Bijlagen

Bijlage I: Wet van 28 november 2000 inzake Informaticacriminaliteit

LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

MINISTERE DE LA JUSTICE

F. 2001 — 298 [S − C − 2001/09035]

28 NOVEMBRE 2000. — Loi du 28 novembre 2000 relative à la criminalité informatique (1)

ALBERT II, Roi des Belges,

A tous, présents et à venir, Salut.

Les Chambres ont adopté et Nous sanctionnons ce qui suit :

CHAPITRE Ier. — *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

CHAPITRE II. — *Dispositions complétant le Code pénal*

Art. 2. L'intitulé du chapitre IV, titre III, livre II du Code pénal, est remplacé par l'intitulé suivant :

« Des faux commis en écritures, en informatique et dans les dépêches télégraphiques. »

Art. 3. A l'article 193 du même Code, les mots « , en informatique » sont insérés entre les mots « en écritures » et les mots « ou dans les dépêches télégraphiques ».

Art. 4. Il est inséré dans le livre II, titre III, chapitre IV, du même Code une section II*bis*, rédigée comme suit :

« Section II*bis*. — Faux en informatique

Art. 210*bis*. § 1er. Celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 2. Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux.

§ 3. La tentative de commettre l'infraction visée au § 1er est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cinquante mille francs ou d'une de ces peines seulement.

§ 4. Les peines prévues par les §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 259*bis*, 314*bis*, 504*quater* ou au titre IX*bis*. »

Art. 5. Il est inséré dans le livre II, titre IX, chapitre II du même Code une section III*bis*, rédigée comme suit :

« Section III*bis*. — Fraude informatique

Art. 504*quater*. § 1er. Celui qui se procure, pour soi-même ou pour autrui, un avantage patrimonial frauduleux en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 2. La tentative de commettre l'infraction visée au § 1er est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cinquante mille francs ou d'une de ces peines seulement.

§ 3. Les peines prévues par les §§ 1er et 2 sont doublées si une infraction a l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis* ou au titre IX*bis*. »

MINISTERIE VAN JUSTITIE

N. 2001 — 298 [S − C − 2001/09035]

28 NOVEMBER 2000. — Wet van 28 november 2000 inzake informaticacriminaliteit (1)

ALBERT II, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamers hebben aangenomen en Wij bekrachtigen hetgeen volgt :

HOOFDSTUK I. — *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK II. — *Bepalingen tot aanvulling van het Strafwetboek*

Art. 2. Het opschrift van hoofdstuk IV, titel III, boek II van het Strafwetboek wordt vervangen als volgt :

« Valsheid in geschriften, in informatica en in telegrammen. »

Art. 3. In artikel 193 van hetzelfde Wetboek worden de woorden « geschriften of in telegrammen » vervangen door de woorden « geschriften, in informatica of in telegrammen ».

Art. 4. In boek II, titel III, hoofdstuk IV van hetzelfde Wetboek wordt een afdeling II*bis* ingevoegd, luidende :

« Afdeling II*bis*. — Valsheid in informatica

Art. 210*bis*. § 1. Hij die valsheid pleegt, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 2. Hij die, terwijl hij weet dat aldus verkregen gegevens vals zijn, hiervan gebruik maakt, wordt gestraft alsof hij de dader van de valsheid was.

§ 3. Poging tot het plegen van het misdrijf, bedoeld in § 1, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank of met een van die straffen alleen.

§ 4. De straffen bepaald in de §§ 1 tot 3 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 259*bis*, 314*bis*, 504*quater* of in titel IX*bis*. »

Art. 5. In boek II, titel IX, hoofdstuk II van hetzelfde Wetboek wordt een afdeling III*bis* ingevoegd, luidende :

« Afdeling III*bis*. — Informaticabedrog

Art. 504*quater*. § 1. Hij die, voor zichzelf of voor een ander, een bedrieglijk vermogensvoordeel verwerft, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 2. Poging tot het plegen van het misdrijf bedoeld in § 1 wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank, of met een van die straffen alleen.

