ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2008

Vyhlásené: 24.04.2008 Vyhlásená verzia v Zbierke zákonov Slovenskej republiky

Obsah tohto dokumentu má informatívny charakter.

137

OZNÁMENIE
Ministerstva zahraničných vecí Slovenskej republiky

Ministerstvo zahraničných vecí Slovenskej republiky oznamuje, že 23. novembra 2001 bol v Budapešti otvorený na podpis Dohovor o počítačovej kriminalite.

Národná rada Slovenskej republiky s dohovorom vyslovila súhlas svojím uznesením č. 583 z 23. októbra 2007.

Prezident republiky dohovor ratifikoval 12. decembra 2007. Ratifikačná listina bola uložená 8. januára 2008 u generálneho tajomníka Rady Európy, depozitára dohovoru.

Dohovor nadobudol platnosť 1. júla 2004 v súlade s článkom 36 ods. 3. Pre Slovenskú republiku nadobudne platnosť 1. mája 2008 v súlade s článkom 36 ods. 4.
Slovenská republika pri ratifikácii uplatnila tieto vyhlásenia a výhrady:

„a) V súlade s článkom 24 ods. 7 písm. a) Slovenská republika vyhlasuje, že orgánom príslušným na zasielanie a prijímanie žiadostí o vydanie je Ministerstvo spravodlivosti Slovenskej republiky (Župné námestie 13, 813 11 Bratislava). Orgánom príslušným na prijatie žiadosti o predbežnú väzbu je príslušný prokurátor krajskej prokuratúry a Ministerstvo spravodlivosti Slovenskej republiky. Orgánom príslušným na zaslanie žiadosti o predbežnú väzbu je Ministerstvo spravodlivosti Slovenskej republiky a súd príslušný na vydanie medzinárodného zatýkacieho rozkazu.

b) V súlade s článkom 27 ods. 2 písm. a) Slovenská republika vyhlasuje, že ústrednými orgánmi sú: Ministerstvo spravodlivosti Slovenskej republiky (Župné námestie 13, 813 11 Bratislava) a Generálna prokuratúra Slovenskej republiky (Štúrova 2, 812 85 Bratislava).

c) Slovenská republika oznamuje, že kontaktným miestom na účely článku 35 dohovoru je Prezídium policajného zboru, Úrad medzinárodnej policajnej spolupráce, Národná ústredňa Interpol Bratislava (Vajnorská 25, 812 72 Bratislava).

d) V súlade s článkom 40 Slovenská republika vyhlasuje, že využíva možnosť ustanoviť dodatočný prvok podľa článku 2 dohovoru a trestnosť nezákonného prístupu podmieňuje tým, že musí byť spáchaný porušením bezpečnostných opatrení s úmyslom získať počítačové údaje alebo s iným nečestným úmyslom, alebo vo vzťahu k počítačovému systému prepojenému s iným počítačovým systémom.

e) Slovenská republika si v súlade s článkom 42 a článkom 29 ods. 4 dohovoru vyhradzuje právo odmietnuť vykonanie žiadosti o uchovanie údajov v prípadoch, v ktorých má dôvody domnievať sa, že v čase sprístupnenia nemožno splniť podmienku obojstrannej trestnosti.

f) V súlade s článkom 42 a článkom 4 ods. 2 Slovenská republika si vyhradzuje právo vyžadovať pre trestnosť konania uvedeného v článku 4 ods. 1, aby jeho následkom bola značná škoda“.

K oznámeniu č. 137
2008 Z. z.

DOHOVOR O POČÍTAČOVEJ KRIMINALITE

Budapešť 23. XI. 2001

Preambula

Členské štáty Rady Európy a ostatné štáty, ktoré sú signatármi tohto dohovoru,

berúc do úvahy, že cieľom Rady Európy je dosiahnuť väčšiu jednotu medzi jej členmi,

uznávajúc význam podpory spolupráce s ostatnými štátmi, ktoré sú zmluvnými stranami tohto dohovoru,

súc presvedčené o potrebe prioritného uskutočňovania spoločnej trestnej politiky zameranej na ochranu spoločnosti proti počítačovej kriminalite, okrem iného prijatím príslušnej legislatívy a podporovaním medzinárodnej spolupráce,

uvedomujúc si zásadné zmeny, ktoré priniesla digitalizácia, zbližovanie a pokračujúca globalizácia počítačových sietí,

súc znepokojené rizikom, že počítačové siete a elektronické informácie môžu byť aj zneužité na páchanie trestných činov a že dôkazy týkajúce sa takých trestných činov sa môžu uchovávať a prenášať prostredníctvom týchto sietí,

uznávajúc potrebu spolupráce medzi štátmi a súkromným sektorom v boji proti počítačovej kriminalite a potrebu chrániť oprávnené záujmy pri používaní a rozvoji informačných technológií,

domnievajúc sa, že účinný boj proti počítačovej kriminalite vyžaduje zvýšenú, rýchlu a dobre fungujúcu medzinárodnú spoluprácu v trestných veciach,

súc presvedčené, že tento dohovor je nevyhnutný na odradenie od činov namierených proti dôvernosti, celistvosti a dostupnosti počítačových systémov, sietí a počítačových údajov, ako aj proti zneužívaniu takých systémov, sietí a údajov tým, že sa zabezpečí trestný postih správania opísaného v tomto dohovore a udelia sa primerané právomoci na účinný boj proti takým trestným činom, aby sa uľahčilo odhaľovanie, vyšetrovanie a trestné stíhanie na vnútroštátnych a medzinárodných úrovniach, a že sa ustanovia postupy umožňujúce rýchlu a spoľahlivú medzinárodnú spoluprácu,

s vedomím potreby zabezpečiť správnu rovnováhu medzi záujmami presadzovania práva a rešpektovania základných ľudských práv zakotvených v Dohovore o ochrane ľudských práv a základných slobôd z roku 1950, v Medzinárodnom pakte o občianskych a politických právach z roku 1966, ako aj v ostatných použiteľných medzinárodných zmluvách o ľudských právach, ktoré opätovne potvrdzujú právo každého na názory bez zasahovania, ako aj právo na slobodu prejavu vrátane slobody vyhľadávať, prijímať a odovzdávať informácie a myšlienky každého druhu bez ohľadu na hranice a práva týkajúce sa rešpektovania súkromia,

dbajúc aj na právo na ochranu osobných údajov, aké ustanovuje napríklad Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov z roku 1981,

berúc do úvahy Dohovor o právach dieťaťa z roku 1989 a Dohovor Medzinárodnej organizácie práce o zákaze a o okamžitých opatreniach na odstránenie najhorších foriem detskej práce č. 182 z roku 1999,

so zreteľom na existujúce dohovory Rady Európy o spolupráci v trestnej oblasti, ako aj na podobné zmluvy, ktoré existujú medzi členskými štátmi Rady Európy a inými štátmi, a zdôrazňujúc, že zámerom tohto dohovoru je doplniť tieto dohovory tak, aby sa zefektívnilo vyšetrovanie a konanie pri trestných činoch súvisiacich s počítačovými systémami a údajmi a aby sa umožnilo zhromažďovanie dôkazov o trestnom čine v elektronickej forme,

vítajúc nedávny vývoj, ktorý ďalej prehlbuje medzinárodné porozumenie a spoluprácu v boji proti počítačovej kriminalite vrátane krokov prijatých Organizáciou Spojených národov, OECD, Európskou úniou a skupinou štátov G8,

odvolávajúc sa na odporúčanie Výboru ministrov č. R (85) 10 o praktickom uplatňovaní Európskeho dohovoru o vzájomnej pomoci v trestných veciach vo vzťahu k dožiadaniam na odpočúvanie telekomunikácií, odporúčanie č. R (88) 2 o opatreniach na boj s pirátstvom v oblasti autorských práv a príbuzných práv, odporúčanie č. R (87) 15 upravujúce používanie osobných údajov v policajnom sektore, odporúčanie č. R (95) 4 o ochrane osobných údajov v oblasti telekomunikačných služieb s osobitným zameraním na telefónne služby, ako aj odporúčanie č. R (89) 9 o kriminalite spojenej s počítačmi, ktoré stanovuje zásady pre vnútroštátnych zákonodarcov týkajúce sa vymedzenia určitých počítačových trestných činov, a na odporúčanie č. (95) 13 o problémoch trestného práva procesného spojených s informačnou technológiou,

so zreteľom na rezolúciu č. 1 prijatú európskymi ministrami spravodlivosti na ich 21. konferencii (Praha 10. a 11. jún 1997), ktorá odporučila, aby Výbor ministrov podporil prácu Európskeho výboru pre problémy kriminality (CDPC) vykonávanú v oblasti počítačovej kriminality s cieľom vzájomne zblížiť ustanovenia vnútroštátneho trestného práva a umožniť využitie účinných prostriedkov na vyšetrovanie takých trestných činov, ako aj so zreteľom na rezolúciu č. 3 prijatú na 23. konferencii európskych ministrov spravodlivosti (Londýn 8. a 9. jún 2000), ktorá povzbudila rokujúce strany, aby pokračovali vo svojom úsilí nájsť vhodné riešenia a umožnili tak čo najväčšiemu počtu štátov stať sa zmluvnými stranami dohovoru a uznali potrebu rýchleho a účinného systému medzinárodnej spolupráce, ktorý náležite zohľadní špecifické požiadavky boja proti počítačovej kriminalite,

so zreteľom na Akčný plán prijatý hlavami štátov a vlád Rady Európy pri príležitosti ich druhého summitu (Štrasburg 10. – 11. október 1997) s cieľom hľadať spoločné odpovede na vývoj nových informačných technológií, vychádzajúc zo štandardov a hodnôt Rady Európy,

dohodli sa takto:

