

0635/01/Huttner-Thompson

Arbeitsübersetzung aus dem Englischen

**EUROPARAT**

Straßburg, den 25. Mai 2001

**N.f.d.D.**

**CDPC (2001) 2 rev**

**EUROPÄISCHER AUSSCHUSS FÜR STRAFRECHTSFRAGEN**  
**(CDPC)**

**SACHVERSTÄNDIGENAUSSCHUSS FÜR DATENNETZKRIMINALITÄT**  
**(PC-CY)**

**ENTWURF EINES ÜBEREINKOMMENS ÜBER DATENNETZKRIMINALITÄT  
UND  
EINES ERLÄUTERNDEN BERICHTS DAZU**

**Bericht des Sekretariats,  
erstellt von der Abteilung für Rechtsfragen**

## **ENTWURF EINES ÜBEREINKOMMENS ÜBER DATENNETZKRIMINALITÄT**

### **Präambel**

Die Mitgliedstaaten des Europarats und die anderen Staaten, die dieses Übereinkommen unterzeichnen,

in der Erwägung, dass es das Ziel des Europarats ist, eine engere Verbindung zwischen seinen Mitgliedern herbeizuführen;

in Anerkennung der Bedeutung einer verstärkten Zusammenarbeit mit den anderen Unterzeichnerstaaten dieses Übereinkommens;

überzeugt von der Notwendigkeit, vorrangig eine gemeinsame Kriminalpolitik zu verfolgen, die den Schutz der Gesellschaft vor Datennetzkriminalität unter anderem durch Annahme geeigneter Rechtsvorschriften und Förderung der internationalen Zusammenarbeit zum Ziel hat;

in dem Bewusstsein der tiefgreifenden Veränderungen, die durch die Digitalisierung, die Konvergenz und die kontinuierliche Globalisierung von Rechnernetzen hervorgerufen werden;

in der Besorgnis über die Gefahr, dass Rechnernetze und elektronische Daten auch zur Begehung von Straftaten benutzt und beweiserhebliche Daten mit diesen Netzen gespeichert und übertragen werden können;

in der Erkenntnis, dass die Staaten und die Privatwirtschaft bei der Bekämpfung der Datennetzkriminalität zusammenarbeiten und berechnete Interessen am Einsatz und an der Weiterentwicklung der Informationstechnik geschützt werden müssen;

in der Überzeugung, dass zur wirksamen Bekämpfung der Datennetzkriminalität eine verstärkte, rasche und gut funktionierende internationale Zusammenarbeit in Strafsachen nötig ist;

in der Überzeugung, dass dieses Übereinkommen notwendig ist, um von Handlungen gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen, Netzen und Com-

puterdaten sowie vom Missbrauch solcher Systeme, Netze und Daten abzuschrecken, indem solches Verhalten entsprechend der Beschreibung in diesem Übereinkommen unter Strafe gestellt wird und hinreichende Befugnisse zur wirksamen Bekämpfung dieser Straftaten vorgesehen werden und indem die Aufdeckung, Untersuchung und Verfolgung solcher Straftaten sowohl auf nationaler als auch auf internationaler Ebene erleichtert und Vorkehrungen für eine rasche und zuverlässige internationale Zusammenarbeit getroffen werden;

eingedenk des Erfordernisses der Wahrung eines angemessenen Gleichgewichts zwischen den Interessen der Strafverfolgung und der Achtung der grundlegenden Menschenrechte im Sinne der Konvention des Europarats zum Schutz der Menschenrechte und Grundfreiheiten (1950), des Internationalen Pakts der Vereinten Nationen über bürgerliche und politische Rechte (1966) sowie anderer anwendbarer völkerrechtlicher Verträge über Menschenrechte , in denen das Recht auf ungestörte Meinungsfreiheit sowie das Recht der freien Meinungsäußerung einschließlich des Rechts, ohne Rücksicht auf Staatsgrenzen Informationen und Ideen jeder Art zu suchen, zu empfangen und weiterzugeben, und die Rechte in Bezug auf die Achtung der Privatsphäre bekräftigt werden;

[eingedenk auch [der Notwendigkeit eines Ausgleichs der Interessen des internationalen Rechtshilfeverkehrs und] des Schutzes personenbezogener Daten, wie er z.B. nach dem Übereinkommen des Europarats von 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vorgesehen ist]<sup>1</sup>;

in Anbetracht des Übereinkommens der Vereinten Nationen von 1989 über die Rechte des Kindes sowie des Übereinkommens der Internationalen Arbeitsorganisation von 1999 gegen besonders schlimme Formen der Kinderarbeit ;

unter Berücksichtigung der bestehenden Übereinkommen des Europarats über die Zusammenarbeit auf strafrechtlichem Gebiet sowie gleichartiger Verträge zwischen Mitgliedstaaten des Europarats und anderen Staaten und unter Hinweis darauf, dass diese Übereinkünfte durch das vorliegende Übereinkommen ergänzt werden sollen, damit die strafrechtlichen Ermittlungen und Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten wirksamer werden und elektronisches Beweismaterial für eine Straftat gesammelt werden kann;

erfreut über die Entwicklungen in der letzten Zeit, welche die internationale Verständigung und Zusammenarbeit bei der Bekämpfung der Datennetzkriminalität einschließlich der Maß-