§ 3. De straffen bepaald in de §§ 1 en 2 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis* of in titel IX*bis*. »

Art. 6. Il est inséré dans le livre II du même Code un titre IX*bis*, rédigé comme suit :

« Titre IX*bis*. — Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes.

Art. 550*bis*. § 1er. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§ 2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d une de ces peines seulement.

§ 3. Celui qui se trouve dans une des situations visées aux §§ 1er et 2 et qui :

1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique;

2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers;

3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système;

est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six francs belges à cinquante mille francs ou d'une de ces peines seulement.

§ 4. La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie des mêmes peines.

§ 5. Celui qui, avec une intention frauduleuse ou dans le but de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique et par lesquelles les infractions prévues par les §§ 1er à 4 peuvent être commises, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 6. Celui qui ordonne la commission d'une des infractions visées aux §§ 1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent francs à deux cent mille francs ou d'une de ces peines seulement.

§ 7. Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 8. Les peines prévues par les §§ 1er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*ter*.

Art. 550*ter*. § 1er. Celui qui, dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation possible de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.

§ 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à septante-cinq mille francs ou d'une de ces peines seulement.

§ 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

Art. 6. In boek II van hetzelfde Wetboek wordt een titel IX*bis* ingevoegd, luidende :

« Titel IX*bis*. — Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen.

Art. 550*bis*. § 1. Hij die, terwijl hij weet dat hij daar toe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van drie maanden tot een jaar en met geldboete van zesentwintig frank tot vijfentwintig duizend frank of met een van die straffen alleen.

Wanneer het misdrijf, bedoeld in het eerste lid, gepleegd wordt met bedrieglijk opzet, bedraagt de gevangenisstraf zes maanden tot twee jaar.

§ 2. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van zes maanden tot twee jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen.

§ 3. Hij die zich in een van de gevallen bedoeld in de §§ 1 en 2 bevindt en :

1° hetzij de gegevens die worden opgeslagen, verwerkt of overgedragen door middel van het informaticasysteem op enige manier overneemt;

2° hetzij enig gebruik maakt van een informaticasysteem van een derde of zich bedient van het informaticasysteem om toegang te verkrijgen tot een informaticasysteem van een derde;

3° hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de gegevens die door middel van het informaticasysteem worden opgeslagen, verwerkt of overgedragen of aan een informaticasysteem van een derde of aan de gegevens die door middel van het laatstgenoemde informaticasysteem worden opgeslagen, verwerkt of overgedragen;

wordt gestraft met gevangenisstraf van een jaar tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank of met een van die straffen alleen.

§ 4. Poging tot het plegen van een van de misdrijven, bedoeld in §§ 1 en 2, wordt gestraft met dezelfde straffen.

§ 5. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem en waarmee de misdrijven, bedoeld in §§ 1 tot 4, gepleegd kunnen worden, opspoort, verzamelt, ter beschikking stelt, verspreidt of verhandelt, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 6. Hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven, bedoeld in §§ 1 tot 5, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van honderd frank tot tweehonderdduizend frank of met een van die straffen alleen.

§ 7 Hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een van de misdrijven bedoeld in §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 8. De straffen bepaald in de §§ 1 tot 7 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis*, 504*quater* of 550*ter*.

Art. 550*ter*. § 1. Hij die, met het oogmerk om te schaden, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist, of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem verandert, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen.

§ 2. Hij die, ten gevolge van het plegen van een misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot vijfenzeventigduizend frank of met een van die straffen alleen.

§ 3. Hij die, ten gevolge van het plegen van een van de misdrijven bedoeld in § 1, de correcte werking van dit of enig ander informaticasysteem geheel of gedeeltelijk belemmert, wordt gestraft met gevangenisstraf van een jaar tot vijf jaar en met geldboete van zesentwintig f rank tot honderdduizend frank of met een van die straffen alleen.

§ 4. Celui qui, avec une intention frauduleuse ou dans le but de nuire, conçoit, met à disposition, diffuse ou commercialise des données stockées, traitées ou transmises par un système informatique, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*bis*. »

CHAPITRE III. — *Dispositions modifiant le Code d'instruction criminelle*

Art. 7. Il est inséré dans le Code d'instruction criminelle un article 39*bis*, rédigé comme suit :

« Art. 39*bis*. § 1er. Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28*sexies*, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique.