KAPITOLA I
POUŽITIE POJMOV

Článok 1
Definície

Na účely tohto dohovoru

a) „počítačový systém“ znamená zariadenie alebo skupinu vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno zariadenie alebo viaceré zariadenia vykonávajú automatizované spracúvanie údajov na základe programu,

b) „počítačové údaje“ znamenajú záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu schopného spôsobiť, že počítačový systém vykoná určitú činnosť,

c) „poskytovateľ služieb“ znamená

i. verejný alebo súkromný subjekt, ktorý poskytuje používateľom svojich služieb možnosť komunikovať prostredníctvom počítačového systému, a
ii. iný subjekt, ktorý spracúva alebo uchováva počítačové údaje pre takú komunikačnú službu alebo pre používateľov takej služby,

d) „prevádzkové údaje“ znamenajú počítačové údaje týkajúce sa komunikácie prostredníctvom počítačového systému vytvorené počítačovým systémom, ktorý tvoril súčasť komunikačného reťazca, s uvedením pôvodu, cieľa, trasy, času, dátumu, objemu a trvania komunikácie alebo typu služby, ktorá bola jej podkladom.

KAPITOLA II
OPATRENIA, KTORÉ JE POTREBNÉ PRIJAŤ NA VNÚTROŠTÁTNEJ ÚROVNI

Oddiel 1
Trestné právo hmotné

HLAVA 1
TRESTNÉ ČINY PROTI DÔVERNOSTI, HODNOVERNOSTI A DOSTUPNOSTI POČÍTAČOVÝCH ÚDAJOV A SYSTÉMOV

Článok 2
Nezákonný prístup

Každá strana prijme potrebné legislatívne a iné opatrenia, aby neoprávnený prístup do počítačového systému ako celku alebo do jeho časti bol trestným činom podľa jej vnútroštátneho právneho poriadku, ak bol spáchaný úmyselne. Strana môže trestnosť činu podmieniť tým, že musí byť spáchaný porušením bezpečnostných opatrení s úmyslom získať počítačové údaje alebo s iným nečestným úmyslom, alebo vo vzťahu k počítačovému systému prepojenému s iným počítačovým systémom.

Článok 3
Nezákonné zachytenie údajov

Každá strana prijme potrebné legislatívne a iné opatrenia, aby neoprávnené zachytávanie neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v rámci tohto systému vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje také počítačové údaje vykonané technickými prostriedkami, bolo trestným činom podľa jej vnútroštátneho právneho poriadku, ak bolo spáchané úmyselne. Strana môže trestnosť činu podmieniť tým, že musí byť spáchaný s nečestným úmyslom alebo vo vzťahu k počítačovému systému prepojenému s iným počítačovým systémom.

Článok 4
Zasahovanie do údajov

1. Každá strana prijme potrebné legislatívne a iné opatrenia, aby neoprávnené poškodenie, vymazanie, zhoršenie kvality, pozmenenie počítačových údajov alebo zamedzenie prístupu k nim boli trestným činom podľa jej vnútroštátneho právneho poriadku, ak boli spáchané úmyselne.
2. Strana si môže vyhradiť právo vyžadovať, aby následkom konania uvedeného v odseku 1 bola značná škoda.

Článok 5
Zasahovanie do systému

Každá strana prijme potrebné legislatívne a iné opatrenia, aby neoprávnené závažné marenie funkčnosti počítačového systému vkladaním, prenášaním, poškodením, vymazaním, zhoršením, pozmenením počítačových údajov alebo zamedzením prístupu k nim bolo trestným činom podľa jej vnútroštátneho právneho poriadku, ak bolo spáchané úmyselne.

Článok 6
Zneužitie zariadení

1. Každá strana prijme potrebné legislatívne a iné opatrenia, aby konania uvedené ďalej, ak boli spáchané úmyselne a bez oprávnenia, boli trestným činom podľa jej vnútroštátneho právneho poriadku:

   a) výroba, predaj, obstarávanie na účely použitia, dovoz, distribúcia alebo iné sprístupnenie
      i. zariadenia vrátane počítačového programu vytvoreného alebo upraveného predovšetkým s cieľom spáchať niektorý z trestných činov vymedzených v článkoch 2 až 5,
      ii. počítačového hesla, prístupového kódu alebo podobných údajov, ktorých pomocou je možný prístup do počítačového systému ako celku alebo do niektorej jeho časti,
   s úmyslom ich použiť na spáchanie niektorého z trestných činov vymedzených v článkoch 2 až 5 a

   b) držba veci uvedenej v odseku 1 písm. a) bode i. alebo ii. s úmyslom ju použiť na spáchanie niektorého z trestných činov vymedzených v článkoch 2 až 5. Strana môže ustanoviť zákonom, že na založenie trestnej zodpovednosti sa vyžaduje držba viacerých takých vecí.

2. Tento článok nemožno vykladať tak, že zakladá trestnú zodpovednosť v prípadoch, ak ide o výrobu, predaj, obstarávanie na účely použitia, dovoz, distribúciu alebo iné sprístupnenie, alebo o držbu uvedenú v odseku 1, ktorých účelom nie je spáchanie niektorého z trestných činov vymedzených v článkoch 2 až 5, ako napríklad pri autorizovanom testovaní alebo autorizovanej ochrane počítačového systému.

3. Každá strana si môže vyhradiť právo neuplatňovať odsek 1 za predpokladu, že výhrada sa netýka predaja, distribúcie alebo iného sprístupnenia údajov uvedených v odseku 1 písm. a) bode ii.

HLAVA 2
POČÍTAČOVÉ TRESTNÉ ČINY

Článok 7
Falšovanie počítačových údajov

Každá strana prijme potrebné legislatívne a iné opatrenia, aby vloženie, pozmenenie, vymazanie počítačových údajov alebo zamedzenie prístupu k nim, v ktorých dôsledku stratia údaje autentickosť, s úmyslom považovať ich za autentické alebo aby sa na základe nich ako autentických údajov konalo, na právne účely, bez ohľadu na to, či tieto údaje sú alebo nie sú priamo čitateľné alebo zrozumiteľné, boli trestným činom podľa jej vnútroštátneho právneho poriadku, ak boli spáchané úmyselne a bez oprávnenia. Strana môže trestnosť činu podmieniť tým, že čin musí byť spáchaný s podvodným alebo iným nečestným úmyslom.

Článok 8
Počítačový podvod

Každá strana prijme potrebné legislatívne a iné opatrenia, aby spôsobenie majetkovej ujmy inému

a) vložením, pozmenením, vymazaním počítačových údajov alebo zamedzením prístupu k nim,

b) zásahom do fungovania počítačového systému

s podvodným alebo nečestným úmyslom neoprávnene získať pre seba alebo pre iného majetkový prospech bolo trestným činom podľa jej vnútroštátneho právneho poriadku, ak bolo spáchané úmyselne a bez oprávnenia.

HLAVA 3
TRESTNÉ ČINY TÝKAJÚCE SA OBSAHU

Článok 9
Trestné činy týkajúce sa detskej pornografie

1. Každá strana prijme potrebné legislatívne a iné opatrenia, aby konania uvedené ďalej, ak boli spáchané úmyselne a bez oprávnenia, boli trestným činom podľa jej vnútroštátneho právneho poriadku:
   a) výroba detskej pornografie na účely jej distribúcie počítačovým systémom,
   b) ponuka alebo sprístupnenie detskej pornografie počítačovým systémom,
   c) distribúcia alebo prenos detskej pornografie počítačovým systémom,
   d) zaobstaranie detskej pornografie počítačovým systémom pre seba alebo pre iného,
   e) držba detskej pornografie v počítačovom systéme alebo na pamäťovom nosiči počítačových údajov.
2. Na účely odseku 1 pojem „detská pornografia“ zahŕňa pornografický materiál, ktorý zobrazuje
   a) maloletú osobu zúčastnenú na zjavnom sexuálnom správaní,
   b) osobu, ktorá sa zdá byť maloletá a ktorá sa zúčastňuje na zjavnom sexuálnom správaní,
   c) realistické zobrazenia maloletej osoby zúčastnenej na zjavnom sexuálnom správaní.
3. Na účely odseku 2 pojem „maloletá osoba“ zahŕňa všetky osoby mladšie ako 18 rokov. Strana však môže určiť nižšiu vekovú hranicu, ktorá nesmie prekročiť hranicu 16 rokov.
4. Každá strana si môže vyhradiť právo neuplatňovať úplne alebo sčasti odsek 1 písm. d) a e) a odsek 2 písm. b) a c).

