczenia zjawiska przestępczości komputerowej.

Państwa członkowskie Unii Europejskiej coraz wyraźniej dostrzegają zagrożenia płynące ze strony przestępców komputerowych, którzy, jak pokazuje praktyka, coraz częściej działają w zorganizowanych grupach przestępczych. Próbując przeciwdziałać temu zjawisku na szczeblu unijnym organy Unii Europejskiej, w szczególności Komisja i Rada, angażują się w proces zmierzający do usprawnienia i ujednolicenia instrumentarium prawnego mającego przyczynić się do zwalczania cyberprzestępczości. W tym celu organizują różne projekty badawcze i informacyjne. Ponadto Komisja organizuje spotkania ekspertów, konferencje z udziałem specjalistów zajmujących się cyberprzestępczością z krajów członkowskich Unii Europejskiej, EUROPOL-u (*European Police Office*), CEPOL-u (*European Police College*), czy EJTN-u (*European Judicial Training Network*).

Ciekawą inicjatywą Komisji Europejskiej jest stworzona przez nią sieć kontaktowa krajowych organów odpowiedzialnych za walkę ze *spamem – Contact Network of Spam Authorities* (CNSA), która regularnie odbywa posiedzenia, na których dochodzi do wymiany spostrzeżeń na temat sprawdzonych rozwiązań i współpracy w zakresie egzekwowania prawa.

Problematyka bezpieczeństwa w cyberprzestrzeni stanowi głównie przedmiot zainteresowania państw wysoko rozwiniętych, państw uprzemysłowionych, posiadających wiedzę i technologie umożliwiające rozwijanie i korzystanie z narzędzi teleinformatycznych w codziennej wymianie informacji i obsłudze ważnych sektorów administracji i gospodarki państwa. Współcześnie, zinformatyzowanie

działalności struktur państwa i funkcjonowania gospodarki stało się udziałem społeczeństw posiadających niezbędny kapitał pozwalający na wykształcenie kadr naukowo-technicznych i stworzenie technologii, które chociażby ze względu na swoją innowacyjność są stosunkowo drogie, a co za tym idzie dostęp do nich jest ograniczony przez czynnik finansowy. Bogate i wykształcone społeczeństwa intensywnie informatyzują się w ostatnich latach kreując tym samym nową międzynarodową rzeczywistość, w której państwa i społeczeństwa pozbawione (na skutek uwarunkowań politycznych, historycznych czy geograficznych) możliwości uczestnictwa w tym swoistym wyścigu informatycznym (rewolucji informacyjnej) pozostają w tyle globalnej rywalizacji. Na tym tle zaciera się, lub przynajmniej ma szansę zatrzeć się tradycyjny podział wschód – zachód, czy północ – południe. W związku z obserwowanym współcześnie w państwach rozwiniętych przesunięciem źródeł dobrobytu z przemysłu ciężkiego i produkcji towarowej angażującej znaczną liczbę pracowników na *know-how*, i gospodarkę opartą na usługach i produkcji zautomatyzowanej wymagającej dla swej obsługi wysoko wykwalifikowanych specjalistów, to wiedza i wykształcenie stają się głównymi determinantami rozwoju i pomyślności współczesnych społeczeństw.

Państwa i społeczeństwa, które pozostają w tyle międzynarodowej rywalizacji teleinformatycznej często nie zdają sobie sprawy z konieczności przewartościowania priorytetów rozwojowych i przekierowania środków publicznych w celu rozwijania edukacji, nauki i pozyskiwania wiedzy i zaawansowanych technologii. Nie zdają sobie sprawy lub, co bardziej prawdopodobne, borykają się z podstawowymi problemami rozwojowymi, takimi jak zapewnienie stabilności politycznej i bezpieczeństwa militarnego, czy wykreowanie przejrzystego systemu gospodarczego pozwalającego na aktywizację ludzkiej przedsiębiorczości oraz zbudowanie sprawnego sektora administracji publicznej wolnego od korupcji. Państwa i społeczeństwa takie pozostają w znacznej mierze niezinformatyzowane, a co za tym idzie nie interesuje ich międzynarodowa współpraca w zwalczaniu zagrożeń w cyberprzestrzeni, jako że te zagrożenia ich bezpośrednio nie dotyczą. Jest to podwójnie niebezpieczne zjawisko. Po pierwsze – tworzy się nowa oś podziału świata na państwa i społeczeństwa zinformatyzowane, korzystające z nowoczesnych technologii i pomnażające