§ 2. Lorsque le procureur du Roi découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

§ 3. Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

§ 4. Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

§ 5. Le procureur du Roi informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.

§ 6. Le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.

Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.

La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents. »

§ 4. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, ontwerpt, ter beschikking stelt, verspreidt of verhandelt, terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 5. De straffen bepaald in de §§ 1 tot 4 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis*, 504*quater* of 550*bis*. »

HOOFDSTUK III. — *Bepalingen tot wijziging van het Wetboek van strafvordering*

Art. 7. In het Wetboek van strafvordering wordt een artikel 39*bis* ingevoegd, luidende :

« Art. 39*bis*. § 1. Onverminderd de specifieke bepalingen van dit artikel, zijn de regels van dit wetboek inzake inbeslagneming, met inbegrip van artikel 28*sexies*, van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem opgeslagen gegevens.

§ 2. Wanneer de procureur des Konings in een informaticasysteem opgeslagen gegevens aantreft die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

§ 3. Hij wendt bovendien de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings alle passende technische middelen aan om deze gegevens ontoegankelijk te maken.

Hij kan evenwel, behoudens in het geval bedoeld in het vorige lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.

§ 4. Wanneer de in § 2 vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt hij de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

§ 5. De procureur des Konings brengt de verantwoordelijke van het informaticasysteem op de hoogte van de zoeking in het informaticasysteem en deelt hem een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.

§ 6. De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.

Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie.

Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informaticasysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen. »

Art. 8. Il est inséré dans le même Code un article 88*ter*, rédigé comme suit :

« Art. 88*ter*. § 1er. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :

— si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et

— si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

§ 2. L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.

§ 3. En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39*bis* s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.

§ 4. L'article 89*bis* est applicable à l'extension de la recherche dans un système informatique. »

Art. 9. Il est inséré dans le même Code un article 88*quater*, rédigé comme suit :

« Art. 88*quater*. § 1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi.

§ 2. Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.

§ 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

§ 4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 5. L'Etat est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système. »

Art. 10. A l'article 89 du même Code, modifié par les lois des 10 juillet 1967 et 20 mai 1997, les mots « et 39 » sont remplacés par les mots « , 39 et 39*bis* ».

Art. 8. In hetzelfde Wetboek wordt een artikel 88*ter* ingevoegd, luidende :

« Art. 88*ter*. § 1. Wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan, kan deze zoeking worden uitgebreid naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt :

— indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

— indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.

§ 2. De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.

§ 3. Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in artikel 39*bis*. De onderzoeksrechter brengt de verantwoordelijke van dit informaticasysteem op de hoogte, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden.

Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.

§ 4. Artikel 89*bis* is van toepassing op de uitbreiding van de zoeking in een informaticasysteem. »

Art. 9. In hetzelfde Wetboek wordt een artikel 88*quater* ingevoegd, luidende :

« Art. 88*quater*. § 1. De onderzoeksrechter, of in zijn opdracht een officier van gerechtelijke politie, hulpofficier van de procureur des Konings, kan personen van wie hij vermoedt dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoeking of van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen, of in een verstaanbare vorm toegang te verkrijgen tot de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. De onderzoeksrechter vermeldt de omstandigheden eigen aan de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings.

§ 2. De onderzoeksrechter kan iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen of de ter zake dienende gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.

Het bevel bedoeld in het eerste lid kan niet worden gegeven aan de verdachte en aan de personen bedoeld in artikel 156.

§ 3. Hij die weigert de in §§1 en 2 gevorderde medewerking te verlenen of de zoeking in het informaticasysteem hindert, wordt gestraft met gevangenisstraf van zes maanden tot één jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.

§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 5. De Staat is burgerrechtelijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt. »

Art. 10. In artikel 89 van hetzelfde Wetboek, gewijzigd bij de wetten van 10 juli 1967 en 20 mei 1997, worden de woorden « en 39, » vervangen door de woorden « , 39 en 39*bis*, ».

