DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 27 maja 2015 r.

Poz. 728

KONWENCJA

Rady Europy o cyberprzestępczości,

sporządzona w Budapeszcie dnia 23 listopada 2001 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 23 listopada 2001 r. w Budapeszcie została sporządzona Konwencja Rady Europy o cyberprzestępczości, w następującym brzmieniu:

Przekład

Konwencja Rady Europy o cyberprzestępczości

Preambuła

Państwa członkowskie Rady Europy i inne Państwa Sygnatariusze niniejszej konwencji,

biorąc pod uwagę, że celem Rady Europy jest osiągnięcie większej jedności między jej członkami;

uznając wartość wspierania współpracy z innymi Państwami Sygnatariuszami niniejszej konwencji;

przekonane o potrzebie prowadzenia, jako kwestii priorytetowej, wspólnej polityki kryminalnej mającej na celu ochronę społeczeństwa przed cyberprzestępczością, między innymi poprzez przyjęcie właściwych przepisów prawnych i wspieranie międzynarodowej współpracy;

świadome głębokich zmian dokonanych na skutek digitalizacji, konwergencji i trwającej globalizacji sieci informatycznych;

zaniepokojone ryzykiem, że sieci informatyczne i informacje elektroniczne mogą być także wykorzystywane w celu popełniania przestępstw oraz że dowód w sprawie takich przestępstw może być przechowywany i przekazywany za pomocą tych sieci;

uznając potrzebę współpracy między państwami i przemysłem prywatnym w zwalczaniu cyberprzestępczości oraz potrzebę ochrony prawnie uzasadnionych interesów w stosowaniu i rozwoju technologii informatycznych;

zdając sobie sprawę, że skuteczna walka z cyberprzestępczością wymaga zwiększonej, szybkiej i dobrze funkcjonującej współpracy międzynarodowej w sprawach karnych;

przekonane, że niniejsza konwencja jest niezbędna dla powstrzymania działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowemu wykorzystywaniu tych systemów, sieci i danych, poprzez uznanie takiego postępowania za przestępstwo, zgodnie z niniejszą konwencją, oraz przyjęcia środków, które będą przydatne w skutecznym zwalczaniu takich przestępstw, poprzez ułatwienie ich wykrywania, prowadzenia dochodzenia i ścigania zarówno na szczeblu krajowym, jak i międzynarodowym, oraz poprzez przyjęcie rozwiązań sprzyjających szybkiej i rzetelnej współpracy międzynarodowej;

pamiętając o konieczności zagwarantowania równowagi pomiędzy egzekwowania prawa a poszanowaniem podstawowych praw człowieka, zgodnie z Konwencją Rady Europy z 1950 roku o Ochronie Praw Człowieka i Podstawowych Wolności oraz Międzynarodowym Paktem Praw Obywatelskich i Politycznych z 1966 roku, jak również innymi traktatami odnoszącymi się do praw człowieka, które potwierdzają prawo każdej jednostki do swobodnego wyrażania opinii, jak również prawo do wolności wypowiedzi, łącznie z wolnością poszukiwania, uzyskiwania i dzielenia się wszelkiego rodzaju informacjami i ideami, bez względu na granice, oraz prawo do poszanowania prywatności;

pamiętając także o prawie do ochrony danych osobowych, przewidzianym np. w Konwencji Rady Europy z 1981 roku o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych;

mając na uwadze Konwencję Narodów Zjednoczonych z 1989 roku o prawach dziecka oraz Konwencję Międzynarodowej Organizacji Pracy z 1999 roku o dotyczącą zakazu i natychmiastowych działań na rzecz eliminowania najgorszych form pracy dzieci;

biorąc pod uwagę istniejące konwencje Rady Europy dotyczące współpracy w dziedzinie spraw karnych, jak również podobne traktaty, które istnieją pomiędzy państwami członkowskimi Rady Europy i innymi państwami oraz podkreślając, że niniejsza konwencja ma na celu uzupełnienie tych konwencji dla zwiększenia skuteczności dochodzeń w sprawach karnych i postępowań dotyczących przestępstw związanych z systemami informatycznymi i danymi, oraz umożliwienie zbierania elektronicznych materiałów dowodowych dotyczących przestępstw;

przyjmując z zadowoleniem ostatnie osiągnięcia sprzyjające dalszemu pogłębianiu zrozumienia i współpracy międzynarodowej w zwalczaniu cyberprzestępczości, łącznie z działaniami Narodów Zjednoczonych, OECD, Unii Europejskiej i G8;

przywołując Zalecenie nr R(85)10 dotyczące praktycznego stosowania Europejskiej konwencji o pomocy prawnej w sprawach karnych w odniesieniu do wniosków rekwizycyjnych dotyczących podsłuchu rozmów telefonicznych, na Zalecenie nr R(88)2 w sprawie naruszeń w dziedzinie prawa autorskiego i praw pokrewnych, na Zalecenie nr R(87)15 dotyczące wykorzystywania danych osobowych w sektorze policji, na Zalecenie nr R(95)4 o ochronie danych osobowych w sferze usług telekomunikacyjnych ze szczególnym uwzględnieniem usług telefonicznych, jak również na Zalecenie nr R(89)9 w sprawie przestępstw komputerowych, które zawiera wytyczne dla legislacji krajowych dotyczące definicji pewnych przestępstw komputerowych, oraz na Zalecenie nr R(95)13 w sprawie problemów prawa karnego procesowego związanych z technologią informatyczną;

biorąc pod uwagę Rezolucję nr 1 przyjętą przez Europejskich Ministrów Sprawiedliwości na ich 21 Konferencji (Praga, 10-11 czerwca 1997 roku), która zaleciła Komitetowi Ministrów wspieranie prac prowadzonych przez Europejski Komitet ds. Przestępczości (CDPC) w zakresie cyberprzestępczości, w celu wzajemnego zbliżenia postanowień w zakresie prawa karnego oraz umożliwienia stosowania efektywnych środków ścigania takich przestępstw, jak również Rezolucję nr 3 przyjętą na 23 Konferencji Europejskich Ministrów Sprawiedliwości (Londyn, 8-9 czerwca 2000 roku), która zachęcała negocjujące strony do kontynuowania ich wysiłków mających na celu znalezienie właściwych rozwiązań, które umożliwiłyby przystąpienie do Konwencji jak największej liczbie państw, oraz uświadomiła potrzebę szybkiego i efektywnego systemu współpracy międzynarodowej, uwzględniającej należycie szczególne wymagania walki z cyberprzestępczością;

mając również na uwadze Plan Działania przyjęty przez szefów państw i rządów Rady Europy podczas ich Drugiego Szczytu (Strasburg, 10-11 października 1997 roku), w celu znalezienia wspólnej odpowiedzi na rozwój nowych technologii, opartej na standardach i wartościach Rady Europy;

uzgodniły co następuje:

ROZDZIAŁ I

TERMINOLOGIA

Artykuł 1

Definicje

Dla celów niniejszej konwencji:

a. „system informatyczny" oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych;

b. „dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny;

c. „dostawca usług" oznacza:

   i. dowolny podmiot prywatny lub publiczny, który umożliwia użytkownikom jego usług komunikowanie się za pomocą systemu informatycznego, oraz

   ii. dowolny inny podmiot, który przetwarza lub przechowuje dane informatyczne w imieniu takich usług komunikacyjnych lub użytkowników takich usług.

d. „dane dotyczące ruchu" oznaczają dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazujące swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę, rozmiar, czas trwania lub rodzaj danej usługi.

ROZDZIAŁ II

ŚRODKI, JAKIE NALEŻY PODJĄĆ NA SZCZEBLU KRAJOWYM

Część 1

Prawo karne materialne

Tytuł 1

Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów

Artykuł 2

Nielegalny dostęp

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego. Strona może wprowadzić 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.

Artykuł 3

Nielegalne przechwytywanie danych

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego przechwytywania 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. Strona może wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym.

Artykuł 4

Naruszenie integralności danych

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych.
2. Strona może zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie 1 musi skutkować poważną szkodą.

Artykuł 5

Naruszenie integralności systemu

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych.

Artykuł 6

Niewłaściwe użycie urządzeń

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnych i bezprawnych:
   a. produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:
      i. urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5;
      ii. hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna,

   z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5; oraz

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

2. Niniejszego artykułu nie należy interpretować jako mającego na celu pociągnięcie do odpowiedzialności karnej w przypadku, kiedy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie, o którym mowa w ustępie 1 niniejszego artykułu, nie jest dokonywane w celu popełnienia przestępstwa określonego zgodnie z artykułami 2-5 niniejszej konwencji, jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego.