dzięki temu swój dobrobyt. Po drugie – państwa, które nie uczestniczą w międzynarodowej współpracy na rzecz bezpieczeństwa w cyberprzestrzeni stanowią tzw. czarne dziury, w których mogą pojawić się niekontrolowane patologie rzutujące na bezpieczeństwo globalnej sieci informatycznej. W szczególności mogą stanowić miejsca koncentracji organizacji przestępczych i terrorystycznych prowadzących swoje ataki cybernetyczne przeciwko państwom i społeczeństwom wysoko rozwiniętym, godząc w ich obywateli, czy wrażliwe systemy bezpieczeństwa.

Przechodząc w tym miejscu do krótkiej charakterystyki obowiązujących na arenie międzynarodowej regulacji prawnych w pierwszej kolejności należy wskazać, że najważniejszym, skupiającym największą liczbę państw, dokumentem wiążącym rangi międzynarodowej jest Konwencja Rady Europy o cyberprzestępczości uchwalona i wyłożona do podpisu 23 listopada 2001 r. na międzynarodowej konferencji w Budapeszcie. Jest to pierwsza w świecie umowa międzynarodowa poruszająca kompleksowo kwestie przestępczości komputerowej, definiująca przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów, definiująca oszustwa i fałszerstwa komputerowe, przestępstwa związane z pornografią dziecięcą, przestępstwa związane z naruszaniem praw autorskich i praw pokrewnych, a także określająca formy odpowiedzialności i rodzaje sankcji.

Konwencja stanowi owoc ponad czterech lat pracy ekspertów w ramach Rady Europy z udziałem przedstawicieli takich państw jak Stany Zjednoczone Ameryki, Kanada, Japonia, czy Republika Południowej Afryki, które wprawdzie nie są członkami Rady Europy, ale wspólnie z krajami członkowskimi podjęły działania pozwalające skuteczniej walczyć ze zjawiskiem cyberprzestępczości.

Umowa ta stanowi jak do tej pory najefektywniejsze narzędzie międzynarodowej ochrony wszystkich podmiotów, które wykorzystują technologie komputerowe lub w stosunku do których technologie te umożliwiają lub ułatwiają popełnianie przestępstw. Jak pokazuje praktyka szereg państw nie będących członkami Rady Europy ani stronami Konwencji o cyberprzestępczości traktuje ją jako wzór do naśladowania i powtarza jej ustalenia w swoich wewnętrznych porządkach prawnych.

Postanowienia Konwencji można podzielić na następujące zasadnicze grupy:

- Normy prawa karnego materialnego – zawierające definicje pojęć i określające znamiona przestępstw (art. 1–13). W ramach tej grupy przepisów zdefiniowano cztery rodzaje cyberprzestępstw:
  - przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów,
  - przestępstwa komputerowe,
  - przestępstwa ze względu na charakter zawartych informacji,
  - przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych,
- Normy prawa karnego procesowego – określające procedury postępowania w sprawach dotyczących przestępstw określonych w Konwencji i innych przestępstw popełnionych przy wykorzystaniu systemu informatycznego oraz zbierania dowodów w formie elektronicznej odnoszących się do tych przestępstw (art. 14–21),
- Regulacje dotyczące jurysdykcji nad przestępstwami określonymi w Konwencji (art. 22),
- Postanowienia dotyczące współpracy międzynarodowej w zakresie ekstradycji i wzajemnej pomocy prawnej oraz wymiany informacji (art. 23–35),
- Postanowienia końcowe (art. 36–48).