HLAVA 4
TRESTNÉ ČINY TÝKAJÚCE SA PORUŠENIA AUTORSKÝCH A PRÍBUZNÝCH PRÁV

Článok 10
Trestné činy týkajúce sa porušenia autorských a príbuzných práv

1. Každá strana prijme potrebné legislatívne a iné opatrenia, aby porušenie autorského práva vymedzeného právnym poriadkom tejto strany v súlade so záväzkami, ktoré prijala podľa Parížskeho aktu z 24. júla 1971, ktorým sa mení Bernský dohovor o ochrane literárnych a umeleckých diel, Dohody o obchodných aspektoch práv na duševné vlastníctvo a Zmluvy Svetovej organizácie duševného vlastníctva (WIPO) o autorskom práve, okrem osobnostných práv priznaných týmito dohovormi, bolo trestným činom podľa jej vnútroštátneho právneho poriadku, ak tieto činy boli spáchané úmyselne, v obchodnom meradle a prostredníctvom počítačového systému.
2. Každá strana prijme potrebné legislatívne a iné opatrenia, aby porušenie príbuzných práv, ako ich vymedzuje jej právny poriadok v súlade so záväzkami, ktoré prijala podľa Medzinárodného dohovoru o ochrane výkonných umelcov, výrobcov zvukových záznamov a rozhlasových organizácií (Rímsky dohovor), Dohody o obchodných aspektoch práv na duševné vlastníctvo a Zmluvy Svetovej organizácie duševného vlastníctva (WIPO) o výkonoch a zvukových záznamoch, okrem osobnostných práv priznaných týmito dohovormi, bolo trestným činom podľa jej vnútroštátneho právneho poriadku, ak tieto činy boli spáchané úmyselne, v obchodnom meradle a prostredníctvom počítačového systému.
3. Strana si môže vyhradiť právo nezaložiť trestnú zodpovednosť podľa odsekov 1 a 2 za predpokladu, že sú dostupné iné účinné právne prostriedky nápravy a že taká výhrada nezmení rozsah medzinárodných záväzkov tejto strany vyplývajúcich z medzinárodných nástrojov uvedených v odsekoch 1 a 2.

HLAVA 5
VEDĽAJŠIA ZODPOVEDNOSŤ A SANKCIE

Článok 11
Pokus a napomáhanie alebo navádzanie

1. Každá strana prijme potrebné legislatívne a iné opatrenia, aby napomáhanie alebo navádzanie na spáchanie trestných činov vymedzených v článkoch 2 až 10 s úmyslom, aby taký trestný čin bol spáchaný, bolo trestným činom podľa jej vnútroštátneho právneho poriadku, ak bol spáchaný úmyselne.
2. Každá strana prijme potrebné legislatívne a iné opatrenia, aby pokus o spáchanie trestných činov vymedzených v článkoch 3 až 5, 7 a 8, v článku 9 ods. 1 písm. a) a c) bol trestným činom podľa jej vnútroštátneho právneho poriadku, ak bol spáchaný úmyselne.
3. Každá strana si môže vyhradiť právo neuplatňovať odsek 2 úplne alebo sčasti.

Článok 12
Zodpovednosť právnických osôb

1. Každá strana prijme potrebné legislatívne a iné opatrenia na založenie zodpovednosti právnickej osoby za trestný čin vymedzený v súlade s týmto dohovorom, ktorý v jej prospech spáchala fyzická osoba samostatne alebo ako súčasť orgánu tejto právnickej osoby a ktorá má vedúce postavenie v rámci tejto právnickej osoby na základe
   a) oprávnenia zastupovať právnickú osobu,
   b) oprávnenia prijímať rozhodnutia v mene právnickej osoby,
   c) oprávnenia vykonávať kontrolu v rámci právnickej osoby.
2. Každá strana prijme okrem prípadov už vymedzených v odseku 1 opatrenia potrebné na ustanovenie zodpovednosti právnickej osoby v prípade, keď nedostatočný dohľad alebo kontrola zo strany fyzickej osoby uvedenej v odseku 1 umožnili spáchanie trestného činu podľa tohto dohovoru v prospech tejto právnickej osoby fyzickou osobou, ktorá koná v rámci poverenia tejto právnickej osoby.
3. V závislosti od právnych zásad strany môže byť zodpovednosť právnickej osoby trestnoprávna, občianskoprávna alebo správna.
4. Taká zodpovednosť nemá vplyv na trestnoprávnu zodpovednosť fyzických osôb, ktoré spáchali trestný čin.

Článok 13
Sankcie a opatrenia

1. Každá strana prijme potrebné legislatívne a iné opatrenia, aby sa trestné činy vymedzené v článkoch 2 až 11 trestali účinnými, primeranými a odrádzajúcimi sankciami vrátane odňatia slobody.
2. Každá strana zabezpečí, aby právnické osoby zodpovedné podľa článku 12 podliehali účinným, primeraným a odrádzajúcim trestnoprávnym alebo netrestnoprávnym sankciám alebo opatreniam vrátane peňažných sankcií.

Oddiel 2
Procesné právo

HLAVA 1
SPOLOČNÉ USTANOVENIA

Článok 14
Rozsah procesných ustanovení

1. Každá strana prijme potrebné legislatívne a iné opatrenia na vymedzenie právomocí a postupov ustanovených v tomto oddiele na účely špecifického vyšetrovania alebo konania v trestných veciach.

2. Ak článok 21 neustanovuje inak, každá strana uplatní právomoci a postupy uvedené v odseku 1 na

   a) trestné činy vymedzené podľa článkov 2 až 11,

   b) iné trestné činy spáchané prostredníctvom počítačového systému a

   c) zhromažďovanie dôkazov o trestnom čine v elektronickej forme.

   3.

   a) Každá strana si môže vyhradiť právo uplatňovať opatrenia uvedené v článku 20 iba na trestné činy alebo kategórie trestných činov uvedené vo výhrade za predpokladu, že rozsah takých trestných činov alebo kategórií trestných činov nie je obmedzený viac ako rozsah tých trestných činov, na ktoré uplatňuje opatrenia uvedené v článku 21. Každá strana zváži obmedzenie takej výhrady, aby umožnila čo najširšie uplatňovanie opatrenia uvedeného v článku 20.

   b) Ak strana nie je schopná v dôsledku obmedzení v jej legislatíve platnej v čase prijatia tohto dohovoru uplatniť opatrenia uvedené v článkoch 20 a 21 na komunikácie uskutočňované v rámci počítačového systému poskytovateľa služieb, ktorý
   i. je prevádzkovaný v prospech uzavretej skupiny užívateľov a
   ii. nevyužíva verejné komunikačné siete a nie je prepojený s iným počítačovým systémom verejným alebo súkromným,

môže si vyhradiť právo neuplatňovať tieto opatrenia na také komunikácie. Každá strana zváži obmedzenie takej výhrady, aby umožnila čo najširšie uplatňovanie opatrenia uvedeného v článkoch 20 a 21.

Článok 15
Podmienky a záruky

1. Každá strana zabezpečí, aby určenie, vykonávanie a uplatňovanie právomocí a postupov vymedzených v tomto oddiele podliehali podmienkam a zárukám jej vnútroštátneho právneho poriadku, ktoré zabezpečujú primeranú ochranu ľudských práv a slobôd vrátane práv vyplývajúcich zo záväzkov, ktoré prijala podľa Dohovoru o ochrane ľudských práv a základných slobôd z roku 1950, Medzinárodného paktu o občianskych a politických právach z roku 1966, ako aj podľa ostatných použiteľných medzinárodných dokumentov o ľudských právach a ktoré obsahujú zásadu primeranosti.

2. Také podmienky a záruky zahŕňajú so zreteľom na charakter danej právomoci alebo postupu okrem iného justičný alebo iný nezávislý dohľad, dôvody oprávňujúce použitie takej právomoci alebo postupu, obmedzenie rozsahu ich pôsobnosti a ich trvanie.

3. Ak je to zlučiteľné s verejným záujmom, najmä s riadnym výkonom spravodlivosti, každá strana posúdi dosah právomocí a postupov v tomto oddiele na práva, povinnosti a oprávnené záujmy tretích strán.

HLAVA 2
URÝCHLENÉ UCHOVANIE ULOŽENÝCH POČÍTAČOVÝCH ÚDAJOV

Článok 16
Urýchlené uchovanie uložených počítačových údajov

1. Každá strana prijme potrebné legislatívne a iné opatrenia, aby umožnila jej príslušným orgánom nariadiť alebo podobným spôsobom zabezpečiť urýchlené uchovanie určených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, najmä ak existujú dôvody domnievať sa, že hrozí osobitné riziko straty alebo pozmenenia týchto počítačových údajov.
2. Ak strana vykonáva odsek 1 formou príkazu osobe, aby uchovala určené uložené počítačové údaje nachádzajúce sa v držbe alebo pod kontrolou tejto osoby, táto strana prijme potrebné legislatívne a iné opatrenia na uloženie povinnosti tejto osobe uchovať a udržať celistvosť týchto počítačových údajov na potrebný čas, najviac však 90 dní, aby príslušné orgány mohli urobiť kroky na ich sprístupnenie. Strana môže stanoviť, že taký príkaz sa môže následne obnoviť.
3. Každá strana prijme potrebné legislatívne a iné opatrenia, aby zaviazala správcu alebo inú osobu, ktorá má uchovať počítačové údaje, aby neposkytla informáciu o prijatí takých postupov po čas ustanovený jej vnútroštátnym právnym poriadkom.
4. Právomoci a postupy uvedené v tomto článku podliehajú článkom 14 a 15.