3. Każda Strona może zastrzec sobie prawo do niestosowania ustępu 1 niniejszego artykułu, pod warunkiem, że zastrzeżenie to nie dotyczy sprzedaży, dystrybucji lub innego udostępniania jednostek wymienionych w ustępie 1.a.ii.

Tytuł 2

Przestępstwa komputerowe

Artykuł 7

Fałszerstwo komputerowe

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego, bezprawnego wprowadzania, dokonywania zmian, wykasowywania lub ukrywania 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. Strona może wprowadzić wymóg, że odpowiedzialność karna dotyczy działania w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze.

Artykuł 8

Oszustwo komputerowe

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania

za przestępstwa w jej prawie wewnętrznym, umyślnego, bezprawnego spowodowania utraty majątku przez inną osobę poprzez:

a. wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych,

b. każdą ingerencję w funkcjonowanie systemu komputerowego,

z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.

Tytuł 3

Przestępstwa ze względu na charakter zawartych informacji

Artykuł 9

Przestępstwa związane z pornografią dziecięcą

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego i bezprawnego:

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

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

   c. rozpowszechniania lub transmitowania pornografii dziecięcej za pomocą systemu informatycznego;

   d. pozyskiwania pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby;

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

2. Dla celów powyższego ustępu 1 pojęcie „pornografia dziecięca" obejmuje materiał pornograficzny, który w sposób widoczny przedstawia:

   a. osobę małoletnią w trakcie czynności wyraźnie seksualnej;

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

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

3. Dla celów powyższego ustępu 2, pojęcie „osoba małoletnia" obejmuje wszystkie osoby poniżej 18 roku życia. Strona może wprowadzić wymóg niższej granicy wieku, która nie może być niższa niż 16 lat.

4. Każda ze Stron może zastrzec sobie prawo niestosowania, w całości lub w części, ustępu 1.d i e oraz ustępu 2.b i c.

Tytuł 4

Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych

Artykuł 10

Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, naruszeń prawa autorskiego zdefiniowanego 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.

2. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, naruszeń praw pokrewnych zdefiniowanych w prawie danej Strony, zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Międzynarodowej konwencji o ochronie wykonawców, producentów fonogramów i organizacji nadawczych zawartej w Rzymie (Konwencja Rzymska), Umowy w sprawie

handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o wykonaniach i fonogramach, z wyłączeniem praw osobistych przewidzianych przez te konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego.

3. Strona może zastrzec sobie prawo do niepociągania do odpowiedzialności karnej na podstawie ustępów 1 i 2 niniejszego artykułu w pewnych przypadkach, pod warunkiem, że istnieją inne skuteczne środki prawne oraz że zastrzeżenie to nie stanowi odstępstwa od międzynarodowych zobowiązań Strony określonych w międzynarodowych instrumentach, wymienionych w ustępach 1 i 2 niniejszego artykułu.

Tytuł 5

Inne formy odpowiedzialności i sankcje

Artykuł 11

Usiłowanie i pomocnictwo lub podżeganie

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego pomocnictwa lub podżegania do popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-10 niniejszej konwencji.

2. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym umyślnego usiłowania popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 3-5, 7, 8, 9 ust. 1.a oraz 9 ust. 1.c niniejszej konwencji.

3. Każde państwo może zastrzec sobie prawo do niestosowania, w całości lub w części, ustępu 2 niniejszego artykułu.

Artykuł 12

Odpowiedzialność osób prawnych

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla zagwarantowania poniesienia odpowiedzialności przez osoby prawne za przestępstwa określone zgodnie z niniejszą konwencją, popełnione dla ich korzyści przez dowolną osobę

fizyczną, działającą samodzielnie bądź jako część organu osoby prawnej, zajmującą w niej pozycję wiodącą z uwagi na:

a. uprawnienia do reprezentowania osoby prawnej;

b. uprawnienia do podejmowania decyzji w imieniu osoby prawnej;

c. uprawnienia do wykonywania wewnętrznej kontroli w ramach osoby prawnej.

2. Oprócz przypadków wymienionych już w ustępie 1 niniejszego artykułu, każda ze Stron podejmie środki niezbędne dla zagwarantowania, że osoba prawna może zostać pociągnięta do odpowiedzialności, gdy brak nadzoru lub kontroli ze strony osoby fizycznej, wymienionej w ustępie 1, umożliwił popełnienie przestępstwa określonego zgodnie z niniejszą konwencją, przez osobę fizyczną dla korzyści tej osoby prawnej.

3. W zależności od zasad prawnych danej Strony, odpowiedzialność osoby prawnej może być karna, cywilna lub administracyjna.

4. Odpowiedzialność taka jest niezależna od odpowiedzialności karnej osób fizycznych, które popełniły przestępstwo.

Artykuł 13

Kary i środki

1. Każda Strona podejmie niezbędne środki prawne lub inne, aby zagwarantować, że przestępstwa określone zgodnie z artykułami 2-11 będą karane za pomocą skutecznych, proporcjonalnych i zniechęcających sankcji, obejmujących pozbawienie wolności.

2. Każda Strona zagwarantuje, że osoby prawne ponoszące odpowiedzialność zgodnie z artykułem 12, podlegać będą skutecznym, proporcjonalnym i zniechęcającym sankcjom lub środkom o charakterze karnym lub innym, w tym sankcjom pieniężnym.

Część 2

Prawo procesowe

Tytuł 1

Przepisy wspólne

Artykuł 14

Zakres przepisów procesowych

1. Każda Strona przyjmie odpowiednie środki prawne i inne, które są niezbędne dla ustanowienia uprawnień i procedur przewidzianych w niniejszej części dla celów prowadzenia specjalnych dochodzeń i postępowań karnych.

2. Za wyjątkiem szczególnych, odmiennych regulacji artykułu 21, każda Strona stosuje środki wymienione w ustępie 1 niniejszego artykułu do:

   a. przestępstw określonych zgodnie z artykułami 2-11 niniejszej konwencji;

   b. wszystkich innych przestępstw popełnionych przy użyciu systemu informatycznego; oraz

   c. zbierania dowodów w formie elektronicznej odnoszących się do przestępstw.

3. a. Każda Strona może sobie zastrzec prawo stosowania środków określonych w artykule 20 wyłącznie do przestępstw lub rodzajów przestępstw wyszczególnionych w zastrzeżeniu, pod warunkiem, że krąg takich przestępstw lub rodzajów przestępstw nie będzie ograniczony bardziej niż krąg przestępstw, do jakich stosuje ona środki określone w artykule 21. Każda Strona powinna rozważyć ograniczenie tego rodzaju zastrzeżenia, aby umożliwić jak najszersze stosowanie środków określonych w artykule 20.

   b. W przypadkach, gdy Strona, z powodu ograniczeń w swoim prawie obowiązującym w czasie przyjęcia niniejszej konwencji, nie jest w stanie stosować środków wskazanych w artykułach 20 i 21 do informacji przekazywanych w ramach systemu informatycznego dostawcy usługi, który to system

      i. funkcjonuje na potrzeby zamkniętej grupy użytkowników i

ii. nie wykorzystuje publicznych sieci komunikacyjnych i nie jest połączony z innym systemem komputerowym publicznym lub prywatnym,

Strona taka może zastrzec sobie prawo do niestosowania tych środków do takich informacji. Każda Strona powinna rozważyć ograniczenie takiego zastrzeżenia, aby umożliwić jak najszersze zastosowanie środków określonych w artykułach 20 i 21.

Artykuł 15

Warunki i zabezpieczenia

1. Każda Strona zapewni, że ustanowienie, wdrożenie i stosowanie uprawnień i procedur, o jakich mowa w niniejszej części, podlega warunkom i gwarancjom przewidzianym w ich prawie wewnętrznym, które powinny zagwarantować odpowiednią ochronę wolności i praw człowieka, w tym praw wynikających – zgodnie z podjętymi zobowiązaniami – z Konwencji Rady Europy z 1950 roku o Ochronie Praw Człowieka i Podstawowych Wolności, Międzynarodowego Paktu Praw Obywatelskich i Politycznych z 1966 roku oraz innych mających zastosowanie międzynarodowych instrumentów z zakresu praw człowieka, i które powinny być oparte na zasadzie proporcjonalności.
2. 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.
3. W zakresie, w jakim jest to zgodne z interesem publicznym, w szczególności z interesem wymiaru sprawiedliwości, każda Strona powinna rozważyć wpływ uprawnień i procedur, o których mowa w tej części, na prawa, obowiązki oraz uzasadnione interesy osób trzecich.