---

<sup>1</sup> Siehe Fußnote zu Artikel 28

nahmen der Vereinten Nationen, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, der Europäischen Union und der G8-Staaten weiter fördern;

unter Hinweis auf die Empfehlung Nr. R (85) 10 über die praktische Anwendung des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen in Bezug auf Rechtshilfeersuchen um Überwachung des Telekommunikationsverkehrs, die Empfehlung Nr. R (88) 2 über die Piraterie im Bereich des Urheberrechts und verwandter Schutzrechte, [die Empfehlung Nr. R (87) 15 zur Regelung der Verwendung personenbezogener Daten im polizeilichen Sektor, die Empfehlung Nr. R (95) 4 über den Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste unter besonderer Berücksichtigung von Telefondiensten]<sup>2</sup> sowie die Empfehlung Nr. R (89) 9 über Computerstraftaten, die Leitlinien für die nationalen Gesetzgeber betreffend die Definition bestimmter Computerstraftaten enthält, und die Empfehlung Nr. R (95) 13 über strafprozessrechtliche Probleme in Zusammenhang mit der Informationstechnik;

unter Hinweis auf die bei der 21. Konferenz der europäischen Justizminister angenommene Entschließung Nr. 1 (Prag, Juni 1997), mit der dem Ministerkomitee empfohlen wurde, die Arbeit des Europäischen Ausschusses für Strafrechtsfragen (CDPC) auf dem Gebiet der Datennetzkriminalität zu unterstützen, um die innerstaatlichen Strafrechtsbestimmungen anzugleichen und den Einsatz wirksamer Mittel zur Untersuchung solcher Straftaten zu ermöglichen, sowie im Hinblick auf die bei der 23. Konferenz der europäischen Justizminister (London, Juni 2000) angenommene Entschließung Nr. 3, mit der die an den Verhandlungen beteiligten Parteien ermuntert wurden, sich weiter um geeignete Lösungen zu bemühen, damit möglichst viele Staaten Vertragsparteien des Übereinkommens werden können, und in der anerkannt wurde, dass ein schnelles und wirksames System der internationalen Zusammenarbeit nötig ist, das den besonderen Erfordernissen der Bekämpfung der Datennetzkriminalität gebührend Rechnung trägt;

im Hinblick ferner auf den Aktionsplan, den die Staats- und Regierungschefs des Europarats bei ihrem Zweiten Gipfeltreffen (Straßburg, 10. - 11. Oktober 1997) verabschiedet haben und mit dem auf der Grundlage der Normen und Werte des Europarats gemeinsame Antworten auf die Entwicklung der neuen Informationstechniken gefunden werden sollen;

sind wie folgt übereingekommen:

---

<sup>2</sup> Siehe Fußnote zu Artikel 28

## Kapitel I - Verwendung von Begriffen

### Artikel 1 - Begriffsbestimmungen

Im Sinne dieses Übereinkommens bedeutet

- a) „Computersystem“ eine Vorrichtung oder eine Gruppe verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Datenverarbeitung durchführen;
- b) „Computerdaten“ jede Darstellung von Fakten, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschließlich eines Programms, das geeignet ist, ein Computersystem zur Durchführung einer Funktion zu veranlassen;
- c) „Dienstanbieter“
  - i) jede öffentliche oder private Organisation, die Nutzern ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren;
  - ii) jede andere Organisation, die für diesen Kommunikationsdienst oder für Nutzer dieses Dienstes Computerdaten verarbeitet oder speichert.
- d) „Verbindungsdaten“ alle Computerdaten in Zusammenhang mit einer Kommunikation mit Hilfe eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen Ursprung, Bestimmung, Leitweg, Uhrzeit, Datum, Umfang oder Dauer der Kommunikation oder die Art des Trägerdienstes hervorgehen.

## **Kapitel II – Maßnahmen auf nationaler Ebene**

### **Abschnitt 1 - Materielles Strafrecht**

#### *Titel 1 - Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen*

##### **Artikel 2 – Rechtswidriger Zugriff**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den unbefugten Zugriff auf ein Computersystem als Ganzes oder auf einen Teil davon nach ihrem innerstaatlichen Recht als Straftat festzulegen, wenn die Handlung vorsätzlich begangen wird. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat durch Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, oder in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

##### **Artikel 3 - Rechtswidriges Abfangen**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübertragungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, nach ihrem innerstaatlichen Recht als Straftat festzulegen, wenn die Handlung vorsätzlich begangen wird. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat in unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

##### **Artikel 4 – Eingriffe in Daten**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten als Straftat nach ihrem innerstaatlichen Recht festzulegen, wenn die Handlung vorsätzlich begangen wird.

(2) Eine Vertragspartei kann sich das Recht vorbehalten, als Voraussetzung vorzusehen, dass das in Absatz 1 beschriebene Verhalten zu einem schweren Schaden geführt haben muss.

### **Artikel 5 – Eingriffe in das System**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die unbefugte und schwere Behinderung der Funktionsweise eines Computersystems durch Eingeben, Übertragen, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten als Straftat nach ihrem innerstaatlichen Recht festzulegen, wenn die Handlung vorsätzlich begangen wird.

### **Artikel 6 – Missbrauch von Vorrichtungen**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn sie vorsätzlich und unbefugt begangen werden, als Straftaten nach ihrem innerstaatlichen Recht festzulegen:

- a) das Herstellen, Verkaufen, Beschaffen zwecks Gebrauch, Einführen, Verbreiten oder anderweitige Zugänglichmachen
  - 1) einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie zu dem Zweck konstruiert oder bearbeitet worden ist, eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen,
  - 2) eines Computerpassworts, eines Zugriffscode oder ähnlicher Daten, die den Zugriff auf ein Computersystem als Ganzes oder auf einen Teil davon ermöglichen,

mit dem Vorsatz, sie zu verwenden, um eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen und

- b) den Besitz eines unter Buchstabe a Ziffer 1 oder 2 bezeichneten Mittels mit dem Vorsatz, es zu verwenden, um eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen. Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass erst der Besitz einer bestimmten Anzahl dieser Mittel die Strafbarkeit begründet.