Článok 17
Urýchlené uchovanie a čiastočné sprístupnenie prevádzkových údajov

1. Každá strana prijme vo vzťahu k prevádzkovým údajom, ktoré majú byť uchované podľa článku 16, potrebné legislatívne a iné opatrenia na

a) zabezpečenie toho, aby také urýchlené uchovanie prevádzkových údajov bolo možné bez ohľadu na to, či do prenosu komunikácie bol zapojený jeden poskytovateľ služieb alebo viac poskytovateľov služieb a

b) zabezpečenie urýchleného sprístupnenia dostatočného množstva prevádzkových údajov príslušným orgánom tejto strany alebo osobe určenej týmto orgánom, ktoré umožní strane identifikovať poskytovateľov služieb a trasu prenosu komunikácie.

2. Právomoci a postupy uvedené v tomto článku podliehajú článkom 14 a 15.

HLAVA 3
PRÍKAZ NA PREDLOŽENIE

Článok 18
Príkaz na predloženie

1. Každá strana prijme potrebné legislatívne alebo iné opatrenia, aby jej príslušné orgány mohli nariadiť

   a) osobe na jej území predloženie určených počítačových údajov, ktoré sú v držbe alebo pod kontrolou tejto osoby, uložených v počítačovom systéme alebo na pamäťovom nosiči počítačových údajov, a

   b) poskytovateľovi služieb, ktorý ponúka svoje služby na území tejto strany, predloženie informácií o predplatiteľovi týkajúcich sa takých služieb, ktoré sú v držbe alebo pod kontrolou poskytovateľa.

2. Právomoci a postupy uvedené v tomto článku podliehajú článkom 14 a 15.
3. Na účely tohto článku sa „informáciou o predplatiteľovi“ rozumie každá informácia obsiahnutá vo forme počítačových údajov alebo v inej forme, ktorú má k dispozícii poskytovateľ služieb, odlišná od prevádzkových alebo obsahových údajov týkajúca sa predplatiteľov jeho služieb a na ktorej základe možno zistiť

   a) typ použitej komunikačnej služby, technické opatrenia prijaté v súvislosti s ňou a obdobie trvania služby,

b) totožnosť predplatiteľa, poštovú alebo zemepisnú adresu, telefónne a iné prístupové číslo, informácie o účtoch a platbách, ktoré sú dostupné na základe dohody alebo dojednania o poskytovaní služieb,

c) iné informácie o mieste inštalácie komunikačného zariadenia, ktoré sú dostupné na základe dohody alebo dojednania o poskytovaní služieb.

HLAVA 4
PREHLIADKA A ZAISTENIE ULOŽENÝCH POČÍTAČOVÝCH ÚDAJOV

Článok 19
Prehliadka a zaistenie uložených počítačových údajov

1. Každá strana prijme potrebné legislatívne alebo iné opatrenia na udelenie oprávnenia jej príslušným orgánom na prehliadku alebo podobný prístup

   a) do počítačového systému alebo do jeho časti a k počítačovým údajom v ňom uloženým a

   b) k pamäťovému nosiču počítačových údajov, na ktorom môžu byť uložené počítačové údaje na jej území.

2. Každá strana prijme potrebné legislatívne alebo iné opatrenia na zabezpečenie toho, aby v prípade, keď jej príslušné orgány prehliadajú alebo podobne vstupujú do určeného počítačového systému alebo do jeho časti podľa odseku 1 písm. a) a majú dôvody domnievať sa, že hľadané údaje sú uložené v inom počítačovom systéme alebo v jeho časti na jej území a že také údaje sú zákonne prístupné z pôvodného systému alebo sú pre tento systém prístupné, tieto orgány boli oprávnené urýchlene rozšíriť prehliadku alebo podobný prístup aj na tento iný systém.

3. Každá strana prijme potrebné legislatívne alebo iné opatrenia na udelenie oprávnenia jej príslušným orgánom zaistiť alebo podobne zabezpečiť počítačové údaje, ku ktorým získali prístup podľa odseku 1 alebo 2. Tieto opatrenia zahŕňajú oprávnenie

   a) zaistiť alebo podobne zabezpečiť počítačový systém alebo jeho časť, alebo pamäťový nosič počítačových údajov,

   b) vyhotoviť a ponechať si kópiu týchto počítačových údajov,

   c) zachovať celistvosť relevantných uložených počítačových údajov,

   d) znemožniť prístup k takým počítačovým údajom alebo ich odstrániť z počítačového systému, do ktorého sa vstúpilo.

4. Každá strana prijme potrebné legislatívne alebo iné opatrenia na udelenie oprávnenia jej príslušným orgánom nariadiť osobe, ktorá má poznatky o fungovaní počítačového systému alebo o opatreniach použitých na ochranu počítačových údajov v tomto systéme, aby v primeranom rozsahu poskytla informácie potrebné na prijatie opatrení uvedených v odsekoch 1 a 2.

5. Právomoci a postupy uvedené v tomto článku podliehajú článkom 14 a 15.

HLAVA 5
ZHROMAŽĎOVANIE POČÍTAČOVÝCH ÚDAJOV V REÁLNOM ČASE

Článok 20
Zhromažďovanie prevádzkových údajov v reálnom čase

1. Každá strana prijme potrebné legislatívne alebo iné opatrenia na udelenie oprávnenia jej príslušným orgánom

   a) zhromažďovať alebo zaznamenávať použitím technických prostriedkov na území tejto strany a

   b) prinútiť poskytovateľa služieb v rámci jeho existujúcej technickej vybavenosti
   i. zhromažďovať alebo zaznamenávať použitím technických prostriedkov na území tejto strany alebo
   ii. spolupracovať a pomáhať príslušným orgánom zhromažďovať alebo zaznamenávať

prevádzkové údaje v reálnom čase súvisiace s určenými komunikáciami prenášané na jej území prostredníctvom počítačového systému.

2. Ak strana nemôže prijať opatrenia uvedené v odseku 1 písm. a) v dôsledku zásad uplatňovaných v jej vnútroštátnom právnom poriadku, môže namiesto toho prijať potrebné legislatívne alebo iné opatrenia na zabezpečenie zhromažďovania alebo zaznamenávania prevádzkových údajov v reálnom čase, ktoré súvisia s určenými komunikáciami, prenášaných na jej území použitím technických prostriedkov na tomto území.
3. Každá strana prijme potrebné legislatívne alebo iné opatrenia na uloženie povinnosti prevádzkovateľovi služieb, aby neposkytol informáciu o výkone oprávnenia ustanoveného v tomto článku ani žiadnu informáciu súvisiacu s týmto výkonom.
4. Právomoci a postupy uvedené v tomto článku podliehajú článkom 14 a 15.

Článok 21

Zachytenie obsahových údajov

1. Každá strana prijme potrebné legislatívne alebo iné opatrenia vo vzťahu ku skupine závažných trestných činov, ktoré vymedzí vo svojom vnútroštátnom právnom poriadku, aby ustanovila právomoc jej príslušných orgánov v reálnom čase

   a) zhromažďovať alebo zaznamenávať použitím technických prostriedkov na území tejto strany a

   b) prinútiť poskytovateľa služieb v rámci jeho existujúcej technickej vybavenosti
   i. zhromažďovať alebo zaznamenávať použitím technických prostriedkov na území tejto strany alebo
   ii. spolupracovať a pomáhať príslušným orgánom zhromažďovať alebo zaznamenávať

obsahové údaje určených komunikácií prenášané na jej území prostredníctvom počítačového systému.

2. Ak strana nemôže prijať opatrenia uvedené v odseku 1 písm. a) v dôsledku zásad uplatňovaných v jej vnútroštátnom právnom poriadku, môže namiesto toho prijať potrebné legislatívne alebo iné opatrenia na zabezpečenie zhromažďovania alebo zaznamenávania obsahových údajov v reálnom čase o určených komunikáciách na jej území použitím technických prostriedkov na tomto území.
3. Každá strana prijme potrebné legislatívne alebo iné opatrenia na uloženie povinnosti poskytovateľovi služieb, aby neposkytol informáciu o výkone oprávnenia ustanoveného v tomto článku ani žiadnu informáciu súvisiacu s týmto výkonom.
4. Právomoci a postupy uvedené v tomto článku podliehajú článkom 14 a 15.

Oddiel 3

Právomoc

Článok 22

Právomoc

1. Každá strana prijme potrebné legislatívne alebo iné opatrenia, aby mala právomoc konať o trestných činoch ustanovených podľa článkov 2 až 11, ak trestný čin bol spáchaný

   a) na jej území alebo

   b) na palube lode plávajúcej pod vlajkou tejto strany, alebo

   c) na palube lietadla registrovaného podľa právneho poriadku tejto strany, alebo

   d) jej občanom, ak je tento čin trestný podľa právneho poriadku miesta, kde bol spáchaný, alebo ak miesto spáchania trestného činu nie je územím žiadneho štátu.

2. Každá strana si môže vyhradiť právo neuplatňovať alebo uplatňovať iba v osobitných prípadoch alebo za osobitných okolností právomoc podľa odseku 1 písm. b) až d) tohto článku alebo jeho časti.
3. Každá strana prijme potrebné legislatívne alebo iné opatrenia, aby mala právomoc konať o trestných činoch uvedených v článku 24 ods. 1 v prípadoch, ak sa údajný páchateľ nachádza

na jej území a táto strana ho po podaní žiadosti o vydanie nevydá druhej strane výlučne z dôvodu jeho štátneho občianstva.