Tytuł 2

Niezwłoczne zabezpieczanie przechowywanych danych informatycznych

Artykuł 16

Niezwłoczne zabezpieczanie przechowywanych danych informatycznych

1. Każda Strona przyjmie środki prawne i inne, które są niezbędne do tego, by umożliwić właściwym organom nakazanie lub uzyskanie przy użyciu podobnych metod,

niezwłocznego zabezpieczenia wyspecyfikowanych danych informatycznych, w tym także danych dotyczących ruchu, przechowywanych przy pomocy systemu informatycznego, w szczególności, gdy istnieją podstawy do tego by sądzić, że dane te są szczególnie podatne na ryzyko utraty lub zmodyfikowania.

2. Jeżeli Strona stosuje ustęp 1 powyżej poprzez nakazanie danej osobie zabezpieczenia wyspecyfikowanych przechowywanych danych informatycznych, znajdujących się w posiadaniu tej osoby lub pod jej kontrolą, to Strona ta powinna przyjąć środki prawne lub inne, które mogą być potrzebne do zobowiązania tej osoby do zabezpieczenia i zachowania całości danych informatycznych przez okres tak długi, jak będzie to konieczne, nie dłużej jednak niż do 90 dni, aby umożliwić właściwym organom podjęcie starań o ich ujawnienie. Strona może przewidzieć późniejszą możliwość odnowienia takiego nakazu.

3. Każda Strona przyjmie środki prawne i inne, które mogą być potrzebne do zobowiązania administratora danych informatycznych lub innej osoby odpowiedzialnej za ich zabezpieczenie, do zachowania tajemnicy co do zastosowania tych procedur przez okres określony w prawie wewnętrznym.

4. Uprawnienia i procedury określone w niniejszym artykule podlegają artykułom 14 i 15.

Artykuł 17

Niezwłoczne zabezpieczenie i częściowe ujawnienie danych dotyczących ruchu

1. W odniesieniu do danych dotyczących ruchu, które należy zabezpieczyć zgodnie z artykułem 16, każda Strona przyjmie środki prawne lub inne, które mogą być potrzebne do:

   a. zapewnienia, że istnieje możliwość takiego niezwłocznego zabezpieczenia danych dotyczących ruchu, niezależnie od tego, czy tylko jeden czy też więcej dostawców usług uczestniczyło w przekazywaniu takich informacji; oraz

   b. zapewnienia niezwłocznego ujawnienia właściwemu organowi Strony lub osobie wyznaczonej przez ten organ, dostatecznej ilości danych dotyczących ruchu, aby umożliwić Stronie identyfikację dostawców usług i kanałów, jakimi przekaz nastąpił.

2. Uprawnienia i procedury wymienione w niniejszym artykule podlegają artykułom 14 i 15.

Tytuł 3

Nakaz dostarczenia

Artykuł 18

Nakaz dostarczenia

1. Każda Strona przyjmie odpowiednie środki prawne i inne, które mogą być potrzebne dla nadania właściwym organom uprawnień do nakazania:

   a. osobie obecnej na terytorium Strony przekazania określonych danych informatycznych, które znajdują się w posiadaniu lub pod kontrolą tej osoby i są przechowywane w systemie informatycznym lub na nośniku służącym do przechowywania danych informatycznych; oraz

   b. dostawcy usług oferowanych na terytorium Strony przekazania informacji odnoszących się do abonenta takich usług, znajdujących się w posiadaniu lub pod kontrolą tego dostawcy usług.

2. Uprawnienia i procedury wymienione w niniejszym artykule podlegają artykułom 14 i 15.

3. Dla celów niniejszego artykułu pojęcie „informacje odnoszące się do abonenta" oznacza wszelkie informacje w postaci danych informatycznych lub w dowolnej innej postaci, znajdujące się w posiadaniu dostawcy usług i odnoszące się do użytkowników tych usług, inne niż dane dotyczące ruchu lub treści, które pozwalają na ustalenie:

   a. rodzaju usług komunikacyjnych, z jakich korzysta użytkownik, zastosowanych w związku z tym rozwiązań technicznych oraz okresu usługi;

   b. tożsamości użytkownika, adresu pocztowego lub geograficznego, numeru telefonu lub innego numeru dostępu, wykazu połączeń i informacji o płatnościach dostępnych na podstawie umowy lub ustaleń dotyczących usługi;

   c. wszelkich innych informacji związanych z miejscem zainstalowania sprzętu komunikacyjnego, dostępnych na podstawie umowy lub ustaleń dotyczących usługi.

Tytuł 4

Przeszukanie i zajęcie przechowywanych danych informatycznych

Artykuł 19

Przeszukanie i zajęcie przechowywanych danych informatycznych

1. Każda Strona przyjmie odpowiednie środki prawne i inne, które mogą być potrzebne dla nadania właściwym organom uprawnień w zakresie przeszukiwania lub uzyskiwania dostępu przy użyciu podobnych metod do:

   a. systemu informatycznego lub jego części oraz do danych informatycznych w nim przechowywanych; oraz

   b. nośnika służącego do przechowywania danych informatycznych na jej terytorium.

2. Każda Strona przyjmie środki prawne i inne, które mogą być potrzebne dla zapewnienia, aby właściwe organy dysponowały odpowiednimi środkami pozwalającymi na niezwłoczne rozszerzenie przeszukania lub podobnych metod uzyskiwania dostępu na inny system, jeżeli podczas dokonywania przez nie przeszukania lub uzyskiwania dostępu przy użyciu podobnych metod do konkretnego systemu informatycznego lub jego części, zgodnie z ustępem 1.a, organy te mają uzasadnione podstawy by sądzić, że poszukiwane dane przechowywane są w innym systemie informatycznym lub w jego części na ich terytorium i że do danych tych można legalnie uzyskać dostęp z systemu pierwotnego lub są one dostępne dla tego systemu.

3. Każda Strona przyjmie środki prawne lub inne, które mogą być potrzebne dla nadania właściwym organom uprawnień do tego, aby mogły zajmować lub zabezpieczać w podobny sposób dane informatyczne, do których uzyskano dostęp zgodnie z ustępami 1 i 2. Środki te obejmują następujące uprawnienia:

   a. zajęcie lub zabezpieczenie w podobny sposób systemu informatycznego lub jego części lub nośnika służącego do przechowywania danych informatycznych;

   b. wykonywanie i zachowywanie kopii tych danych informatycznych;

   c. zachowywanie całości odpowiednich przechowywanych danych informatycznych;

d. uczynienie niedostępnymi lub usunięcie danych informatycznych z danego systemu informatycznego.

4. Każda Strona przyjmie środki prawne lub inne, które mogą być potrzebne dla nadania właściwym organom uprawnień do tego, by mogły nakazać każdej osobie mającej wiedzę o funkcjonowaniu systemu informatycznego lub środkach stosowanych dla zabezpieczenia danych informatycznych zawartych w tym systemie, udostępnienie, o ile jest to uzasadnione, informacji, które są niezbędne dla umożliwienia zastosowania środków, o jakich mowa w ustępach 1 i 2.

5. Uprawnienia i procedury wymienione w niniejszym artykule podlegają artykułom 14 i 15.

Tytuł 5

Gromadzenie w czasie rzeczywistym danych informatycznych

Artykuł 20

Gromadzenie w czasie rzeczywistym danych dotyczących ruchu

1. Każda Strona przyjmie odpowiednie środki prawne i inne, które mogą być potrzebne dla nadania właściwym organom uprawnień w zakresie:

   a. gromadzenia lub rejestrowania przy pomocy środków technicznych istniejących na jej terytorium;

   b. zmuszenia dostawcy usług, aby w ramach możliwości technicznych, jakimi dysponuje:

      i. gromadził lub rejestrował przy pomocy środków technicznych istniejących na jej terytorium, lub

      ii. współpracował i udzielał pomocy właściwym organom przy gromadzeniu lub rejestrowaniu,

   w czasie rzeczywistym, danych dotyczących ruchu, wiążących się z konkretnymi przekazami realizowanymi na jej terytorium przy użyciu środków informatycznych.

2. Jeżeli Strona, z uwagi na zasady jej krajowego porządku prawnego, nie jest w stanie przyjąć środków, o jakich mowa w ustępie 1.a, może w ich miejsce przyjąć środki prawne

lub inne, które mogą być potrzebne dla zapewnienia zbierania lub rejestrowania w czasie rzeczywistym danych dotyczących ruchu wiążących się z konkretnymi przekazami realizowanymi na jej terytorium przez zastosowanie środków technicznych na tym terytorium.

3. Każda Strona przyjmie odpowiednie środki prawne lub inne, które mogą być potrzebne dla zobowiązania dostawcy usług do zachowania w tajemnicy faktu wykonywania uprawnień przewidzianych w niniejszym artykule oraz wszelkich odnoszących się do tego informacji.