(2) Dieser Artikel darf nicht so ausgelegt werden, als schreibe er die Strafbarkeit in Fällen vor, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauch, Einführen, Verbreiten oder anderweitige Zugänglichmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 festgelegten Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.

(3) Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, soweit der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Zugänglichmachen der in Absatz 1 Buchstabe a Ziffer 2 bezeichneten Mittel betrifft.

## *Titel 2 - Computerstraftaten*

### **Artikel 7 - Computerurkundenfälschung**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das vorsätzliche und unbefugte Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten als Straftat nach ihrem innerstaatlichen Recht vorzusehen, wenn dies zu unechten Daten führt und beabsichtigt ist, dass diese Daten für rechtliche Zwecke angesehen oder einer Handlung zugrunde gelegt werden, als wären sie echt, gleichviel, ob die Daten unmittelbar lesbar und verständlich sind. Eine Vertragspartei kann als Voraussetzung vorsehen, dass erst eine betrügerische oder ähnliche unredliche Absicht die Strafbarkeit begründet.

### **Artikel 8 - Computerbetrug**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die vorsätzliche und unbefugte Beschädigung des Vermögens eines anderen durch

- a) Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten,
- b) Eingreifen in die Funktionsweise eines Computers oder Systems

in der betrügerischen oder unredlichen Absicht, sich oder einem anderen unbefugt einen wirtschaftlichen Vorteil zu verschaffen, als Straftat nach ihrem innerstaatlichen Recht festzulegen.



**Artikel 9 – Straftaten in Bezug auf Kinderpornografie**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die folgenden Handlungen, wenn sie vorsätzlich und unbefugt begangen werden, als Straftaten nach ihrem innerstaatlichen Recht festzulegen:

- a) das Herstellen von Kinderpornografie zum Zweck ihrer Verbreitung über ein Computersystem;
- b) das Anbieten oder Zugänglichmachen von Kinderpornografie über ein Computersystem;
- c) das Verbreiten oder Übertragen von Kinderpornografie über ein Computersystem;
- d) das Beschaffen von Kinderpornografie über ein Computersystem für sich selbst oder einen anderen;
- e) den Besitz von Kinderpornografie in einem Computersystem oder auf einem Computerdatenträger.

(2) Im Sinne von Absatz 1 umfasst „Kinderpornografie“ pornografisches Material mit der visuellen Darstellung

- a) einer minderjährigen Person bei sexuell eindeutigen Handlungen;
- b) einer Person, die als eine minderjährige Person bei sexuell eindeutigen Handlungen erscheint;
- c) realistischer Bilder, die eine minderjährige Person bei sexuell eindeutigen Handlungen zeigen.

---

<sup>3</sup> Der PC-CY hat die Möglichkeit erörtert, andere als die in Artikel 9 beschriebenen inhaltsbezogenen Straftaten einzubeziehen, wie das Verbreiten rassistischer Propaganda über Computersysteme. Die Einbeziehung dieses Tatbestands als Straftat wurde zwar weitgehend begrüßt, doch einige Delegationen äußerten starke Bedenken dagegen aus Gründen der freien Meinungsäußerung. Es wurde entschieden, dass der PC-CY die Frage einer zügigen Erarbeitung eines diesbezüglichen Zusatzprotokolls zum vorliegenden Übereinkommen dem Europäischen Ausschuss für Strafrechtsfragen (CDPC) vorlegt.

(3) Im Sinne von Absatz 2 umfasst der Ausdruck „minderjährige Person“ alle Personen unter 18 Jahren. Eine Vertragspartei kann jedoch eine niedrigere Altersgrenze vorsehen, wobei 16 Jahre nicht unterschritten werden dürfen.

(4) Jede Vertragspartei kann sich das Recht vorbehalten, die Absätze 1 Buchstaben d und e sowie 2 Buchstaben b und c ganz oder teilweise nicht anzuwenden.

*Titel 4 – Straftaten in Zusammenhang mit Verletzungen des Urheberrechts  
und verwandter Schutzrechte*

**Artikel 10 - Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Urheberrechtsverletzungen, wie sie nach dem Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach der Pariser Fassung vom 24. Juli 1971 der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst, dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Urheberrechtsübereinkommen umschrieben sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte als Straftaten nach ihrem innerstaatlichem Recht festzulegen, wenn diese Handlungen vorsätzlich, [mindestens]<sup>4</sup> in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Verletzungen verwandter Schutzrechte, wie sie nach dem Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach dem in Rom unterzeichneten Internationalen Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen (Abkommen von Rom), dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Vertrag betreffend Darbietungen und Tonträger umschrieben sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte als Straftaten nach ihrem innerstaatlichem Recht

---

<sup>4</sup> Dieser Zusatz wurde von einer Delegation in der zweiten Sitzung des vormaligen PC-CY-Ausschusses (April 2001) vorgeschlagen, aber über seine Annahme oder Ablehnung ist nicht förmlich entschieden worden. Über den Vorschlag wurde aus Zeitmangel auch in der letzten Sitzung (Mai 2001) nicht entschieden. Die Entscheidung darüber bleibt nun dem CDPC überlassen. Zwischenzeitlich hat eine andere Delegation die folgende alternative Formulierung vorgeschlagen: „Die Vertragsparteien ziehen in Erwägung, die in den Absätzen 1 und 2 beschriebenen Handlungen in Fallkonstellationen ohne gewerbsmäßigen Umfang als Straftaten festzulegen.“

festzulegen, wenn diese Handlungen vorsätzlich, [mindestens]<sup>5</sup> in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden.