Art. 11. A l'article 90*ter*, § 2, du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois des 7 avril 1995, 13 avril 1995, 10 juin 1998 et 10 janvier 1999, sont apportées les modifications suivantes :

A) le 1°*bis* est remplacé par les dispositions suivantes :

« 1°*bis*. A l'article 210*bis* du même Code;

1°*ter*. A l'article 259*bis* du même Code;

1°*quater*. A l'article 314*bis* du même Code;

1°*quinquies*. Aux articles 324*bis* et 324*ter* du même Code »;

B) il est inséré un 10°*bis*, rédigé comme suit :

« 10°*bis*. A l'article 504*quater* du même Code »;

C) il est inséré un 13°*bis*, rédigé comme suit :

« 13°*bis*. Aux articles 550*bis* et 550*ter* du même Code. »

Art. 12. L'article 90*quater* du même Code, inséré par la loi du 30 juin 1994 et modifié par la loi du 10 juin 1998, est complété par un § 4, rédigé comme suit :

« § 4. Le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.

Il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

Celui qui refuse de fournir la collaboration ordonnée conformément aux alinéas précédents, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est appelée à y prêter son concours technique, est liée par le secret de l'instruction. Toute violation du secret sera punie conformément à l'article 458 du Code pénal. »

Art. 13. A l'article 90*septies* du même Code, inséré par la loi du 30 juin 1994 et remplacé par la loi du 10 juin 1998, il est inséré entre le quatrième et le cinquième alinéa, un nouvel alinéa, rédigé comme suit :

« Les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée et, dans la mesure du possible, pour réaliser sa transcription ou sa traduction. La même règle vaut pour la conservation au greffe des enregistrements et de leur transcription ou de leur traduction et pour les mentions dans le registre spécial. Le Roi détermine, après avoir recueilli l'avis de la Commission de la protection de la vie privée, ces moyens et le moment où ils remplacent la conservation sous pli scellé ou le registre spécial prévus aux alinéas 3 et 4. »

CHAPITRE IV. — *Disposition modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques*

Art. 14. A l'article 109*ter*, E, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, inséré par la loi du 21 décembre 1994, renuméroté par la loi du 19 décembre 1997 et remplacé par la loi du 10 juin 1998, sont apportées les modifications suivantes :

— 1° l'alinéa 1er du § 2 est complété comme suit :

« , ainsi que les obligations pour les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications d'enregistrer et de conserver, pendant un certain délai en vue de l'investigation et de la poursuite d'infractions pénales, dans les cas à déterminer par arrêté royal délibéré en Conseil des ministres et sur proposition du ministre de la Justice et du ministre qui a les Télécommunications et les Entreprises et Participations publiques dans ses attributions, les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services de télécommunications. Ce délai, qui ne peut jamais être inférieur à 12 mois, ainsi que les données d'appel et d'identification seront déterminés par arrêté royal délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée.

Art. 11. In artikel 90*ter*, § 2, van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 7 april 1995, 13 april 1995,10 juni 1998 en 10 januari 1999, worden de volgende wijzigingen aangebracht :

A) het 1°*bis* wordt vervangen door de volgende bepalingen :

« 1 °*bis*. Artikel 210*bis* van hetzelfde Wetboek;

1°*ter*. Artikel 259*bis* van hetzelfde Wetboek;

1°*quater*. Artikel 314*bis* van hetzelfde Wetboek;

1°*quinquies*. Artikelen 324*bis* en 324*ter* van hetzelfde Wetboek »;

B) er wordt een 10°*bis* ingevoegd, luidende :

« 10°*bis*. Artikel 504*quater* van hetzelfde Wetboek »;

C) er wordt een 13°*bis* ingevoegd, luidende :

« 13°*bis*. Artikelen 550*bis* en 550*ter* van hetzelfde Wetboek. »

Art. 12. In artikel 90*quater* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wet van 10 juni 1998, wordt een § 4 toegevoegd, luidende :

« § 4. De onderzoeksrechter kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van de telecommunicatiedienst waarop de bewakingsmaatregel betrekking heeft of van diensten om gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud van telecommunicatie die wordt of is overgebracht.