4. Uprawnienia i procedury wymienione w niniejszym artykule podlegają artykułom 14 i 15.

Artykuł 21

Przechwytywanie danych dotyczących treści

1. Każda Strona przyjmie odpowiednie środki prawne i inne, które mogą być potrzebne, w odniesieniu do grupy poważnych przestępstw, jakie zostaną określone w prawie wewnętrznym, dla nadania właściwym organom uprawnień w zakresie:

   a. gromadzenia lub rejestrowania przy pomocy środków technicznych istniejących na jej terytorium;

   b. zmuszenia dostawcy usług, aby w ramach możliwości technicznych, jakimi dysponuje:

      i. gromadził lub rejestrował przy pomocy środków technicznych istniejących na jej terytorium, lub

      ii. współpracował i udzielał pomocy właściwym organom przy gromadzeniu lub rejestrowaniu,

      w czasie rzeczywistym, danych dotyczących treści konkretnych przekazów realizowanych na jej terytorium przy użyciu środków informatycznych.

2. Jeżeli któraś ze Stron, z uwagi na zasady jej krajowego porządku prawnego, nie jest w stanie przyjąć środków, o jakich mowa w ustępie 1.a, może w ich miejsce przyjąć środki prawne lub inne, które mogą być potrzebne dla zapewnienia zbierania lub rejestrowania w czasie rzeczywistym danych dotyczących treści konkretnych przekazów realizowanych na jej terytorium przez zastosowanie środków technicznych.

3. Każda Strona przyjmie odpowiednie środki prawne lub inne, które mogą być potrzebne dla zobowiązania dostawcy usług do zachowania w tajemnicy faktu wykonywania uprawnień, o jakich mowa w niniejszym artykule oraz wszelkich odnoszących się do tego informacji.

4. Uprawnienia i procedury wymienione w niniejszym artykule podlegają artykułom 14 i 15.

Część 3

Jurysdykcja

Artykuł 22

Jurysdykcja

1. Każda Strona przyjmie środki prawne lub inne, które mogą być potrzebne dla ustanowienia swojej jurysdykcji w odniesieniu do przestępstw określonych zgodnie z artykułami 2-11 niniejszej konwencji, gdy przestępstwo popełnione jest:

   a. na jej terytorium; lub

   b. na pokładzie statku pływającego pod banderą tej Strony; lub

   c. na pokładzie samolotu zarejestrowanego na podstawie prawa tej Strony; lub

   d. przez jednego z jej obywateli, jeżeli przestępstwo jest karalne według prawa miejsca jego popełnienia lub jeśli przestępstwo popełnione zostało poza jurysdykcją terytorialną jakiegokolwiek państwa.

2. Każde państwo może zastrzec sobie prawo do niestosowania lub stosowania tylko w ściśle określonych przypadkach lub warunkach, zasad jurysdykcji, o jakich mowa w ustępie 1.b-1.d niniejszego artykułu lub w dowolnej części tego ustępu.

3. Każda Strona przyjmie środki, które mogą być potrzebne dla zapewnienia swojej jurysdykcji w odniesieniu do każdego przestępstwa, o jakim mowa w artykule 24 ust. 1 niniejszej konwencji, w przypadkach gdy domniemany sprawca przestępstwa przebywa na jej terytorium i nie może zostać poddany ekstradycji do drugiej Strony wyłącznie ze względu na jego obywatelstwo, po otrzymaniu wniosku ekstradycyjnego.

4. Niniejsza konwencja nie wyłącza jurysdykcji wykonywanej przez Stronę zgodnie z jej

prawem krajowym.

5. Jeżeli kilka Stron uznaje swoją jurysdykcję w odniesieniu do domniemanego przestępstwa określonego w niniejszej konwencji, Strony te, o ile jest to uzasadnione, podejmują konsultacje w celu określenia, czyja jurysdykcja jest najwłaściwsza dla ścigania tego przestępstwa.

ROZDZIAŁ III

WSPÓŁPRACA MIĘDZYNARODOWA

Część 1

Zasady ogólne

Tytuł 1

Ogólne zasady współpracy międzynarodowej

Artykuł 23

Ogólne zasady współpracy międzynarodowej

Strony współpracują zgodnie z postanowieniami niniejszego rozdziału oraz z zastosowaniem właściwych instrumentów międzynarodowych o międzynarodowej współ-pracy w sprawach karnych, porozumień uzgodnionych na podstawie jednolitego lub wzajemnego ustawodawstwa oraz ich prawa krajowego, w sposób możliwie jak najszerszy, dla celów ścigania i prowadzenia postępowań odnoszących się do przestępstw związanych z systemami i danymi informatycznymi lub dla celów zbierania dowodów w postaci elektronicznej, odnoszących się do przestępstw.

Tytuł 2

Zasady dotyczące ekstradycji

Artykuł 24

Ekstradycja

1. a. Niniejszy artykuł stosuje się do ekstradycji między Stronami w związku z przestępstwami określonymi zgodnie z artykułami 2-11 niniejszej konwencji, pod

warunkiem, że są one karalne na podstawie prawa obu zainteresowanych Stron karą pozbawienia wolności w wymiarze co najmniej jednego roku lub większą karą.

b. Jeżeli zgodnie z porozumieniem uzgodnionym na podstawie jednolitego lub wzajemnego ustawodawstwa albo zgodnie z traktatem ekstradycyjnym, w tym Europejską konwencją o ekstradycji (ETS nr 24), obowiązującym między dwiema lub więcej stronami zastosowanie ma inna kara minimalna, stosuje się karę minimalną przewidzianą w takim porozumieniu lub traktacie.

2. Przestępstwa opisane w ustępie 1 niniejszego artykułu uważa się za przestępstwa mogące stanowić podstawę do ekstradycji przewidzianej w dowolnym traktacie ekstradycyjnym obowiązującym między Stronami. Strony zobowiązują się do włączenia takich przestępstw, jako przestępstw stanowiących podstawę do ekstradycji, do wszelkich traktatów ekstradycyjnych, jakie mogą zostać zawarte przez nie lub między nimi.

3. Jeżeli Strona uzależnia ekstradycję od istnienia traktatu i otrzymuje wniosek o ekstradycję od drugiej Strony, z którą nie ma zawartego traktatu ekstradycyjnego, może traktować niniejszą konwencję jako podstawę prawną do ekstradycji w odniesieniu do wszelkich przestępstw, o jakich mowa w ustępie 1 niniejszego artykułu.

4. Strony, które nie uzależniają ekstradycji od istnienia traktatu, uznają przestępstwa wymienione w ustępie 1 niniejszego artykułu, za przestępstwa mogące stanowić w ich wzajemnych stosunkach podstawę do ekstradycji.

5. Ekstradycja podlega warunkom określonym w prawie krajowym Strony wezwanej lub w obowiązujących traktatach ekstradycyjnych, co odnosi się także do przyczyn, dla których Strona wezwana może odmówić ekstradycji.

6. Jeżeli ekstradycja w związku z przestępstwem, o jakim mowa w ustępie 1 niniejszego artykułu, spotyka się z odmową wyłącznie ze względu na obywatelstwo osoby poszukiwanej, lub ze względu na to, że Strona wezwana uznaje swoją jurysdykcję dla danego przestępstwa, Strona wezwana, na wniosek Strony wzywającej, przedkłada sprawę swoim właściwym organom w celu ścigania oraz informuje Stronę wzywającą o sposobie zakończenia sprawy. Organy te podejmują decyzje i prowadzą czynności śledcze i postępowanie w taki sam sposób, jak w przypadku każdego innego przestępstwa

o porównywalnym charakterze, zgodnie z przepisami tej Strony.

7. a. Każda Strona w chwili podpisywania lub składania instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia, poinformuje Sekretarza Generalnego Rady Europy o nazwie i adresie każdego organu odpowiedzialnego za sporządzanie lub przyjmowanie wniosków ekstradycyjnych lub wniosków o tymczasowe aresztowanie w przypadku braku traktatu.

   b. Sekretarz Generalny Rady Europy założy i będzie prowadzić aktualny rejestr organów wyznaczonych przez Strony. Każda Strona powinna zapewnić, że szczegółowe dane zawarte w rejestrze są w każdym czasie miarodajne.

Tytuł 3

Ogólne zasady wzajemnej pomocy prawnej

Artykuł 25

Ogólne zasady dotyczące wzajemnej pomocy prawnej

1. Strony będą świadczyć sobie możliwie jak najdalej idącą pomoc wzajemną dla celów prowadzenia czynności śledczych lub postępowań odnoszących się do przestępstw związanych z systemami i danymi informatycznymi, lub w celu gromadzenia dowodów w postaci elektronicznej, odnoszących się do przestępstw.

2. Każda Strona przyjmie takie środki prawne lub inne, które mogą być potrzebne dla właściwego wywiązania się ze zobowiązań określonych w artykułach 27-35.