4. Tento dohovor nevylučuje trestnú právomoc strany vykonávanú podľa jej vnútroštátneho právneho poriadku.

5. Ak viac strán má právomoc konať o údajnom trestnom čine vymedzenom v tomto dohovore, dotknuté strany, ak je to vhodné, navzájom konzultujú, aby určili, kde je najvhodnejšie miesto na trestné stíhanie.

KAPITOLA III
MEDZINÁRODNÁ SPOLUPRÁCA

Oddiel 1
Všeobecné zásady

HLAVA 1
VŠEOBECNÉ ZÁSADY TÝKAJÚCE SA MEDZINÁRODNEJ SPOLUPRÁCE

Článok 23
Všeobecné zásady týkajúce sa medzinárodnej spolupráce

Strany spolupracujú v súlade s ustanoveniami tejto kapitoly a s použitím príslušných medzinárodných nástrojov na medzinárodnú spoluprácu v trestných veciach, dojednaní prijatých na základe vzorového zákona alebo vzájomnosti a vnútroštátnych zákonov v čo najväčšom rozsahu na účely vyšetrovania alebo konania o trestných činoch súvisiacich s počítačovými systémami a údajmi alebo na zhromažďovanie dôkazov o trestnom čine v elektronickej forme.

HLAVA 2
ZÁSADY TÝKAJÚCE SA EXTRADÍCIE

Článok 24
Extradícia

1.

a) Tento článok sa použije na vydanie medzi stranami pre trestné činy vymedzené podľa článkov 2 až 11 tohto dohovoru za predpokladu, že podľa právnych poriadkov oboch dotknutých strán za ne možno uložiť trest odňatia slobody alebo ochranné opatrenie s hornou hranicou najmenej jeden rok alebo prísnejší trest.

b) Ak sa podľa dojednania prijatého na základe vzorového zákona alebo vzájomnosti, alebo extradičnej zmluvy vrátane Európskeho dohovoru o vydávaní (ETS č. 24), ktoré sa dajú použiť medzi dvoma alebo viacerými stranami, má uplatniť iný minimálny trest, použije sa minimálny trest ustanovený takým dojednaním alebo zmluvou.

2. Trestné činy uvedené v odseku 1 sa považujú za extradičné trestné činy v každej extradičnej zmluve, ktorou sú navzájom viazané. Strany sa zaväzujú zahrnúť také trestné činy ako extradičné do každej extradičnej zmluvy, ktorú medzi sebou uzatvoria.

3. Ak strana, ktorá podmieňuje vydanie existenciou zmluvy, dostane žiadosť o vydanie od inej strany, s ktorou nemá uzatvorenú extradičnú zmluvu, môže považovať tento dohovor za právny základ na vydanie vo vzťahu ku každému trestnému činu uvedenému v odseku 1.

4. Strany, ktoré nepodmieňujú vydanie existenciou zmluvy, uznávajú medzi sebou trestné činy uvedené v odseku 1 za extradičné trestné činy.

5. Vydanie podlieha podmienkam ustanoveným právnym poriadkom dožiadanej strany alebo použiteľnými extradičnými zmluvami vrátane dôvodov, na ktorých základe môže dožiadaná strana odmietnuť vydanie.

6. Ak sa vydanie za trestný čin uvedený v odseku 1 odmietne výlučne z dôvodu štátneho občianstva vyžiadanej osoby alebo z dôvodu, že dožiadaná strana zastáva názor, že má právomoc konať o trestnom čine, dožiadaná strana predloží prípad na žiadosť dožadujúcej

strany svojim príslušným orgánom na účely trestného stíhania a v primeranej lehote podá správu o konečnom výsledku dožadujúcej strane. Tieto orgány prijmú rozhodnutie a vedú vyšetrovanie a konanie rovnakým spôsobom ako v prípade trestných činov porovnateľnej povahy podľa právneho poriadku tejto strany.

7.

a) Každá strana oznámi pri podpise alebo pri ukladaní svojej ratifikačnej listiny, listiny o prijatí, schválení alebo o prístupe generálnemu tajomníkovi Rady Európy názov a adresu každého orgánu zodpovedného za zasielanie alebo prijímanie žiadostí o vydanie alebo za predbežnú väzbu v prípade, ak neexistuje zmluva.

b) Generálny tajomník zriadi a aktualizuje register orgánov takto určených stranami. Každá strana priebežne zabezpečuje správnosť jednotlivých údajov v registri.

HLAVA 3
VŠEOBECNÉ ZÁSADY TÝKAJÚCE SA PRÁVNEJ POMOCI

Článok 25
Všeobecné zásady týkajúce sa právnej pomoci

1. Strany si poskytujú pomoc v čo najširšom rozsahu na účely vyšetrovania alebo konania o trestných činoch súvisiacich s počítačovými systémami a údajmi alebo na zhromažďovanie dôkazov o trestnom čine v elektronickej forme.
2. Každá strana tiež prijme potrebné legislatívne alebo iné opatrenia na plnenie záväzkov ustanovených v článkoch 27 až 35.
3. Každá strana môže za naliehavých okolností zasielať žiadosti o právnu pomoc alebo s nimi súvisiacu korešpondenciu prostredníctvom rýchlych komunikačných prostriedkov vrátane faxu alebo elektronickej pošty v rozsahu, v akom tie prostriedky poskytujú primeranú úroveň bezpečnosti a hodnovernosti (vrátane použitia šifrovania, ak je potrebné), s nasledujúcim formálnym potvrdením, ak to vyžaduje dožiadaná strana. Dožiadaná strana prijme žiadosť a odpovie na ňu akýmkoľvek z rýchlych komunikačných prostriedkov.
4. Ak články tejto kapitoly osobitne neustanovujú inak, právna pomoc závisí od podmienok ustanovených právnym poriadkom dožiadanej strany alebo použiteľnými zmluvami o právnej pomoci vrátane dôvodov, na ktorých základe môže dožiadaná strana odmietnuť spoluprácu. Dožiadaná strana neuplatní právo odmietnuť právnu pomoc vo vzťahu k trestným činom uvedeným v článkoch 2 až 11 výlučne z dôvodu, že žiadosť sa týka trestného činu, ktorý považuje za fiškálny trestný čin.
5. Ak dožiadaná strana môže v súlade s ustanoveniami tejto kapitoly podmieniť právnu pomoc existenciou obojstrannej trestnosti, považuje sa tá podmienka za splnenú bez ohľadu na to, či jej právny poriadok zaraďuje toto protiprávne konanie do tej istej kategórie protiprávnych konaní, alebo označuje toto protiprávne konanie rovnakou terminológiou ako dožadujúca strana, ak je konanie, ktoré charakterizuje toto protiprávne konanie, kvôli ktorému sa žiada o pomoc, trestným činom podľa jej právneho poriadku.

Článok 26
Spontánne informácie

1. Strana môže v medziach svojho vnútroštátneho právneho poriadku a bez predchádzajúcej žiadosti zaslať druhej strane informácie získané počas vyšetrovania, ak sa domnieva, že poskytnutie takých informácií by mohlo pomôcť prijímajúcej strane začať alebo vykonať vyšetrovanie alebo trestné konanie o trestných činoch vymedzených v tomto dohovore alebo by mohli viesť k podaniu žiadosti o spoluprácu touto stranou podľa tejto kapitoly.
2. Pred poskytnutím takých informácií môže poskytujúca strana požadovať zachovanie ich dôvernosti alebo podmieniť ich použitie za určitých podmienok. Ak prijímajúca strana nemôže vyhovieť tejto žiadosti, upovedomí o tom poskytujúcu stranu, ktorá určí, či informácie aj napriek tomu poskytne. Ak prijímajúca strana prijme informácie, ktoré podliehajú takým podmienkam, je nimi viazaná.

HLAVA 4
POSTUPY VZŤAHUJÚCE SA NA ŽIADOSTI O PRÁVNU POMOC V PRÍPADE, KEĎ NEEXISTUJÚ POUŽITEĽNÉ MEDZINÁRODNÉ DOHODY

Článok 27
Postupy vzťahujúce sa na žiadosti o vzájomnú pomoc v prípade, keď neexistujú použiteľné medzinárodné dohody

1. Ak medzi dožadujúcou a dožiadanou stranou neexistuje zmluva alebo dojednanie o právnej pomoci na základe vzorového zákona alebo vzájomnosti, použijú sa ustanovenia odsekov 2 až 9. Ustanovenia tohto článku sa nepoužijú, ak existuje taká zmluva, dojednanie alebo zákon, alebo vzájomnosť, že ak sa dotknuté strany nedohodnú, namiesto nich uplatnia niektoré alebo všetky ostatné odseky tohto článku.