Hij kan personen bevelen om de inhoud van de telecommunicatie toegankelijk te maken in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.

Hij die weigert de overeenkomstig de vorige leden bevolen medewerking te verlenen, wordt gestraft met gevangenisstraf van zes maanden tot een jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of die ertoe wordt geroepen zijn technische medewerking te verlenen, is gebonden door het geheim van het gerechtelijk onderzoek. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. »

Art. 13. In artikel 90*septies* van hetzelfde Wetboek ingevoegd bij de wet van 30 juni 1994 en vervangen bij de wet van 10 juni 1998, wordt tussen het vierde en het vijfde lid een nieuw lid ingevoegd, luidende :

« De passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen communicatie of telecommunicatie te waarborgen, en voor zover mogelijk, de overschrijving of vertaling hiervan tot stand te brengen. Hetzelfde geldt voor de bewaring op de griffie van de opnamen en de overschrijving of vertaling hiervan en voor de vermeldingen in het bijzonder register. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, deze middelen en het ogenblik waarop ze de bewaring onder verzegelde omslag of het bijzonder register, bedoeld in het derde en het vierde lid, vervangen. »

HOOFDSTUK IV. — *Bepaling tot wijziging van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven*

Art. 14. In artikel 109*ter*, E, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij de wet van 21 december 1994, hernummerd bij de wet van 19 december 1997 en vervangen bij de wet van 10 juni 1998, worden de volgende wijzigingen aangebracht :

— 1° het eerste lid van § 2 wordt aangevuld als volgt :

« , evenals de verplichtingen voor de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten om de oproepgegevens van telecommunicatiemiddelen en de identificatiegegevens van gebruikers van telecommunicatiediensten te registreren en gedurende een bepaalde termijn te bewaren met het oog op de opsporing en vervolging van strafbare feiten, in de gevallen, te bepalen bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, Overheidsbedrijven en Participaties. Deze termijn, die nooit minder mag zijn dan 12 maanden, alsook de oproepgegevens en de identificatiegegevens worden bepaald bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Cette conservation imposée aux opérateurs de réseaux de télécommunications et aux fournisseurs de services de télécommunications doit s'effectuer à l'intérieur des limites du territoire de l'Union européenne. »;

— 2° l'article 109*ter*, E, est complété comme suit :

« § 3. Celui qui ne respecte pas les obligations prévues par le Roi en vertu des paragraphes précédents est puni d'un emprisonnement de trois mois à six mois et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

§ 4. Le Roi par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée prévoit les modalités et les moyens appropriés pour garantir la confidentialité et l'intégrité des données d'appels et d'identification visées au § 2. »

Promulguons la présente loi, ordonnons qu'elle soit revêtue du Sceau de l'Etat et publiée par le *Moniteur belge*.

Donné à Bruxelles, le 28 novembre 2000.

ALBERT

Par le Roi :

Le Ministre de la Justice,
M. VERWILGHEN

Scellé du Sceau de l'État :

Le Ministre de la Justice,
M. VERWILGHEN

Note

(1) Session 1999—2000.

Chambre des représentants.

Documents parlementaires. — Projet de loi, n° 50-213/1. — Amendements n^os^ 50-213/2 et 50-213/3. — Rapport de la commission, n° 50-213/4. — Texte adopté par la commission, n° 50-213/5. — Amendements, n° 50-213/6. — Texte adopté en séance plénière et transmis au Sénat, n° 50-213/7.

Annales parlementaires. — Discussion et adoption. Séance du 30 mars 2000.

Sénat.

Documents parlementaires. — Projet transmis par la Chambre des représentants, n° 2-392/1. — Amendements, n° 2-392/2. — Rapport de la commission, n° 2-392/3. — Texte adopté par la commission, n° 2-392/4. — Amendements, n^os^ 2-392/5 et 2-392/6. — Texte amendé en séance plénière et renvoyé à la Chambre des représentants, n° 2-392/7.