3. W nagłych okolicznościach każda Strona może sporządzić wniosek o pomoc wzajemną lub informacje odnoszące się do niego przy pomocy środków szybkiego komunikowania się, w tym faksu lub poczty elektronicznej, o ile środki te zapewniają odpowiedni poziom bezpieczeństwa i gwarancje autentyczności (w tym użycie kodowania, o ile to konieczne) i następnie potwierdzić wniosek oficjalnie, jeśli wymaga tego Strona wezwana. Strona wezwana powinna zaakceptować i odpowiedzieć na taki wniosek przy pomocy środków szybkiego komunikowania się.

4. O ile nie ma wyraźnych, odmiennych postanowień w niniejszym rozdziale, wzajemna pomoc prawna podlega warunkom określonym w prawie krajowym Strony wezwanej lub

w obowiązujących traktach o wzajemnej pomocy prawnej, co dotyczy także przyczyn, dla których Strona wezwana może odmówić współpracy. Strona wezwana nie powinna wykonywać swojego prawa do odmowy współpracy w odniesieniu do przestępstw określonych w artykułach 2-11 tylko na tej podstawie, że wniosek dotyczy przestępstwa, które traktuje ona jako przestępstwo skarbowe.

5. Jeżeli, zgodnie z postanowieniami niniejszego rozdziału, Strona wezwana jest upoważniona do uzależniania udzielenia pomocy wzajemnej od istnienia podwójnej karalności, warunek ten należy uważać za spełniony, jeżeli przestępcze zachowanie, w związku z którym złożono wniosek o pomoc, stanowi przestępstwo według prawa tej Strony, niezależnie od tego, czy prawo to klasyfikuje dane przestępstwo w tej samej kategorii przestępstw lub czy opisuje je przy użyciu tej samej terminologii, co prawo Strony wzywającej.

Artykuł 26

Informacja z własnej inicjatywy

1. Każda Strona może, w granicach wynikających z jej prawa krajowego i bez wcześniejszego wniosku, przekazywać drugiej Stronie informacje uzyskane w ramach swoich własnych działań śledczych, jeżeli uzna, że ujawnienie takich informacji może pomóc tej Stronie w podjęciu lub prawidłowym przeprowadzeniu czynności śledczych lub postępowań związanych z przestępstwami określonych zgodnie z niniejszą konwencją lub gdy informacje te mogłyby doprowadzić do sporządzenia przez tę Stronę wniosku o współpracę na podstawie niniejszego rozdziału.
2. Przed przekazaniem takich informacji Strona dostarczająca informacje może zażądać, aby pozostały one poufne lub były wykorzystywane tylko pod pewnymi warunkami. Jeżeli Strona otrzymująca informacje nie może spełnić tego żądania, powinna poinformować o tym drugą Stronę, która wówczas winna zadecydować, czy pomimo to informacje należy przekazać. Jeżeli Strona otrzymująca informacje zaakceptuje warunki dotyczące wykorzystania informacji, to jest tymi warunkami związana.

Tytuł 4

Procedury związane z wnioskami o udzielenie wzajemnej pomocy prawnej przy braku obowiązujących porozumień międzynarodowych

Artykuł 27

Procedury związane z wnioskami o udzielenie wzajemnej pomocy prawnej przy braku obowiązujących porozumień międzynarodowych

1. W wypadku braku traktatu o wzajemnej pomocy prawnej lub porozumienia opartego na jednolitym lub wzajemnym ustawodawstwie, obowiązujących między Stroną wzywającą i Stroną wezwaną, stosuje się przepisy ustępów 2-9 niniejszego artykułu. Przepisów niniejszego artykułu nie stosuje się, gdy istnieje tego typu traktat, porozumienie lub ustawodawstwo, chyba że zainteresowane Strony postanowią w ich miejsce stosować całość lub część wspomnianych przepisów niniejszego artykułu.

2. a. Każda Strona wyznaczy jeden lub kilka organów centralnych odpowiedzialnych za wysyłanie wniosków o pomoc wzajemną lub za udzielanie odpowiedzi na takie wnioski, ich wykonywanie lub przekazywanie organom właściwym do ich wykonania.

   b. Organy centralne porozumiewają się ze sobą bezpośrednio.

   c. Każda Strona, w chwili podpisania lub złożenia instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia, poinformuje Sekretarza Generalnego Rady Europy o nazwach i adresach organów wyznaczonych zgodnie z niniejszym ustępem.

   d. Sekretarz Generalny Rady Europy założy i będzie prowadzić aktualny rejestr organów centralnych wyznaczonych przez Strony. Każda Strona powinna zapewnić, że szczegółowe dane zawarte w rejestrze są w każdym czasie miarodajne.

3. Wnioski o pomoc wzajemną na podstawie niniejszego artykułu wykonuje się zgodnie z procedurą określoną przez Stronę wzywającą, chyba że jest ona niezgodna z prawem Strony wezwanej.

4. Poza wypadkami przewidzianymi w artykule 25 ust. 4 Strona wezwana może odmówić pomocy wzajemnej w następujących przypadkach:

   a. jeżeli wniosek dotyczy przestępstwa, które Strona wezwana uważa za polityczne lub

związane z przestępstwem politycznym;

b. jeżeli Strona wezwana uważa, że realizacja wniosku może stanowić zagrożenie dla jej suwerenności, bezpieczeństwa, porządku publicznego lub innych podstawowych interesów.

5. Strona wezwana może odroczyć wykonanie czynności określonej we wniosku, jeżeli taka czynność mogłaby spowodować szkodę dla czynności śledczych lub postępowań prowadzonych przez organy tej Strony.

6. Przed odmową lub odroczeniem wykonania wniosku o pomoc Strona wezwana powinna, o ile to uzasadnione po przeprowadzeniu konsultacji ze Stroną wzywającą, rozważyć częściowe wykonanie wniosku lub wykonanie pod pewnymi warunkami, które uzna na nieodzowne.

7. Strona wezwana winna niezwłocznie poinformować Stronę wzywającą o sposobie wykonania wniosku o pomoc. W przypadku odmowy wykonania wniosku lub odroczenia jego wykonania, winna uzasadnić swoją odmowę lub odroczenie. Strona wezwana winna również poinformować Stronę wzywającą o wszelkich przyczynach, które powodują, że wniosek nie może zostać wykonany lub które mogą w sposób znaczący opóźnić jego wykonanie.

8. Strona wzywająca może zażądać, aby Strona wezwana zachowała w tajemnicy fakt złożenia wniosku na podstawie niniejszego rozdziału oraz jego treść, z wyłączeniem tego, co niezbędne dla wykonania tego wniosku. Jeżeli Strona wezwana nie może zastosować się do żądania zachowania tajemnicy, powinna niezwłocznie poinformować o tym Stronę wzywającą, która wówczas winna zadecydować, czy pomimo to wniosek należy wykonać.

9. a. W pilnych przypadkach wnioski o pomoc wzajemną lub związane z nimi informacje organy sądownicze Strony wzywającej mogą kierować bezpośrednio do takich organów Strony wezwanej. W każdym takim przypadku należy jednocześnie skierować kopię pisma do organu centralnego Strony wezwanej za pośrednictwem organu centralnego Strony wzywającej.

b. Każdy wniosek lub informacja sporządzone na podstawie niniejszego ustępu mogą być przekazane za pośrednictwem Międzynarodowej Organizacji Policji Kryminalnej

(Interpol).

c. Jeżeli wniosek został skierowany na podstawie punktu a. niniejszego ustępu, a organ nie jest właściwy do jego załatwienia, przekazuje go właściwemu organowi krajowemu, informując o tym bezpośrednio Stronę wzywającą.

d. Wnioski lub informacje sporządzane na podstawie niniejszego punktu, niewymagające stosowania środków przymusu, mogą być przekazywane bezpośrednio przez właściwe organy Strony wzywającej do właściwych organów Strony wezwanej.

e. Każda Strona, w chwili podpisywania lub składania instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia, może poinformować Sekretarza Generalnego Rady Europy, że ze względu na konieczność zapewnienia skuteczności, wnioski sporządzane na podstawie niniejszego ustępu należy kierować do jej organu centralnego.