(3) Eine Vertragspartei kann sich das Recht vorbehalten, eine strafrechtliche Verantwortlichkeit nach den Absätzen 1 und 2 unter begrenzten Umständen nicht vorzusehen, soweit andere wirksame Abhilfen zur Verfügung stehen und dieser Vorbehalt die internationalen Verpflichtungen dieser Vertragspartei aus den in den Absätzen 1 und 2 genannten völkerrechtlichen Übereinkünften nicht beeinträchtigt.

#### *Titel 5 - Nebenformen der Verantwortlichkeit und Sanktionen*

### **Artikel 11 - Versuch und Beteiligung**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die vorsätzliche Beteiligung an der Begehung einer der nach den Artikeln 2 bis 10 festgelegten Straftaten mit dem Vorsatz, eine solche Straftat zu begehen, als Straftat nach ihrem innerstaatlichen Recht festzulegen.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den Versuch der Begehung einer der nach den Artikeln 3 bis 5 sowie 7, 8, 9 Absatz 1 Buchstabe a und 9 Absatz 1 Buchstabe c festgelegten Straftaten als Straftat nach ihrem innerstaatlichen Recht festzulegen, wenn dieser Versuch vorsätzlich begangen wird.

(3) Jeder Staat kann sich das Recht vorbehalten, Absatz 2 ganz oder teilweise nicht anzuwenden.

### **Artikel 12 – Verantwortlichkeit juristischer Personen**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass eine juristische Personen für eine nach diesem Übereinkommen festgelegte Straftat verantwortlich gemacht werden kann, die zu ihrem Vorteil von einer natürlichen Person begangen wird, die allein oder als Teil eines Organs der juristischen Person handelt und innerhalb der juristischen Person eine Führungsposition auf folgender Grundlage innehat:

---

<sup>5</sup> Siehe vorhergehende Fußnote.

- a) Befugnis zur Vertretung der juristischen Person,
- b) Befugnis, Entscheidungen im Namen der juristischen Person zu treffen,
- c) Kontrollbefugnis innerhalb der juristischen Person.

(2) Abgesehen von den in Absatz 1 bereits genannten Fällen trifft jede Vertragspartei die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch eine natürliche Person nach Absatz 1 es ermöglicht hat, dass eine in ihrem Auftrag handelnde natürliche Person eine nach diesem Übereinkommen festgelegte Straftat zum Vorteil der juristischen Person begeht.

(3) Vorbehaltlich der Rechtsgrundsätze der Vertragspartei kann die Verantwortlichkeit einer juristischen Person straf-, zivil- oder verwaltungsrechtlicher Art sein.

(4) Diese Verantwortlichkeit berührt nicht die strafrechtliche Verantwortlichkeit der natürlichen Personen, welche die Straftat begangen haben.

### **Artikel 13 – Sanktionen und Maßnahmen**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass die nach den Artikeln 2 bis 11 festgelegten Straftaten mit wirksamen, angemessenen und abschreckenden Sanktionen bedroht werden, die Freiheitsentziehung einschließen.

(2) Jede Vertragspartei stellt sicher, dass juristische Personen, die nach Artikel 12 verantwortlich gemacht werden, mit wirksamen, angemessenen und abschreckenden strafrechtlichen oder nichtstrafrechtlichen Sanktionen oder Maßnahmen bedroht werden, die Geldsanktionen umfassen.

## **Abschnitt 2 – Verfahrensrecht**

### *Titel 1 – Allgemeine Bestimmungen*

#### **Artikel 14 – Geltungsbereich verfahrensrechtlicher Bestimmungen**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die Befugnisse und Verfahren festzulegen, die in diesem Abschnitt für die Zwecke besonderer strafrechtlicher Ermittlungen oder Verfahren vorgesehen sind.

(2) Soweit in Artikel 21 nicht eigens etwas anderes vorgesehen ist, wendet jede Vertragspartei die in Absatz 1 bezeichneten Befugnisse und Verfahren an in Bezug auf

a) die nach den Artikeln 2 bis 11 festgelegten Straftaten,

b) andere mittels eines Computersystems begangene Straftaten und

c) die Erhebung in elektronischer Form vorhandener Beweise für eine Straftat.

(3) Jede Vertragspartei kann sich das Recht vorbehalten, die in Artikel 20 bezeichneten Maßnahmen nur auf Straftaten oder Arten von Straftaten anzuwenden, die in dem Vorbehalt bezeichnet sind; die Reihe dieser Straftaten oder Arten von Straftaten darf nicht enger gefasst sein als die Reihe der Straftaten, auf die sie die in Artikel 21 bezeichneten Maßnahmen anwendet. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt so zu beschränken, dass die in Artikel 20 bezeichnete Maßnahme im weitesten Umfang angewendet werden kann.

#### **Artikel 15 – Bedingungen und Garantien**

(1) Jede Vertragspartei stellt sicher, dass für die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren Bedingungen und Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten einschließlich der Rechte vorsehen, die sich aus ihren Verpflichtungen nach dem Übereinkommen des Europarats zum Schutz der Menschenrechte und Grundfreiheiten (1950), dem Internationalen Pakt der Vereinten Nationen über bürgerliche und politische Rechte (1966) und anderen anwendbaren völkerrechtlichen Übereinkünften über Menschenrechte ergeben und zu denen der Grundsatz der Verhältnismäßigkeit gehören muss.