Annales parlementaires. — Discussion et adoption. Séance du 12 et 13 juillet 2000.

Chambre des représentants.

Documents parlementaires. — Projet amendé par le Sénat, n° 50-213/8. — Amendements, n°s 50-213/9 et 50-213/10. — Rapport de la commission, n° 50-213/11. — Texte adopté par la commission, n° 50-213/12. — Texte adopté en séance plénière et renvoyé au Sénat, n° 50-213/13.

Annales parlementaires. — Discussion et adoption. Séance du 26 octobre 2000.

Sénat.

Documents parlementaires. — Projet amendé par la Chambre des représentants, n° 2-392/8. — Rapport de la commission, n° 2-392/9. — Texte adopté par la commission, n° 2-392/10. — Décision de se rallier au projet réamendé par la Chambre, n° 2-392/11.

Annales parlementaires. — Discussion et adoption. Séance du 16 novembre 2000.

Deze bewaringsplicht voor de operatoren van de telecommunicatienetwerken en de verstrekkers van de telecommunicatiediensten moet worden uitgevoerd binnen de grenzen van de Europese Unie. »;

— 2° artikel 109*ter*, E, wordt als volgt aangevuld :

« § 3. Hij die de verplichtingen door de Koning krachtens de vorige paragrafen bepaald, niet nakomt, wordt gestraft met gevangenisstraf van drie maanden tot zes maanden en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.

§ 4. De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer de modaliteiten en de middelen om de vertrouwelijkheid en de integriteit van de oproep- en identificatiegegevens bedoeld in § 2 te waarborgen. »

Kondigen deze wet af, bevelen dat zo met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 28 november 2000.

ALBERT

Van Koningswege :

De Minister van Justitie,
M. VERWILGHEN

Met 's Lands zegel gezegeld :

De Minister van Justitie,
M. VERWILGHEN

Nota

(1) Zitting 1999-2000.

Kamer van volksvertegenwoordigers.

Parlementaire bescheiden. — Wetsontwerp, nr. 50-213/1. — Amendementen nrs. 50-213/2 en 50-213/3. —Verslag van de commissie, nr. 50-213/4. —Tekst aangenomen door de commissie, nr. 50-213/5. — Amendementen, nr. 50-213/6. — Tekst aangenomen in plenaire vergadering en overgezonden aan de Senaat, nr. 50-213/7.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 30 maart 2000.

Senaat.

Parlementaire bescheiden. — Ontwerp overgezonden door de Kamer van volksvertegenwoordigers, nr. 2-392/1. — Amendementen, nr. 2-392/2. — Verslag van de commissie, nr. 2-392/3. — Tekst aangenomen door de commissie, nr. 2-392/4. — Amendementen, nrs. 2-392/5 en 2-392/6. — Tekst geamendeerd in plenaire vergadering en teruggezonden naar de Kamer van volksvertegenwoordigers, nr. 2-392/7.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 12 en 13 juli 2000.

Kamer van volksvertegenwoordigers.

Parlementaire bescheiden. — Ontwerp geamendeerd door de Senaat, nr. 50-213/8. — Amendementen, nrs. 50-213/9 en 50-213/10. — Verslag van de commissie, nr. 50-213/11. — Tekst aangenomen door de commissie, nr. 50-213/12. — Tekst aangenomen in plenaire vergadering en teruggezonden aan de Senaat, nr. 50-213/13.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 26 oktober 2000.

Senaat.

Parlementaire bescheiden. — Ontwerp geamendeerd door de Kamer van volksvertegenwoordigers, nr. 2-392/8. — Verslag van de commissie, nr. 2-392/9. — Tekst aangenomen door de commissie, nr. 2-392/10. — Beslissing om in te stemmen met het door de Kamer opnieuw geamendeerd ontwerp, nr. 2-392/11.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 16 november 2000.

Bijlage II: Europese Cybercrime-Conventie

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

European Treaty Series - No. 18

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.


71 0963 0
732 387 09838510
2876 236 0832