Artykuł 28

Poufność i ograniczenia dotyczące wykorzystania informacji

1. W wypadku braku traktatu o wzajemnej pomocy prawnej lub porozumienia na podstawie jednolitego lub wzajemnego ustawodawstwa obowiązujących między Stroną wzywającą i Stroną wezwaną, stosuje się przepisy niniejszego artykułu. Przepisów niniejszego artykułu nie stosuje się, gdy istnieje tego typu traktat, porozumienie lub ustawodawstwo, chyba że zainteresowane Strony postanowią w ich miejsce stosować całość lub część wspomnianych przepisów niniejszego artykułu

2. Strona wezwana może uzależnić przekazanie informacji lub materiałów w odpowiedzi na wniosek od następujących warunków:

   a. zachowania poufności, gdy bez spełnienia tego warunku wniosek o wzajemną pomoc prawną nie mógłby zostać wykonany, lub

   b. nie wykorzystywania tych informacji lub materiałów na użytek czynności śledczych lub postępowań innych niż wymienione we wniosku.

3. Jeżeli Strona wzywająca nie może spełnić warunków określonych w ustępie 2, winna niezwłocznie poinformować o tym Stronę wzywaną, która winna wówczas zadecydować

czy pomimo to informacje należy przekazać. Jeżeli Strona wzywająca zaakceptuje warunki, to jest tymi warunkami związana.

4. Każda Strona przekazująca informacje lub materiały pod warunkami, o jakich mowa w ustępie 2, może zażądać od drugiej Strony wyjaśnienia, w jaki sposób – w kontekście tych warunków – informacje lub materiały zostały wykorzystane.

Część 2

Postanowienia szczegółowe

Tytuł 1

Wzajemna pomoc prawna w zakresie środków tymczasowych

Artykuł 29

Niezwłoczne zabezpieczanie przechowywanych danych informatycznych

1. Strona może zwrócić się do drugiej Strony z wnioskiem o nakazanie lub uzyskanie przy użyciu podobnych metod niezwłocznego zabezpieczenia danych przechowywanych w systemie informatycznym, znajdującym się na terytorium drugiej Strony, w stosunku do których Strona wzywająca ma zamiar złożyć wniosek o pomoc wzajemną dotyczący przeszukania lub uzyskania dostępu przy użyciu podobnych metod, zajęcia lub podobnego zabezpieczenia albo ujawnienia danych.
2. Wniosek o zabezpieczenie, złożony na mocy ustępu 1, powinien zawierać następujące elementy:
   a. organ wnoszący o zabezpieczenie;
   b. przestępstwo stanowiące przedmiot czynności śledczych lub postępowania oraz krótki opis związanych z nim faktów;
   c. przechowywane dane informatyczne, które należy zabezpieczyć i ich związek z przestępstwem;
   d. wszelkie dostępne informacje pozwalające na zidentyfikowanie osoby odpowiedzialnej za przechowywanie danych informatycznych lub lokalizację systemu informatycznego;

e. uzasadnienie dla zabezpieczenia; oraz

f. wskazanie, że Strona zamierza złożyć wniosek o pomoc wzajemną dotyczący przeszukania lub uzyskania dostępu przy użyciu podobnych metod, zajęcia lub podobnego zabezpieczenia albo ujawnienia przechowywanych danych informatycznych.

3. Po otrzymaniu wniosku drugiej Strony, Strona wezwana podejmie wszelkie odpowiednie środki, aby niezwłocznie zabezpieczyć wyszczególnione dane, zgodnie z przepisami swojego prawa krajowego. Dla celów wykonania wniosku, podwójna karalność nie jest wymagana jako warunek przeprowadzenia zabezpieczenia.

4. Strona wymagająca podwójnej karalności jako warunku wykonania wniosku o pomoc wzajemną dotyczącego przeszukania lub uzyskania dostępu przy użyciu podobnych metod, zajęcia lub podobnego zabezpieczenia albo ujawnienia przechowywanych danych, może, w odniesieniu do przestępstw innych niż określone w artykułach 2-11 niniejszej konwencji, zastrzec sobie prawo odmowy wykonania wniosku o zabezpieczenie na podstawie niniejszego artykułu w przypadkach, gdy ma podstawy sądzić, że w chwili ujawnienia warunek podwójnej karalności nie będzie mógł zostać spełniony.

5. Ponadto, można odmówić wykonania wniosku o zabezpieczenie wyłącznie w następujących przypadkach:

   a. jeżeli wniosek odnosi się do przestępstwa, które Strona wezwana uważa za mające charakter polityczny lub za związane z przestępstwem o charakterze politycznym;

   b. jeżeli Strona wezwana uważa, że wykonanie wniosku może stanowić zagrożenie dla jej suwerenności, bezpieczeństwa, porządku publicznego lub innych podstawowych interesów.

6. Jeżeli Strona wezwana uzna, że zabezpieczenie nie zapewni przyszłej dostępności danych albo zagrozi poufności lub w inny sposób zaszkodzi czynnościom śledczym prowadzonym przez Stronę wzywającą, powinna poinformować o tym niezwłocznie Stronę wzywającą, która wówczas winna zadecydować, czy pomimo to wniosek należy wykonać.

7. Każde zabezpieczenie przeprowadzone w wykonaniu wniosku, o jakim mowa w ustępie 1, będzie obowiązywać przez okres co najmniej 60 dni, aby umożliwić Stronie wzywającej

złożenie wniosku o dokonanie przeszukania lub uzyskanie dostępu przy użyciu podobnych metod, zajęcie lub podobne zabezpieczenie albo ujawnienie danych. Po otrzymaniu takiego wniosku dane należy przechowywać w dalszym ciągu w oczekiwaniu na decyzję dotyczącą wniosku.

Artykuł 30

Niezwłoczne ujawnienie przechowywanych danych

1. Jeżeli podczas wykonywania wniosku złożonego na podstawie artykułu 29 o zabezpieczenie danych dotyczących ruchu, odnoszących się do konkretnego przekazu, Strona wezwana odkryje, że dostawca usług w innym państwie uczestniczył w tym przekazie, Strona wezwana niezwłocznie ujawni Stronie wzywającej dostateczną ilość danych dotyczących ruchu, które pozwolą na identyfikację dostawcy usług oraz drogi, jaką przekaz został zrealizowany.
2. Można odmówić ujawnienia danych dotyczących ruchu, o których mowa w ust. 1, wyłącznie w następujących przypadkach:
   a. jeżeli wniosek odnosi się do przestępstwa, które Strona wezwana uważa za mające charakter polityczny lub za związane z przestępstwem o charakterze politycznym, lub
   b. jeżeli Strona wezwana uważa, że wykonanie wniosku może stanowić zagrożenie dla jej suwerenności, bezpieczeństwa, porządku publicznego lub innych podstawowych interesów.

Tytuł 2

Wzajemna pomoc prawna odnosząca się do środków śledczych

Artykuł 31

Wzajemna pomoc prawna odnosząca się do dostępu do przechowywanych danych informatycznych

1. Strona może zwrócić się do drugiej Strony z wnioskiem o przeszukanie lub uzyskanie dostępu przy użyciu podobnych metod, zajęcie lub podobne zabezpieczenie albo ujawnienie danych przechowywanych przy użyciu systemu informatycznego, znajdującego się na terytorium Strony wezwanej, w tym także danych zabezpieczonych

zgodnie z artykułem 29.

2. Strona wezwana wykonuje wniosek stosując instrumenty międzynarodowe, porozumienia i ustawodawstwo, o jakich mowa w artykule 23, oraz zgodnie z odpowiednimi przepisami niniejszego rozdziału.

3. Wniosek należy wykonać w trybie przyspieszonym, jeżeli:

   a. istnieją podstawy, aby sądzić, że odpowiednie dane są szczególnie narażone na ryzyko utraty lub modyfikacji, lub

   b. instrumenty, porozumienia i ustawodawstwo, o jakich mowa w ustępie 2, przewidują inne przypadki współpracy w trybie przyspieszonym.

Artykuł 32

Ponadgraniczny dostęp do przechowywanych danych, za zgodą lub gdy są one publicznie dostępne

Strona, bez zezwolenia drugiej Strony, może:

a. uzyskać dostęp do przechowywanych danych informatycznych, które są publicznie dostępne (źródło otwarte), niezależnie od geograficznej lokalizacji tych danych, lub

b. uzyskać dostęp lub otrzymać przy pomocy systemu informatycznego znajdującego się na własnym terytorium dane informatyczne przechowywane na terytorium innego państwa, jeżeli Strona uzyska prawnie skuteczną i dobrowolną zgodę osoby upoważnionej do ujawnienia Stronie tych danych przy pomocy tego systemu informatycznego.

Artykuł 33

Wzajemna pomoc prawna przy gromadzeniu w czasie rzeczywistym danych dotyczących ruchu

1. Strony powinny świadczyć sobie wzajemną pomoc prawną w gromadzeniu w czasie rzeczywistym danych dotyczących ruchu, związanych z określonymi przekazami na ich terytorium, realizowanymi przy pomocy systemu informatycznego. Pomoc ta, z zastrzeżeniem ustępu 2, podlega warunkom i procedurom określonym prawem

krajowym.