(2) Diese Bedingungen und Garantien umfassen, soweit dies in Anbetracht der Art der betreffenden Befugnis oder des betreffenden Verfahrens angebracht ist, unter anderem die Kontrolle dieser Befugnis oder dieses Verfahrens durch ein Gericht oder eine andere unabhängige Stelle, die Begründung der Anwendung und eine Begrenzung im Hinblick auf den Umfang und die Dauer dieser Befugnis oder dieses Verfahrens.

(3) Soweit dies mit dem öffentlichen Interesse, insbesondere mit der ordnungsgemäßen Rechtspflege, vereinbar ist, berücksichtigt eine Vertragspartei die Auswirkungen der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren auf die Rechte, Verantwortlichkeiten und berechtigten Interessen Dritter.

## *Titel 2 – Beschleunigte Sicherung gespeicherter Computerdaten*

### **Artikel 16 – Beschleunigte Sicherung gespeicherter Computerdaten**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ihre zuständigen Behörden die beschleunigte Sicherung bestimmter Computerdaten einschließlich Verbindungsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.

(2) Führt eine Vertragspartei Absatz 1 so durch, dass eine Person im Wege der Anordnung aufgefordert wird, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder ihrer Verfügungsgewalt befinden, sicherzustellen, so trifft diese Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen, um diese Person zu verpflichten, die Integrität dieser Computerdaten so lange wie notwendig für die Dauer von bis zu 90 Tagen zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, um deren Weitergabe zu ersuchen. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschließend verlängert werden kann.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen oder anderen Maßnahmen, um den Verwahrer oder eine andere Person, welche die Computerdaten zu sichern hat, zu verpflichten, die Durchführung dieser Verfahren für den nach ihrem innerstaatlichem Recht vorgesehenen Zeitraum vertraulich zu behandeln.

- (4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

### **Artikel 17 – Beschleunigte Sicherung und Teilweitergabe von Verbindungsdaten**

(1) Jede Vertragspartei trifft in Bezug auf Verbindungsdaten, die nach Artikel 16 zu sichern sind, alle erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen,

- a) dass diese beschleunigte Sicherung von Verbindungsdaten unabhängig davon zu möglich ist, ob ein oder mehrere Dienstanbieter an der Übertragung dieser Kommunikation mitgewirkt haben;
- b) dass Verbindungsdaten in so ausreichender Menge beschleunigt an die zuständige Behörde der Vertragspartei oder an eine von dieser Behörde bezeichnete Person weitergegeben werden, dass die Vertragspartei die Dienstanbieter und den Weg feststellen kann, auf dem die Kommunikation übertragen wurde.

- (2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

### *Titel 3 – Herausgabeanordnung*

### **Artikel 18 – Herausgabeanordnung**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, anzuordnen,

- a) dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder ihrer Verfügungsgewalt befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und
- b) dass ein Dienstanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Kundendaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder seiner Verfügungsgewalt befinden, vorzulegen hat.

(2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

(3) Im Sinne dieses Artikels bedeuten „Kundendaten“ alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Dienstanbieter über Kunden seiner Dienste vorliegen, mit Ausnahme von Verbindungsdaten oder inhaltsbezogenen Daten, durch die folgendes festgestellt werden kann:

- a) die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dienstdauer;
- b) die Identität des Kunden, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen.
- c) gegebenenfalls andere Informationen über den Ort der Installation der Kommunikationsanlage, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.

#### *Titel 4 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten*

### **Artikel 19 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen,

- a) ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und
- b) einen Computerdatenträger, auf dem Computerdaten gespeichert sein können,

in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem



oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon in ihrem Hoheitsgebiet gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, Computerdaten, auf die nach Absatz 1 oder 2 Zugriff genommen wurde, zu beschlagnahmen oder in ähnlicher Weise sicherzustellen. Diese Maßnahmen umfassen die Befugnis,

- a) ein Computersystem oder einen Teil davon oder einen Computerdatenträger zu beschlagnahmen oder in ähnlicher Weise sicherzustellen,
- b) eine Kopie dieser Computerdaten anzufertigen und zurückzubehalten,
- c) die Integrität der einschlägigen gespeicherten Computerdaten zu erhalten und
- d) diese Computerdaten in dem Computersystem, auf das Zugriff genommen wurde, unzugänglich zu machen oder sie daraus zu entfernen.

(4) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, anzuordnen, dass jede Person, die Kenntnisse über die Funktionsweise des Computersystems oder Maßnahmen zum Schutz der darin enthaltenen Daten hat, in vernünftigem Maß die notwendigen Auskünfte zu erteilen hat, um die Durchführung der in den Absätzen 1 und 2 genannten Maßnahmen zu ermöglichen.

(5) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

**Artikel 20 – Echtzeit-Erhebung von Verbindungsdaten<sup>6</sup>**

- (1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen,
- a) Verbindungsdaten, die mit bestimmten in ihrem Hoheitsgebiet mittels eines Computersystems übertragenen Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und
  - b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,
    - (i) solche Verbindungsdaten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder
    - (ii) bei der Erhebung oder Aufzeichnung solcher Verbindungsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.
- (2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht ergreifen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass Verbindungsdaten, die mit bestimmten Kommunikationen in ihrem Hoheitsgebiet in Zusammenhang stehen, durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.
- (3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Dienstanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

---

<sup>6</sup> Zwei Delegationen wünschten, dass zu den Artikeln 20 und 21 eine Vorbehaltsklauseln aufgenommen wird, nach der diese Bestimmungen nach ihrem innerstaatlichen Recht auf bestimmte Arten von Dienstanbietern nicht angewendet werden können.