Pierwsza grupa wskazanych przepisów zawiera definicje cyberprzestępstw. Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów zawierają definicje takich przestępstw jak: nielegalny dostęp (umyślny, bezprawny dostęp do całości lub części systemu informatycznego; państwo strona może wprowadzić dodatkowy wymóg, 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 innym systemem informatycznym), nielegalne przechwytywanie danych (umyślne, bezprawne przechwytywanie danych za 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; państwo strona może wprowadzić dodatkowy wymóg,

że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym), naruszenie integralności danych (umyślne, bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych; państwo strona może rozszerzyć powyższą definicję o stwierdzenie, że takie zachowanie musi skutkować poważną szkodą), naruszenie integralności systemu (umyślne, bezprawne poważne zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, transmisję, zniszczenie, wykasowanie, uszkodzenie, dokonanie zmian lub usunięcie danych informatycznych), niewłaściwe użycie urządzeń (umyślna i bezprawna produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnienie urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego dla celów popełnienia któregokolwiek z cyberprzestępstw oraz hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego stanie się dostępna z zamiarem wykorzystania dla celów popełnienia któregokolwiek z cyberprzestępstw; umyślne i bezprawne posiadanie urządzenia lub hasła dostępu z zamiarem wykorzystania ich w celu popełnienia cyberprzestępstwa). Przestępstwa komputerowe zostały zdefiniowane jako: fałszerstwo komputerowe (umyślne, bezprawne wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane na potrzeby postępowania prawnego jako autentyczne, bez względu na to czy są one możliwe do bezpośredniego odczytania i zrozumiałe), oszustwo komputerowe (umyślne, bezprawne spowodowania utraty majątku przez inną osobę poprzez: wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych, lub każdą ingerencję w funkcjonowanie systemu komputerowego, z zamiarem oszustwa lub z nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby). Przestępstwa ze względu na charakter zawartych informacji zawierają następujący katalog: przestępstwa związane z pornografią dziecięcą [umyślne, bezprawne: a) produkowanie pornografii dziecięcej dla celów jej rozpowszechniania za pomocą systemu informatycznego; b) oferowanie lub udostępnianie pornografii dziecięcej za pomocą

systemu informatycznego; c) rozpowszechnianie 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]. Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych nie zostały precyzyjnie zdefiniowane, natomiast stwierdzono, że każde państwo strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym naruszenia prawa autorskiego zdefiniowane 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.

Druga grupa wskazanych przepisów zawiera normy prawa karnego procesowego – określające procedury postępowania w sprawach dotyczących przestępstw określonych w Konwencji i innych przestępstw popełnionych przy wykorzystaniu systemu informatycznego oraz zbierania dowodów w formie elektronicznej odnoszących się do tych przestępstw. Już na wstępie części proceduralnej stwierdzono, że każde państwo strona powinno zapewnić, że ustanowienie, wdrożenie i stosowanie uprawnień i procedur, o jakich mowa w części proceduralnej Konwencji, powinno zagwarantować odpowiednią ochronę wolności i praw człowieka, w tym praw wynikających – zgodnie z podjętymi zobowiązaniami – z Konwencji Rady Europy z 1950 r. o ochronie praw człowieka i podstawowych wolności, Międzynarodowego paktu Narodów Zjednoczonych z 1966 r. o prawach obywatelskich i politycznych i innych mających zastosowanie międzynarodowych instrumentów z zakresu praw człowieka. Takie warunki i gwarancje powinny obejmować, stosownie do rodzaju danego uprawnienia lub procedury, m.in. sądową lub inną niezależną kontrolę, podawanie uzasadnienia dla ich stosowania, ograniczenia co do zakresu i czasu stosowania takich uprawnień i procedur. W zakresie, w jakim jest to zgodne z interesem