2. Każda Strona winna udzielić takiej pomocy przynajmniej w odniesieniu do przestępstw, w stosunku do których gromadzenie danych dotyczących ruchu byłoby możliwe w wypadku podobnej sprawy o charakterze krajowym.

Artykuł 34

Wzajemna pomoc prawna w zakresie przechwytywania danych dotyczących treści

W zakresie dozwolonym przez obowiązujące traktaty i prawo krajowe, Strony powinny świadczyć sobie pomoc wzajemną w zakresie gromadzenia lub rejestrowania w czasie rzeczywistym danych dotyczących treści określonych przekazów realizowanych przy pomocy systemu informatycznego.

Tytuł 3

Sieć 24/7

Artykuł 35

Sieć 24/7

1. Każda ze Stron wyznaczy punkt kontaktowy dostępny 24 godziny na dobę przez 7 dni w tygodniu, w celu zapewnienia natychmiastowej pomocy dla celów prowadzenia czynności śledczych lub postępowań odnoszących się do przestępstw związanych z systemami i danymi informatycznymi lub dla celów zbierania dowodów w postaci elektronicznej dotyczących przestępstw. Pomoc ta będzie obejmowała ułatwienia lub, jeżeli jest to dopuszczalne przez prawo krajowe lub praktykę, bezpośrednie zastosowanie następujących środków:
   a. zapewnienie doradztwa technicznego;
   b. zabezpieczenie danych zgodnie z artykułami 29 i 30;
   c. gromadzenie dowodów, dostarczanie informacji o prawie oraz lokalizowanie osób podejrzanych.
2. a. Punkt kontaktowy Strony będzie mógł porozumiewać się z punktem kontaktowym

drugiej Strony w trybie przyspieszonym.

b. Jeżeli punkt kontaktowy wyznaczony przez Stronę nie jest częścią organu lub organów tej Strony odpowiedzialnych za międzynarodową pomoc prawną lub ekstradycję, punkt kontaktowy powinien zapewnić istnienie szybkiej koordynacji z tym organem lub organami.

3. Każda Strona zapewni odpowiednio przeszkolony i wyposażony personel dla ułatwienia funkcjonowania sieci.

ROZDZIAŁ IV

POSTANOWIENIA KOŃCOWE

Artykuł 36

Podpisanie i wejście w życie konwencji

1. Niniejsza konwencja jest otwarta do podpisu dla państw członkowskich Rady Europy oraz państw, które nie są członkami Rady Europy, lecz uczestniczyły w jej opracowywaniu.

2. Niniejsza konwencja podlega ratyfikacji, akceptacji lub zatwierdzeniu. Instrumenty ratyfikacyjne, akceptacji lub zatwierdzenia składa się Sekretarzowi Generalnemu Rady Europy.

3. Niniejsza konwencja wejdzie w życie pierwszego dnia miesiąca następującego po upływie trzymiesięcznego okresu od dnia, w którym pięć państw, w tym co najmniej trzy państwa członkowskie Rady Europy, wyrażą swoją zgodę na związanie się postanowieniami konwencji, zgodnie z ustępami 1 i 2.

4. Wobec każdego Państwa-Sygnatariusza, które w późniejszym okresie wyrazi swoją zgodę na związanie się Konwencją, wejdzie ona w życie pierwszego dnia miesiąca następującego po upływie trzymiesięcznego okresu od dnia wyrażenia zgody na związanie się konwencją, zgodnie z ustępami 1 i 2.

Artykuł 37

Przystąpienie do Konwencji

1. Po wejściu w życie niniejszej konwencji, Komitet Ministrów Rady Europy, po

przeprowadzeniu konsultacji z Państwami-Stronami konwencji i uzyskaniu ich jednomyślnej zgody, będzie mógł zaprosić każde inne państwo niebędące członkiem Rady Europy i nieuczestniczące w jej opracowywaniu, do przystąpienia do niniejszej konwencji. Decyzja zostanie podjęta większością głosów, zgodnie z artykułem 20.d. Statutu Rady Europy, oraz przy jednomyślności przedstawicieli Państw-Stron uprawnionych do zasiadania w Komitecie Ministrów.

2. W odniesieniu do wszystkich państw przystępujących do konwencji zgodnie z ustępem 1 powyżej, konwencja wejdzie w życie pierwszego dnia miesiąca po upływie trzymiesięcznego okresu od dnia złożenia Sekretarzowi Generalnemu Rady Europy instrumentu przystąpienia.

Artykuł 38

Zakres terytorialny

1. Każde państwo, w chwili podpisywania lub składania swojego instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia, może wskazać terytorium lub terytoria, do których stosować się będzie niniejsza konwencja.

2. Każda Strona może w dowolnym momencie złożyć Sekretarzowi Generalnemu Rady Europy deklarację o rozszerzeniu stosowania niniejszej konwencji na każde inne terytorium określone w tej deklaracji. Konwencja wejdzie w życie na tym terytorium pierwszego dnia miesiąca po upływie trzymiesięcznego okresu od dnia przyjęcia deklaracji przez Sekretarza Generalnego Rady Europy.

3. Każda deklaracja złożona na podstawie dwóch poprzednich ustępów może zostać wycofana w odniesieniu do każdego terytorium wymienionego w drodze notyfikacji skierowanej do Sekretarza Generalnego Rady Europy. Wycofanie wchodzi w życie pierwszego dnia miesiąca po upływie trzymiesięcznego okresu od dnia przyjęcia notyfikacji przez Sekretarza Generalnego Rady Europy.

Artykuł 39

Skutki konwencji

1. Celem niniejszej konwencji jest uzupełnienie obowiązujących traktatów lub umów wielostronnych lub dwustronnych zawartych między Stronami, w tym postanowień:
   - Europejskiej konwencji o ekstradycji otwartej do podpisu w Paryżu w dniu 13 grudnia 1957 roku (ETS nr 24);
   - Europejskiej konwencji o pomocy prawnej w sprawach karnych otwartej do podpisu w Strasburgu w dniu 20 kwietnia 1959 roku (ETS nr 30);
   - Protokołu dodatkowego do Europejskiej konwencji o pomocy prawnej w sprawach karnych otwartego do podpisu w Strasburgu w dniu 17 marca 1978 roku (ETS nr 99).
2. Jeżeli dwie lub więcej Strony zawarły porozumienie lub traktat odnoszący się do kwestii uregulowanych niniejszą konwencją lub jeżeli uregulowały w inny sposób swoje stosunki związane z tymi zagadnieniami, lub uczynią to w przyszłości, są one uprawnione do stosowania postanowień tych porozumień lub traktatów oraz odpowiedniego uregulowania swoich stosunków. Jednakże, gdy strony uregulują wzajemne stosunki odnoszące się do kwestii, jakimi zajmuje się niniejsza konwencja, odmiennie niż w konwencji, powinny to uczynić w sposób, który nie jest sprzeczny z celami i zasadami konwencji.
3. Żadne postanowienie niniejszej konwencji nie może wpływać na inne prawa, ograniczenia, obowiązki i zobowiązania Strony.

Artykuł 40

Deklaracje

Każde państwo, w pisemnej deklaracji skierowanej do Sekretarza Generalnego Rady Europy, może w chwili podpisywania lub składania swojego instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia oświadczyć, że zastrzega sobie możliwość stawiania dodatkowych wymagań, o których mowa w artykułach 2, 3, 6 ust. 1.b, 7, 9 ust. 3 i 27 ust. 9.e.

Artykuł 41

Klauzula federalna

1. Państwo federalne może zastrzec sobie prawo wykonywania zobowiązań wynikających z Rozdziału II niniejszej konwencji zgodnie z jej podstawowymi zasadami regulującymi stosunki między władzami federalnymi a państwami wchodzącymi w skład federacji lub innymi analogicznymi jednostkami terytorialnymi, pod warunkiem, że jest nadal w stanie prowadzić współpracę na podstawie Rozdziału III.
2. Przy składaniu zastrzeżenia na podstawie ustępu 1 państwo federalne nie może formułować warunków, które zniweczą lub istotnie ograniczą jego zobowiązania do stosowania środków przewidzianych w Rozdziale II. Generalnie, powinno dysponować prawną zdolnością do szerokiego i skutecznego wykonywania takich środków.
3. W odniesieniu do postanowień niniejszej konwencji, których wykonywanie należy do jurysdykcji państw wchodzących w skład federacji lub innych analogicznych jednostek terytorialnych, niemających obowiązku – zgodnie z ich konstytucyjnym systemem federalnym dotyczących przestępstw – podejmowania działań legislacyjnych, władze federalne powinny przedstawić właściwym organom tych państw informację o wspomnianych przepisach łącznie ze swoją pozytywną o nich opinią, aby zachęcić je do podjęcia stosownych działań implementacyjnych.