- (4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

### **Artikel 21 – Abfangen von Inhaltsdaten<sup>7</sup>**

- (1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden in Bezug auf eine Reihe schwerer Straftaten, die nach ihrem innerstaatlichen Recht zu bestimmen sind, die Befugnis zu erteilen,
- a) inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mit einem Computersystem übertragen wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und
  - b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,
    - (i) solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder
    - (ii) bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.
- (5) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht ergreifen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.
- (6) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Dienstanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

---

<sup>7</sup> Siehe vorstehende Fußnote.

- (2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

### **Abschnitt 3 – Gerichtsbarkeit**

#### **Artikel 22 – Gerichtsbarkeit**

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die Gerichtsbarkeit für eine Straftat, die in Übereinstimmung mit den Artikeln 2 bis 11 dieses Übereinkommens festgelegt worden ist, zu begründen, wenn die Straftat wie folgt begangen wird:

- a) in ihrem Hoheitsgebiet,
- b) an Bord eines Schiffs, das ihre Flagge führt,
- c) an Bord eines Flugzeugs, das nach den Rechtsvorschriften dieser Vertragspartei eingetragen ist, oder
- d) von einem ihrer Staatsangehörigen, wenn die Tat nach dem am Tatort geltenden Recht strafbar ist oder die Straftat außerhalb der territorialen Gerichtsbarkeit irgendeines Staates begangen wird.

(2) Jeder Staat kann sich das Recht vorbehalten, die in Absatz 1 Buchstaben b bis d oder in Teilen davon enthaltenen Vorschriften in Bezug auf die Gerichtsbarkeit nicht oder nur in bestimmten Fällen oder unter bestimmten Bedingungen anzuwenden.

(3) Jede Vertragspartei trifft die erforderlichen Maßnahmen, um ihre Gerichtsbarkeit für die in Artikel 24 Absatz 1 bezeichneten Straftaten in den Fällen zu begründen, in denen sich ein mutmaßlicher Täter in ihrem Hoheitsgebiet aufhält und sie ihn allein wegen seiner Staatsangehörigkeit nicht an eine andere Vertragspartei ausliefert, nachdem ein Auslieferungsgesuchen gestellt worden ist.

(4) Dieses Übereinkommen schließt die Ausübung einer Strafgerichtsbarkeit nach innerstaatlichem Recht nicht aus.

(5) Wird die Gerichtsbarkeit für eine angebliche Straftat, die in Übereinstimmung mit diesem Übereinkommen festgelegt worden ist, von mehr als einer Vertragspartei in Anspruch

genommen, so konsultieren die beteiligten Vertragsparteien einander gegebenenfalls, um die für die Strafverfolgung am ehesten geeignete Gerichtsbarkeit zu bestimmen.

### **Kapitel III– Internationale Zusammenarbeit**

#### **Abschnitt 1 – Allgemeine Grundsätze**

##### *Titel 1 – Allgemeine Grundsätze der internationalen Zusammenarbeit*

#### **Artikel 23 – Allgemeine Grundsätze der internationalen Zusammenarbeit**

Die Vertragsparteien arbeiten untereinander nach den Bestimmungen dieses Kapitels und durch Anwendung einschlägiger völkerrechtlicher Übereinkünfte über die internationale Zusammenarbeit in Strafsachen sowie Vereinbarungen, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurden, und innerstaatlicher Rechtsvorschriften für der Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und Computerdaten oder für die Erhebung von in elektronischer Form vorliegenden Beweisen für eine Straftat im größtmöglichen Umfang zusammen.

##### *Titel 2 – Grundsätze der Auslieferung*

#### **Abschnitt 2 – Auslieferung**

#### **Artikel 24 – Auslieferung**

- (1) a) Dieser Artikel findet auf den Auslieferungsverkehr zwischen den Vertragsparteien wegen der in Übereinstimmung mit den Artikeln 2 bis 11 festgelegten Straftaten Anwendung, soweit sie nach den Rechtsvorschriften der beiden beteiligten Vertragsparteien mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr oder mit einer schwereren Strafe bedroht sind.
- b) Gilt nach einer Vereinbarung auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften oder nach einem Auslieferungsvertrag einschließlich des Europäischen Auslieferungsvertrags (ETS Nr. 24), der zwischen zwei oder mehreren Vertragsparteien anwendbar ist, eine andere Mindeststrafe, so findet

die nach dieser Vereinbarung oder nach diesem Vertrag vorgesehene Mindeststrafe Anwendung.

(2) Die in Absatz 1 umschriebenen Straftaten gelten als in jeden zwischen den Vertragsparteien bestehenden Auslieferungsvertrag einbezogene, der Auslieferung unterliegende Straftaten. Die Vertragsparteien verpflichten sich, diese Straftaten als der Auslieferung unterliegende Straftaten in jeden zwischen ihnen zu schließenden Auslieferungsvertrag aufzunehmen.

(3) Erhält eine Vertragspartei, welche die Auslieferung vom Bestehen eines Vertrags abhängig macht, ein Auslieferungersuchen von einer anderen Vertragspartei, mit der sie keinen Auslieferungsvertrag hat, so kann sie dieses Übereinkommen als Rechtsgrundlage für die Auslieferung in Bezug auf die in Absatz 1 bezeichneten Straftaten ansehen.

(4) Vertragsparteien, welche die Auslieferung nicht vom Bestehen eines Vertrags abhängig machen, erkennen unter sich die in Absatz 1 bezeichneten Straftaten als der Auslieferung unterliegende Straftaten an.

(5) Die Auslieferung unterliegt den im Recht der ersuchten Vertragspartei oder in den geltenden Auslieferungsverträgen vorgesehenen Bedingungen einschließlich der Gründe, aus denen die ersuchte Vertragspartei die Auslieferung ablehnen kann.