2.

a) Každá strana určí ústredný orgán alebo orgány, ktoré sú zodpovedné za zasielanie žiadostí o právnu pomoc a za odpovedanie na tieto žiadosti, vybavovanie takých žiadostí alebo ich predloženie orgánom príslušným na ich vybavenie.

b) Ústredné orgány komunikujú medzi sebou priamo.

c) Každá strana pri podpise alebo pri uložení svojej ratifikačnej listiny, listiny o prijatí, schválení alebo o prístupe oznámi generálnemu tajomníkovi Rady Európy názvy a adresy orgánov určených podľa tohto odseku.

d) Generálny tajomník Rady Európy zriadi a aktualizuje register ústredných orgánov určených stranami. Každá strana priebežne zabezpečuje správnosť jednotlivých údajov v registri.

3. Žiadosti o právnu pomoc podľa tohto článku sa vybavujú v súlade s postupmi určenými dožadujúcou stranou okrem prípadov, keď sú tieto postupy nezlučiteľné s právnym poriadkom dožiadanej strany.

4. Dožiadaná strana môže okrem dôvodov odmietnutia vymedzených v článku 25 ods. 4 odmietnuť pomoc, ak sa

a) žiadosť týka trestného činu, ktorý dožiadaná strana považuje za politický trestný čin alebo za trestný čin súvisiaci s politickým trestným činom, alebo

b) domnieva, že vybavením žiadosti by pravdepodobne došlo k narušeniu jej zvrchovanosti, bezpečnosti, verejného poriadku alebo iných zásadných záujmov.

5. Dožiadaná strana môže odložiť vybavenie žiadosti, ak by jej vybavenie mohlo negatívne ovplyvniť vyšetrovanie alebo trestné konanie vedené jej orgánmi.

6. Dožiadaná strana predtým, ako odmietne alebo odloží vykonanie právnej pomoci, vo vhodných prípadoch po konzultácii s dožadujúcou stranou zváži, či by nemohla žiadosť vybaviť čiastočne alebo pri splnení ňou uložených podmienok.

7. Dožiadaná strana okamžite informuje dožadujúcu stranu o výsledku vybavenia žiadosti o právnu pomoc. Každé odmietnutie alebo odloženie vybavenia žiadosti sa odôvodní. Dožiadaná strana informuje dožadujúcu stranu aj o dôvodoch, pre ktoré nie je možné vybaviť žiadosť alebo ktoré môžu spôsobiť významný odklad jej vybavenia.

8. Dožadujúca strana môže žiadať, aby dožiadaná strana zachovala mlčanlivosť o skutočnosti, že bola podaná žiadosť podľa tejto kapitoly, ako aj o jej predmete, okrem rozsahu nevyhnutného na jej vybavenie. Ak dožiadaná strana nemôže splniť požiadavku na zachovanie mlčanlivosti, okamžite o tom informuje dožadujúcu stranu, ktorá určí, či sa má žiadosť aj napriek tomu vybaviť.

9.

a) V naliehavých prípadoch môžu žiadosti o právnu pomoc alebo s nimi súvisiacu korešpondenciu zasielať priamo justičné orgány dožadujúcej strany justičným orgánom dožiadanej strany. V každom takom prípade sa súčasne zašle kópia ústrednému orgánu dožiadanej strany prostredníctvom ústredného orgánu dožadujúcej strany.

b) Každú žiadosť alebo korešpondenciu podľa tohto odseku možno zaslať prostredníctvom Medzinárodnej organizácie kriminálnej polície (Interpol).

c) Ak sa žiadosť zašle podľa písmena a) tohto odseku a daný orgán nie je príslušný na jej vybavenie, postúpi žiadosť príslušnému štátnemu orgánu a priamo o tom informuje dožadujúcu stranu.

d) Žiadosti alebo korešpondenciu zaslanú podľa tohto odseku, ktoré neobsahujú donucovací úkon, môžu zasielať príslušné orgány dožadujúcej strany priamo príslušným orgánom dožiadanej strany.

e) Každá strana môže pri podpise alebo pri uložení svojej ratifikačnej listiny, listiny o prijatí, schválení alebo o prístupe informovať generálneho tajomníka Rady Európy, že žiadosti podľa tohto odseku sa majú z dôvodu efektívnosti zasielať jej ústrednému orgánu.

Článok 28

Dôvernosť a obmedzenie použitia

1. Ak medzi dožadujúcou a dožiadanou stranou neexistuje zmluva alebo dojednanie o právnej pomoci na základe vzorového zákona alebo vzájomnosti, použijú sa ustanovenia tohto článku. Ustanovenia tohto článku sa nepoužijú, ak existuje taká zmluva, dojednanie, zákon alebo vzájomnosť, ak sa dotknuté strany nedohodnú, že namiesto nich uplatnia niektoré alebo všetky ostatné odseky tohto článku.
2. Dožiadaná strana môže v odpovedi na žiadosť podmieniť poskytnutie informácií alebo materiálov tým, že sa
   a) zachová ich dôvernosť, ak nemožno vyhovieť žiadosti o vzájomnú právnu pomoc bez splnenia tejto podmienky, alebo
   b) nepoužijú na iné vyšetrovania alebo trestné konania ako tie, ktoré sú uvedené v žiadosti.
3. Ak dožadujúca strana nemôže vyhovieť podmienke ustanovenej v odseku 2, okamžite o tom informuje druhú stranu, ktorá potom určí, či informácie aj napriek tomu poskytne. Ak dožadujúca strana tieto podmienky prijme, je nimi viazaná.
4. Každá strana, ktorá poskytne informácie alebo materiály podliehajúce podmienke uvedenej v odseku 2, môže požadovať od druhej strany, aby vo vzťahu k tejto podmienke vysvetlila, ako sa informácie alebo materiály použili.

Oddiel 2

Osobitné ustanovenia

HLAVA 1

PRÁVNA POMOC TÝKAJÚCA SA PREDBEŽNÝCH OPATRENÍ

Článok 29

Urýchlené uchovanie uložených počítačových údajov

1. Strana môže požiadať inú stranu, aby nariadila alebo inak zabezpečila urýchlené uchovanie údajov uložených prostredníctvom počítačového systému umiestneného na území tej inej strany a vo vzťahu ku ktorému má dožadujúca strana záujem zaslať žiadosť o právnu pomoc týkajúcu sa prehliadky alebo podobného prístupu, zaistenia alebo podobného zabezpečenia alebo sprístupnenia údajov.
2. V žiadosti o uchovanie údajov podanej podľa odseku 1 sa uvedie
   a) orgán žiadajúci o uchovanie,
   b) trestný čin, ktorý je predmetom vyšetrovania alebo trestného konania, a stručný súhrn súvisiacich skutočností,
   c) uložené počítačové údaje, ktoré sa majú uchovať, a ich súvis s trestným činom,
   d) dostupné informácie preukazujúce totožnosť správcu uložených počítačových údajov alebo umiestnenie počítačového systému,
   e) dôvod uchovania a

f) záujem strany predložiť žiadosť o právnu pomoc týkajúcu sa prehliadky alebo podobného prístupu, zaistenia alebo podobného zabezpečenia, alebo sprístupnenia uložených počítačových údajov.

3. Po doručení žiadosti inej strany prijme dožiadaná strana všetky vhodné opatrenia na urýchlené uchovanie určených údajov v súlade s jej vnútroštátnym právnym poriadkom. Na účely vybavenia žiadosti sa obojstranná trestnosť nevyžaduje ako podmienka na zabezpečenie takého uchovania údajov.

4. Strana, ktorá vyžaduje obojstrannú trestnosť ako podmienku na vybavenie žiadosti o právnu pomoc týkajúcu sa prehliadky alebo podobného prístupu, zaistenia alebo podobného zabezpečenia, alebo sprístupnenia uložených údajov, si môže vo vzťahu k iným trestným činom ako tým, ktoré sú ustanovené v článkoch 2 až 11 tohto dohovoru, vyhradiť právo odmietnuť žiadosť o ich uchovanie podľa tohto článku v prípadoch, v ktorých má dôvody domnievať sa, že v čase sprístupnenia nie je možné splniť podmienku obojstrannej trestnosti.

5. Okrem toho žiadosť o uchovanie možno odmietnuť iba vtedy, ak

a) sa žiadosť týka trestného činu, ktorý dožiadaná strana považuje za politický trestný čin alebo za trestný čin súvisiaci s politickým trestným činom, alebo

b) dožiadaná strana sa domnieva, že vybavením žiadosti by mohlo dôjsť k narušeniu jej zvrchovanosti, bezpečnosti, verejného poriadku alebo iných zásadných záujmov.

6. Ak sa dožiadaná strana domnieva, že uchovanie nezabezpečí dostupnosť údajov v budúcnosti alebo že ohrozí dôvernosť vyšetrovania dožadujúcej strany, alebo ho inak naruší, okamžite o tom informuje dožadujúcu stranu, ktorá potom určí, či sa má žiadosť aj napriek tomu vykonať.

7. Každé uchovanie vykonané na základe žiadosti uvedenej v odseku 1 trvá najmenej počas 60 dní, aby dožadujúca strana mohla predložiť žiadosť o prehliadku alebo podobný prístup, zaistenie alebo podobné zabezpečenie, alebo sprístupnenie údajov. Po doručení takej žiadosti ostanú údaje naďalej uchované do času, kým sa o nej nerozhodne.