Artykuł 42

Zastrzeżenia

Każde państwo, w pisemnej notyfikacji skierowanej do Sekretarza Generalnego Rady Europy, może, w chwili podpisywania lub składania swojego instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia, złożyć zastrzeżenie lub zastrzeżenia, o jakich mowa w artykułach 4 ust. 2, 6 ust. 3, 9 ust. 4, 10 ust. 3, 11 ust. 3, 14 ust. 3, 22 ust. 2, 29 ust. 4. i 41 ust. 1. Składanie innych zastrzeżeń jest niedopuszczalne.

Artykuł 43

Status i wycofanie zastrzeżeń

1. Strona, która zgłosiła zastrzeżenie zgodnie z artykułem 42, może wycofać je w całości lub

w części w drodze notyfikacji skierowanej do Sekretarza Generalnego Rady Europy. Wycofanie to wejdzie w życie z dniem otrzymania tej notyfikacji przez Sekretarza Generalnego. Jeżeli w notyfikacji podaje się, że wycofanie zastrzeżenia wchodzi w życie z konkretną datą oraz jeżeli data jest późniejsza od daty otrzymania notyfikacji przez Sekretarza Generalnego, wycofanie wejdzie w życie w tej późniejszej dacie.

2. Strona, która złożyła zastrzeżenie zgodnie z artykułem 42, powinna wycofać to zastrzeżenie w całości lub w części, gdy tylko pozwolą na to okoliczności.

3. Sekretarz Generalny może okresowo zwracać się do Stron, które złożyły jedno lub kilka zastrzeżeń zgodnie z artykułem 42, o przedstawienie informacji o perspektywach wycofania tego zastrzeżenia lub zastrzeżeń.

Artykuł 44

Zmiany

1. Każda Strona może zgłaszać propozycje zmian w konwencji; każda taka propozycja zostanie przedstawiona przez Sekretarza Generalnego Rady Europy państwom członkowskim Rady Europy, państwom niebędącym członkami, które uczestniczyły w opracowywaniu niniejszej konwencji, jak też każdemu państwu, które przystąpiło do konwencji lub które zostało zaproszone do przystąpienia do niej zgodnie z postanowieniami artykułu 37.

2. Każda zmiana proponowana przez Stronę będzie przekazywana Europejskiemu Komitetowi ds. Przestępczości (CDPC), który przedłoży Komitetowi Ministrów swoją opinię dotyczącą proponowanej zmiany.

3. Komitet Ministrów zbada proponowaną zmianę oraz opinię przedłożoną przez CDPC i po konsultacjach z Państwami-Stronami konwencji, niebędącymi członkami Rady Europy może przyjąć zmianę.

4. Tekst każdej zmiany przyjętej przez Komitet Ministrów zgodnie z ustępem 3 niniejszego artykułu zostaje przekazany Stronom do akceptacji.

5. Każda zmiana przyjęta zgodnie z ustępem 3 niniejszego artykułu wejdzie w życie trzydziestego dnia po dacie, w której Strony poinformowały Sekretarza Generalnego

o zaakceptowaniu zmiany.

Artykuł 45

Rozstrzyganie sporów

1. Europejski Komitet ds. Przestępczości Rady Europy (CDPC) będzie informowany o sposobie interpretowania i stosowania niniejszej konwencji.

2. W razie rozbieżności między Stronami w odniesieniu do interpretacji lub stosowania niniejszej konwencji, Strony dążyć będą do rozstrzygnięcia sporu na drodze negocjacji lub przy użyciu innych środków pokojowych, jakie same wybiorą, w tym także przez przedłożenie sporu CDPC, sądowi arbitrażowemu, którego decyzje będą wiążące dla Stron lub Międzynarodowemu Trybunałowi Sprawiedliwości, stosownie do uzgodnień między zainteresowanymi Stronami.

Artykuł 46

Konsultacje między Stronami

1. Strony prowadzić będą, w miarę potrzeb, okresowe konsultacje celem ułatwienia:

   a. skutecznego stosowania i wdrażania konwencji, w tym identyfikacji problemów w tym zakresie, a także skutków deklaracji i zastrzeżeń złożonych na podstawie niniejszej konwencji;

   b. wymiany informacji o najnowszych istotnych zmianach w prawie, polityce lub w dziedzinie techniki, odnoszących się do cyberprzestępczości oraz zbierania dowodów w postaci elektronicznej;

   c. badania możliwości uzupełnienia lub wprowadzenia zmian do konwencji.

2. Europejski Komitet ds. Przestępczości (CDPC) będzie okresowo informowany o wynikach konsultacji, o jakich mowa w ustępie 1.

3. CDPC będzie, w miarę potrzeb, ułatwiał konsultacje, o jakich mowa w ustępie 1, oraz podejmował działania niezbędne dla udzielenia Stronom pomocy w ich wysiłkach zmierzających do uzupełnienia lub wprowadzenia zmian do konwencji. Najpóźniej w terminie trzech lat od daty wejścia w życie niniejszej konwencji, Europejski Komitet ds.

Przestępczości (CDPC) dokona, we współpracy ze Stronami, przeglądu wszystkich postanowień konwencji, i w miarę potrzeby zaleci odpowiednie zmiany.

4. Koszty związane z realizacją postanowień ustępu 1 ponoszą Strony, w sposób przez nie ustalony, za wyjątkiem tych kosztów, które ponosi Rada Europy.

5. Sekretariat Rady Europy udziela Stronom pomocy w wykonywaniu ich zadań zgodnie z niniejszym artykułem.

Artykuł 47

Wypowiedzenie

1. Każda Strona może w dowolnej chwili wypowiedzieć niniejszą konwencję kierując do Sekretarza Generalnego Rady Europy odpowiednią notyfikację.

2. Wypowiedzenie wchodzi w życie pierwszego dnia miesiąca po upływie trzymiesięcznego okresu od dnia otrzymania notyfikacji przez Sekretarza Generalnego Rady Europy.

Artykuł 48

Notyfikacja

Sekretarz Generalny Rady Europy notyfikuje państwom członkowskim, państwom niebędącym członkami Rady Europy, które uczestniczyły w opracowywaniu niniejszej konwencji, jak też wszystkim państwom, które przystąpiły do konwencji lub zostały zaproszone do przystąpienia do niej:

a. każdy akt podpisania konwencji;

b. złożenie instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia;

c. każdą datę wejścia w życie niniejszej konwencji zgodnie z jej artykułami 36 i 37;

d. każdą deklarację złożoną na mocy artykułu 40 lub każde zastrzeżenie złożone na mocy artykułu 42;

e. wszelkie inne akty, notyfikacje lub informacje związane z niniejszą konwencją.

Na dowód czego, niżej podpisani, odpowiednio do tego uprawomocnieni, podpisali niniejszą

konwencję.

Sporządzono w Budapeszcie dnia 23 listopada 2001 roku w językach francuskim i angielskim, przy czym obie wersje językowe są jednakowo autentyczne, w jednym egzemplarzu, który zostanie złożony w archiwum Rady Europy. Sekretarz Generalny Rady Europy przekaże poświadczone kopie każdemu państwu członkowskiemu Rady Europy, państwom niebędącym członkami Rady Europy, które uczestniczyły w opracowywaniu konwencji oraz każdemu państwu zaproszonemu do przystąpienia do konwencji.

Convention on Cybercrime

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I - Use of terms

Article 1 - Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II - Measures to be taken at the national level

Section 1 - Substantive criminal law

Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 - Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 - Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 - Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 - Expedited preservation of stored computer data

Article 16 - Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III - International co-operation

Section 1 - General principles

Title 1 – General principles relating to international co-operation

Article 23 - General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 - Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 - Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 - Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 - Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 - Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 - Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 - Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 - Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 - Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 - Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 - Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at [Budapest], this [23rd day of November 2001], in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Po zaznajomieniu się z powyższą konwencją, w imieniu Rzeczypospolitej Polskiej oświadczam, że:

– została ona uznana za słuszną zarówno w całości, jak i każde z postanowień w niej zawartych,

– jest przyjęta, ratyfikowana i potwierdzona,

– będzie niezmiennie zachowywana, z uwzględnieniem zastrzeżenia do artykułu 29 ustęp 4 i deklaracji do artykułu 24 ustęp 7, artykułu 27 ustęp 2 litera a oraz do artykułu 35 konwencji.

Na dowód czego wydany został akt niniejszy, opatrzony pieczęcią Rzeczypospolitej Polskiej.

Dano w Warszawie dnia 29 stycznia 2015 r.

Prezydent Rzeczypospolitej Polskiej: *B. Komorowski*

L.S.

Prezes Rady Ministrów: *E. Kopacz*