(6) Wird die Auslieferung wegen einer in Absatz 1 bezeichneten Straftat allein aufgrund der Staatsangehörigkeit des Verfolgten oder deswegen abgelehnt, weil die ersuchte Vertragspartei der Auffassung ist, sie habe die Gerichtsbarkeit für die Straftat, so unterbreitet die ersuchte Vertragspartei auf Ersuchen der ersuchenden Vertragspartei den Fall ihren zuständigen Behörden zum Zweck der Strafverfolgung und teilt der ersuchenden Vertragspartei zu gegebener Zeit das endgültige Ergebnis mit. Diese Behörden entscheiden und betreiben die Ermittlungen und das Verfahren in derselben Weise wie bei jeder nach dem Recht dieser Vertragspartei vergleichbaren anderen Straftat.

(7) a) Jede Vertragspartei teilt dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde die Bezeichnung und Anschrift jeder Behörde mit, die für die Stellung oder Entgegennahme eines Ersuchens um Auslieferung oder vorläufige Inhaftnahme auf vertragloser Grundlage zuständig ist.

- b) Der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien so bestimmten Behörden. Jede Vertragspartei stellt sicher, dass die in dem Verzeichnis enthaltenen Angaben stets richtig sind.

### *Titel 3 – Allgemeine Grundsätze der Rechtshilfe*

#### **Artikel 25 – Allgemeine Grundsätze der Rechtshilfe**

- (1) Die Vertragsparteien leisten einander im größtmöglichen Umfang Rechtshilfe für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und Computerdaten oder für die Erhebung von in elektronischer Form vorliegenden Beweisen für eine Straftat.
- (2) Jede Vertragspartei trifft ferner die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den in den Artikeln 27 bis 35 bezeichneten Verpflichtungen nachzukommen.
- (3) In dringenden Fällen kann jede Vertragspartei Rechtshilfeersuchen oder damit in Zusammenhang stehende Mitteilungen durch schnelle Kommunikationsmittel einschließlich Telefax oder elektronischer Post übersenden, soweit diese Mittel einen angemessenen Sicherheits- und Authentisierungsstandard bieten (erforderlichenfalls auch unter Einsatz einer Verschlüsselung) und eine förmliche Bestätigung folgt, wenn die ersuchte Vertragspartei dies verlangt. Die ersuchte Vertragspartei nimmt das Ersuchen durch jedes dieser schnellen Kommunikationsmittel entgegen und beantwortet es auf diesem Weg.
- (4) Soweit in den Artikeln dieses Kapitels nicht ausdrücklich etwas anderes vorgesehen ist, unterliegt die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den geltenden Rechtshilfeverträgen vorgesehenen Bedingungen einschließlich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann. Die ersuchte Vertragspartei darf das Recht auf Ablehnung der Rechtshilfe nicht allein mit der Begründung ausüben, dass das Ersuchen eine Straftat betrifft, die von ihr als fiskalische Straftat angesehen wird.
- (5) Darf die ersuchte Vertragspartei nach den Bestimmungen dieses Kapitels die Rechtshilfe von der Bedingung abhängig machen, dass die beiderseitige Strafbarkeit gegeben ist, so gilt, gleichviel, ob die Straftat nach ihren Rechtsvorschriften in dieselbe Gruppe von Straftaten fällt oder mit den gleichen Worten umschrieben ist wie nach den Rechtsvorschriften der ersuchenden Vertragspartei, diese Bedingung als erfüllt, wenn die Handlung,

die der Straftat, derentwegen um Rechtshilfe ersucht wird, zugrunde liegt, nach ihren Rechtsvorschriften eine Straftat ist.

### **Artikel 26 – Unaufgeforderte Übermittlung von Informationen**

(1) Eine Vertragspartei kann in den Grenzen ihres innerstaatlichen Rechts einer anderen Vertragspartei ohne vorheriges Ersuchen Informationen übermitteln, die sie im Rahmen eigener Ermittlungen gewonnen hat, wenn sie der Auffassung ist, dass die Übermittlung dieser Informationen der anderen Vertragspartei bei der Einleitung oder Durchführung von Ermittlungen oder Verfahren wegen nach diesem Übereinkommen festgelegter Straftaten helfen oder dazu führen könnte, dass diese Vertragspartei ein Ersuchen um Zusammenarbeit nach diesem Kapitel stellt.

(2) Vor Übermittlung dieser Informationen kann die übermittelnde Vertragspartei um vertrauliche Behandlung oder bedingte Verwertung dieser Informationen ersuchen. Kann die andere Vertragspartei diesem Ersuchen nicht entsprechen, so teilt sie dies der übermittelnden Vertragspartei mit; diese entscheidet dann, ob die Informationen dennoch übermittelt werden sollen. Nimmt die andere Vertragspartei die Informationen unter den Bedingungen an, so ist sie an diese Bedingungen gebunden.

#### *Titel 4 - Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte*

### **Artikel 27 – Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte**

(1) Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Vereinbarung, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so finden die Absätze 2 bis 10 Anwendung. Liegen ein solcher Vertrag, eine solche Vereinbarung oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung, wenn die betreffenden Vertragsparteien übereinkommen, an Stelle dieses Vertrags, dieser Vereinbarung oder dieser Rechtsvorschriften die übrigen Absätze dieses Artikels ganz oder teilweise anzuwenden.

(2) a) Jede Vertragspartei bestimmt eine zentrale Behörde oder mehrere Behörden, welche die Aufgabe haben, Rechtshilfeersuchen abzusenden, zu beantworten, zu erledigen oder an die für die Erledigung zuständigen Behörden weiterzuleiten.