Článok 30

Urýchlené sprístupnenie uchovaných prevádzkových údajov

1. Ak dožiadaná strana počas vybavovania žiadosti o uchovanie prevádzkových údajov týkajúcich sa určenej komunikácie zaslanej podľa článku 29 zistí, že do prenosu tej komunikácie bol zapojený poskytovateľ služieb v inom štáte, dožiadaná strana urýchlene sprístupní dožadujúcej strane dostatočné množstvo prevádzkových údajov na určenie totožnosti tohto poskytovateľa služieb a trasy, po ktorej sa uskutočnila komunikácia.

2. Sprístupnenie prevádzkových údajov podľa odseku 1 možno odmietnuť iba vtedy, ak

a) sa žiadosť týka trestného činu, ktorý dožiadaná strana považuje za politický trestný čin alebo trestný čin súvisiaci s politickým trestným činom, alebo

b) dožiadaná strana sa domnieva, že vybavením žiadosti by mohlo dôjsť k narušeniu jej zvrchovanosti, bezpečnosti, verejného poriadku alebo iných zásadných záujmov.

HLAVA 2

VZÁJOMNÁ POMOC TÝKAJÚCA SA VYŠETROVACÍCH PRÁVOMOCÍ

Článok 31

Vzájomná pomoc týkajúca sa prístupu k uloženým počítačovým údajom

1. Strana môže požiadať inú stranu, aby vykonala prehliadku alebo podobne sprístupnila, zaistila alebo podobne zabezpečila, alebo sprístupnila údaje uložené počítačovým systémom umiestneným na území dožiadanej strany vrátane údajov uchovaných podľa článku 29.

2. Dožiadaná strana vybaví žiadosť s použitím medzinárodných nástrojov, dojednaní a zákonov uvedených v článku 23 a v súlade s ostatnými relevantnými ustanoveniami tejto kapitoly.

3. Žiadosť sa vybaví urýchleným spôsobom, ak

a) existujú dôvody domnievať sa, že hrozí osobitné riziko straty alebo pozmenenia týchto počítačových údajov, alebo

b) nástroje, dojednania a zákony uvedené v odseku 2 inak upravujú urýchlenú spoluprácu.

Článok 32

Cezhraničný prístup k uloženým počítačovým údajom so súhlasom alebo v prípadoch, keď sú verejne prístupné

Strana môže bez povolenia inou stranou

a) pristupovať k verejne dostupným (otvorené zdroje) uloženým počítačovým údajom bez ohľadu na to, na ktorom území sa tie údaje nachádzajú, alebo

b) počítačovým systémom z jej územia pristupovať alebo prijímať uložené počítačové údaje nachádzajúce sa na území druhej strany, ak tá strana získa zákonný a dobrovoľný súhlas osoby, ktorá je zo zákona oprávnená sprístupniť údaje strane cez tento počítačový systém.

Článok 33

Vzájomná pomoc pri zhromažďovaní prevádzkových údajov v reálnom čase

1. Strany si poskytujú pomoc pri zhromažďovaní prevádzkových údajov v reálnom čase, ktoré súvisia s určenými komunikáciami na ich území, prenášaných počítačovým systémom. Okrem ustanovení odseku 2 sa táto pomoc riadi podmienkami a postupmi ustanovenými vo vnútroštátnom právnom poriadku.
2. Každá strana poskytne takú pomoc aspoň vo vzťahu k trestným činom, pri ktorých by zhromažďovanie prevádzkových údajov v reálnom čase bolo možné v podobnom vnútroštátnom prípade.

Článok 34

Vzájomná pomoc týkajúca sa zachytenia obsahových údajov

Strany si poskytujú pomoc pri zhromažďovaní alebo zaznamenávaní obsahových údajov určených komunikácií v reálnom čase, prenášaných počítačovým systémom v rozsahu prípustnom podľa ich použiteľných zmlúv a vnútroštátnych právnych poriadkov.

HLAVA 3

SIEŤ 24/7

Článok 35

Sieť 24/7

1. Každá strana určí kontaktné miesto dostupné 24 hodín denne 7 dní v týždni na zabezpečenie poskytovania okamžitej pomoci na účel vyšetrovania alebo konania v prípade trestných činov súvisiacich s počítačovými systémami a údajmi, alebo na účel zhromažďovania dôkazov o trestnom čine v elektronickej forme. Taká pomoc zahŕňa uľahčenie, alebo ak to jej vnútroštátny právny poriadok a prax umožňujú, priame vykonanie týchto opatrení:
   a) poskytovanie technického poradenstva,
   b) uchovávanie údajov podľa článkov 29 a 30 a
   c) zhromažďovanie dôkazov, poskytnutie právnych informácií a lokalizovanie podozrivých osôb.
   2.
   a) Kontaktné miesto strany musí byť schopné realizovať urýchlenú komunikáciu s kontaktným miestom druhej strany.
   b) Ak kontaktné miesto, ktoré určila strana, nie je súčasťou orgánu alebo orgánov tej strany zodpovedných za medzinárodnú vzájomnú pomoc alebo vydávanie, kontaktné miesto zabezpečí, aby bolo schopné urýchlene zaistiť koordináciu s takým orgánom alebo orgánmi.
3. Každá strana zabezpečí vyškolený personál a potrebné vybavenie na uľahčenie prevádzky siete.

KAPITOLA IV
ZÁVEREČNÉ USTANOVENIA

Článok 36
Podpis a nadobudnutie platnosti

1. Tento dohovor je otvorený na podpis členským štátom Rady Európy a nečlenským štátom, ktoré sa zúčastnili na jeho vypracovaní.
2. Tento dohovor podlieha ratifikácii, prijatiu alebo schváleniu. Ratifikačné listiny, listiny o prijatí alebo schválení sa uložia u generálneho tajomníka Rady Európy.
3. Tento dohovor nadobudne platnosť prvý deň mesiaca nasledujúceho po uplynutí troch mesiacov odo dňa, keď päť štátov vrátane najmenej troch členských štátov Rady Európy vyjadrí súhlas byť viazané dohovorom v súlade s ustanoveniami odsekov 1 a 2.
4. Vo vzťahu ku každému signatárskemu štátu, ktorý vyjadrí súhlas byť viazaný dohovorom neskôr, nadobudne dohovor platnosť prvý deň mesiaca nasledujúceho po uplynutí troch mesiacov odo dňa, keď vyjadril súhlas byť viazaný dohovorom v súlade s ustanoveniami odsekov 1 a 2.

Článok 37
Pristúpenie k dohovoru

1. Po nadobudnutí platnosti tohto dohovoru môže Výbor ministrov Rady Európy po konzultácii a získaní jednomyseľného súhlasu zmluvných štátov dohovoru prizvať ktorýkoľvek nečlenský štát Rady, ktorý sa nezúčastnil na jeho vypracovaní, aby pristúpil k dohovoru. Rozhodnutie sa prijme väčšinou ustanovenou v článku 20 písm. d) Štatútu Rady Európy a jednomyseľným hlasovaním zástupcov zmluvných štátov oprávnených zasadať vo Výbore ministrov.
2. Vo vzťahu ku všetkým štátom, ktoré pristupujú k dohovoru podľa odseku 1, nadobudne dohovor platnosť prvý deň mesiaca nasledujúceho po uplynutí troch mesiacov odo dňa uloženia listiny o prístupe u generálneho tajomníka Rady Európy.

Článok 38
Územná pôsobnosť

1. Každý štát môže pri podpise alebo pri uložení svojej ratifikačnej listiny, listiny o prijatí, schválení alebo prístupe určiť územie alebo územia, na ktoré sa dohovor uplatní.
2. Každý štát môže kedykoľvek neskôr vyhlásením adresovaným generálnemu tajomníkovi Rady Európy rozšíriť pôsobnosť tohto dohovoru na akékoľvek iné územie uvedené vo vyhlásení. Vo vzťahu k takému územiu nadobudne dohovor platnosť prvý deň mesiaca nasledujúceho po uplynutí troch mesiacov odo dňa doručenia vyhlásenia generálnemu tajomníkovi.
3. Každé vyhlásenie urobené podľa predchádzajúcich dvoch odsekov možno odvolať vo vzťahu k akémukoľvek územiu označenému v tomto vyhlásení oznámením zaslaným generálnemu tajomníkovi Rady Európy. Odvolanie nadobúda platnosť prvý deň mesiaca nasledujúceho po uplynutí troch mesiacov odo dňa doručenia oznámenia generálnemu tajomníkovi.

Článok 39
Účinky dohovoru

1. Cieľom tohto dohovoru je doplniť použiteľné mnohostranné alebo dvojstranné zmluvy alebo dojednania medzi stranami vrátane ustanovení
   – Európskeho dohovoru o vydávaní otvoreného na podpis v Paríži 13. decembra 1957 (ETS č. 24),
   – Európskeho dohovoru o vzájomnej pomoci v trestných veciach otvoreného na podpis v Štrasburgu 20. apríla 1959 (ETS č. 30),
   – Dodatkového protokolu k Európskemu dohovoru o vzájomnej pomoci v trestných veciach otvoreného na podpis v Štrasburgu 17. marca 1978 (ETS č. 99).
2. Ak dve strany alebo viac strán už uzavreli dohodu alebo zmluvu o veciach, ktorými sa zaoberá tento dohovor, alebo upravili svoje vzťahy v tých veciach inou formou, alebo ak tak urobia v

budúcnosti, sú tiež oprávnené uplatňovať takú dohodu alebo zmluvu alebo postupovať podľa dojednanej úpravy. Ak však strany upravia svoje vzťahy vo veciach, ktorými sa zaoberá tento dohovor, odlišne od tohto dohovoru, musia tak urobiť spôsobom, ktorý neodporuje cieľom a zásadám dohovoru.

3. Nič v tomto dohovore nemá vplyv na iné práva, obmedzenia, záväzky či zodpovednosti strany.

Článok 40

Vyhlásenia

Každý štát môže písomným oznámením zaslaným generálnemu tajomníkovi Rady Európy pri podpise alebo uložení svojej ratifikačnej listiny, listiny o prijatí, schválení alebo prístupe vyhlásiť, že využíva možnosť ustanoviť dodatočné prvky upravené v článkoch 2, 3, článku 6 ods. 1 písm. b), článku 7, článku 9 ods. 3 a článku 27 ods. 9 písm. e).

Článok 41

Federálna doložka

1. Federálny štát si môže vyhradiť právo, že prevezme záväzky podľa kapitoly II tohto dohovoru, ktoré sú v súlade so základnými zásadami upravujúcimi vzťah medzi jeho federálnou vládou a štátmi alebo územnými celkami, ktoré tvoria federálny štát, za predpokladu, že je spôsobilý spolupracovať podľa kapitoly III.
2. Pri uplatnení výhrady podľa odseku 1 nesmie federálny štát formulovať podmienky takej výhrady tak, aby vylúčil alebo značne obmedzil svoje záväzky poskytovať opatrenia uvedené v kapitole II. Celkovo musí zabezpečiť širokú a účinnú schopnosť presadzovať právo vo vzťahu k tým opatreniam.
3. Pokiaľ ide o ustanovenia tohto dohovoru, ktorých uplatňovanie patrí do právomoci jednotlivých štátov alebo územných celkov, ktoré podľa ústavného systému federácie nie sú povinné prijímať legislatívne opatrenia, federálna vláda oboznámi príslušné orgány tých štátov o daných ustanoveniach so svojím kladným stanoviskom a bude ich nabádať, aby prijali kroky potrebné na ich uplatňovanie.

Článok 42

Výhrady

Každý štát môže písomným oznámením zaslaným generálnemu tajomníkovi Rady Európy pri podpise alebo pri uložení svojej ratifikačnej listiny, listiny o prijatí, schválení alebo prístupe vyhlásiť, že uplatňuje jednu výhradu alebo viaceré výhrady uvedené v článku 4 ods. 2, článku 6 ods. 3, článku 9 ods. 4, článku 10 ods. 3, článku 11 ods. 3, článku 14 ods. 3, článku 22 ods. 2, článku 29 ods. 4 a článku 41 ods. 1. Iné výhrady nie sú možné.

Článok 43

Stav a odvolanie výhrad

1. Strana, ktorá urobila výhradu podľa článku 42, môže ju úplne alebo čiastočne odvolať vyhlásením zaslaným generálnemu tajomníkovi Rady Európy. Odvolanie nadobúda platnosť v deň doručenia takého oznámenia generálnemu tajomníkovi. Ak sa v oznámení uvádza, že odvolanie výhrady nadobúda platnosť v deň uvedený v tomto oznámení, a ak tento dátum nastane po doručení oznámenia generálnemu tajomníkovi, odvolanie nadobúda platnosť od toho neskoršieho dátumu.
2. Strana, ktorá urobila výhradu uvedenú v článku 42, ju úplne alebo čiastočne odvolá ihneď, ako to umožnia okolnosti.
3. Generálny tajomník Rady Európy môže pravidelne zisťovať u strán, ktoré urobili jednu výhradu alebo viac výhrad uvedených v článku 42, aké sú možnosti na odvolanie takých výhrad alebo takej výhrady.

Článok 44

Zmeny

1. Zmeny tohto dohovoru môže navrhnúť každá strana a generálny tajomník Rady Európy ich oznámi členským štátom Rady Európy, nečlenským štátom, ktoré sa zúčastnili na vypracovaní tohto dohovoru, ako aj každému štátu, ktorý pristúpil alebo bol prizvaný, aby pristúpil k dohovoru v súlade s ustanoveniami článku 37.
2. Každá zmena navrhnutá stranou sa oznámi Európskemu výboru pre problémy kriminality (CDPC), ktorý predloží Výboru ministrov svoje stanovisko k navrhovanej zmene.
3. Výbor ministrov posúdi navrhovanú zmenu a stanovisko predložené Európskym výborom pre problémy kriminality (CDPC) a po konzultácii s nečlenskými štátmi, zmluvnými stranami, môže zmenu schváliť.
4. Text každej zmeny schválenej Výborom ministrov podľa odseku 3 sa zašle stranám na prijatie.
5. Každá zmena podľa odseku 3 nadobudne platnosť v tridsiaty deň po tom, ako všetky strany informovali generálneho tajomníka o jej prijatí.

Článok 45

Riešenie sporov

1. Európskemu výboru pre problémy kriminality (CDPC) sa priebežne poskytujú informácie o výklade a uplatňovaní tohto dohovoru.
2. V prípade sporu medzi stranami týkajúceho sa výkladu alebo uplatňovania tohto dohovoru sa strany budú snažiť o urovnanie sporu rokovaním alebo inými zmierlivými prostriedkami podľa vlastného výberu vrátane predloženia sporu Európskemu výboru pre problémy kriminality (CDPC) alebo rozhodcovskému súdu, ktorého rozhodnutie je záväzné pre strany, alebo Medzinárodnému súdnemu dvoru podľa dohody medzi dotknutými zmluvnými stranami.

Článok 46

Konzultácie strán

1. Strany budú podľa potreby pravidelne konzultovať s cieľom uľahčiť
   a) účinné používanie a vykonávanie tohto dohovoru vrátane identifikácie akýchkoľvek problémov s tým spojených, ako aj účinky každého vyhlásenia alebo výhrady urobenej podľa tohto dohovoru,
   b) výmenu informácií o významných právnych, všeobecných alebo technologických zmenách, ktoré sa týkajú počítačovej kriminality a zhromažďovania dôkazov v elektronickej forme,
   c) posudzovanie prípadných zmien alebo dodatkov k dohovoru.
2. Európskemu výboru pre problémy kriminality (CDPC) sa pravidelne poskytnú informácie o výsledkoch rokovaní uvedených v odseku 1.
3. Európsky výbor pre problémy kriminality (CDPC) podľa potreby uľahčí konzultácie uvedené v odseku 1 a prijme opatrenia potrebné na to, aby pomohol stranám v ich úsilí o zmeny alebo dodatky k dohovoru. Európsky výbor pre problémy kriminality (CDPC) v spolupráci so stranami preskúma najneskôr tri roky po nadobudnutí platnosti súčasného dohovoru všetky ustanovenia dohovoru, a ak je to potrebné, odporučí vhodné zmeny.
4. Náklady, ktoré vznikli pri vykonávaní odseku 1, hradia strany spôsobom, aký si určia, okrem prípadov, keď túto zodpovednosť prevezme Rada Európy.
5. Stranám pri vykonávaní úloh podľa tohto článku pomáha Sekretariát Rady Európy.

Článok 47

Výpoveď

1. Každá strana môže kedykoľvek vypovedať tento dohovor oznámením zaslaným generálnemu tajomníkovi Rady Európy.
2. Výpoveď nadobúda platnosť prvý deň mesiaca nasledujúceho po uplynutí troch mesiacov odo dňa doručenia oznámenia generálnemu tajomníkovi.

Článok 48

Oznámenie

Generálny tajomník Rady Európy informuje členské štáty Rady Európy, nečlenské štáty, ktoré sa zúčastnili na vypracovaní tohto dohovoru, ako aj každý štát, ktorý pristúpil k dohovoru alebo bol prizvaný, aby k nemu pristúpil, o

a) každom podpise,

b) uložení každej ratifikačnej listiny, listiny o prijatí, schválení alebo prístupe,

c) každom dátume nadobudnutia platnosti tohto dohovoru podľa článkov 36 a 37,

d) každom vyhlásení urobenom podľa článku 40 alebo výhrade urobenej v súlade s článkom 42,

e) každom inom úkone, oznámení alebo korešpondencii týkajúcich sa tohto dohovoru.

Na dôkaz toho podpísaní, riadne na to splnomocnení, podpísali tento dohovor.

Dané v Budapešti 23. novembra 2001 v anglickom a vo francúzskom jazyku, pričom obe znenia majú rovnakú platnosť, v jednom vyhotovení, ktoré sa uloží v archívoch Rady Európy. Generálny tajomník Rady Európy zašle overené kópie každému členskému štátu Rady Európy, nečlenským štátom, ktoré sa zúčastnili na vypracovaní tohto dohovoru, a každému inému štátu prizvanému na pristúpenie k dohovoru.

Dohovor o počítačovej kriminalite - anglická verzia

K oznámeniu č. 137/2008 Z. z.

CONVENTION
ON CYBERCRIME

Budapest, 23. XI. 2001

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.

Vydavateľ Zbierky zákonov Slovenskej republiky a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je Ministerstvo spravodlivosti Slovenskej republiky, Župné námestie 13, 813 11 Bratislava, tel.: 02 571 01 000, e-mail: helpdesk@slov-lex.sk.