- b) Die zentralen Behörden verkehren unmittelbar miteinander.
  - c) Jede Vertragspartei teilt dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde die Bezeichnung und Anschrift der nach diesem Absatz bestimmten Behörden mit.
  - d) Der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien so bestimmten zentralen Behörden. Jede Vertragspartei stellt sicher, dass die in dem Verzeichnis enthaltenen Angaben stets richtig sind.
- (3) Rechtshilfeersuchen nach diesem Artikel werden nach den von der ersuchenden Vertragspartei bezeichneten Verfahren erledigt, soweit das Recht der ersuchten Vertragspartei dem nicht entgegensteht.
- (4) Zusätzlich zu den Ablehnungsgründen nach Artikel 25 Absatz 4 kann die ersuchte Vertragspartei die Rechtshilfe ablehnen, wenn
- a) das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als eine politische oder als eine mit einer solchen zusammenhängende Straftat angesehen wird, oder
  - b) sie der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, die Souveränität, die Sicherheit, die öffentliche Ordnung (*ordre public*) oder andere wesentliche Interessen<sup>8</sup> ihres Landes zu beeinträchtigen.
- (5) Die ersuchte Vertragspartei kann die Durchführung der in einem Ersuchen genannten Maßnahmen aufschieben, wenn die Gefahr besteht, dass sie die von ihren Behörden geführten strafrechtlichen Ermittlungen oder Verfahren beeinträchtigen.
- (6) Bevor die ersuchte Vertragspartei die Rechtshilfe ablehnt oder aufschiebt, prüft sie, gegebenenfalls nach Konsultation der ersuchenden Vertragspartei, ob dem Ersuchen zum Teil oder vorbehaltlich der von ihr für erforderlich erachteten Bedingungen entsprochen werden kann.

---

<sup>8</sup> Siehe Fußnote zu Artikel 28.

(7) Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei umgehend das Ergebnis der Erledigung eines Rechtshilfeersuchens mit. Wird das Ersuchen abgelehnt oder aufgeschoben, so ist die Ablehnung oder der Aufschub zu begründen. Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei gegebenenfalls auch die Gründe mit, aus denen die Erledigung des Ersuchens unmöglich ist oder sich wahrscheinlich erheblich verzögern wird.

(8) Die ersuchende Vertragspartei kann die ersuchte Vertragspartei bitten, das Vorliegen eines Ersuchens nach diesem Kapitel und dessen Inhalt vertraulich zu behandeln, soweit die Erledigung des Ersuchens nichts anderes gebietet. Kann die ersuchte Vertragspartei der erbetenen Vertraulichkeit nicht entsprechen, so teilt sie dies der ersuchenden Vertragspartei umgehend mit; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.

(9) a) In dringenden Fällen können Rechtshilfeersuchen oder damit in Zusammenhang stehende Mitteilungen unmittelbar von den Justizbehörden der ersuchenden Vertragspartei an solche Behörden der ersuchten Vertragspartei übermittelt werden. In diesen Fällen ist gleichzeitig über die zentrale Behörde der ersuchenden Vertragspartei eine Abschrift an die zentrale Behörde der ersuchten Vertragspartei zu senden.

b) Jedes Ersuchen oder jede Mitteilung nach diesem Absatz kann über die Internationale Kriminalpolizeiliche Organisation (Interpol) übermittelt werden.

c) Wird ein Ersuchen nach Buchstabe a) übermittelt und ist die befasste Behörde für die Erledigung nicht zuständig, so leitet sie das Ersuchen an die zuständige Behörde ihres Landes weiter und setzt die ersuchende Vertragspartei unmittelbar davon in Kenntnis.

d) Ersuchen oder Mitteilungen nach diesem Absatz, die keine Zwangsmaßnahmen umfassen, können unmittelbar von den zuständigen Behörden der ersuchenden Vertragspartei den zuständigen Behörden der ersuchten Vertragspartei übermittelt werden.

e) Jede Vertragspartei kann dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde mitteilen, dass Ersuchen nach diesem Absatz aus Gründen der Effizienz an ihre zentrale Behörde zu richten sind.

## Artikel 28 – Vertraulichkeit und Beschränkung der Verwendung<sup>9</sup>

(1) Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Vereinbarung, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so findet dieser Artikel Anwendung. Liegen ein solcher Vertrag, eine solche Vereinbarung oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung, wenn die betreffenden Vertragsparteien übereinkommen, an Stelle dieses Vertrags, dieser Vereinbarung oder dieser Rechtsvorschriften die übrigen Absätze dieses Artikels ganz oder teilweise anzuwenden.

(2) Die ersuchte Vertragspartei kann<sup>10</sup> die Überlassung von Informationen oder Unterlagen in Erledigung eines Ersuchens von der Bedingung abhängig machen, dass sie

- a) vertraulich behandelt werden, wenn das Rechtshilfeersuchen ohne diese Bedingung nicht erledigt werden könnte, oder
- b) nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet werden.

---

<sup>9</sup> Zwei Delegationen haben vorgeschlagen, in Artikel 27 Absatz 4 einen weiteren Grund für die Versagung der Rechtshilfe aufzunehmen, wenn die ersuchte Vertragspartei „der Ansicht ist, dass die ersuchende Vertragspartei nicht in der Lage ist, in dem speziellen Fall, wie im Ersuchen ausgeführt, in ausreichendem Maß für den Schutz personenbezogener Daten zu sorgen.“ Darüber hinaus haben dieselben Delegationen vorgeschlagen, Artikel 28 Absatz 2 zu ändern, indem am Anfang folgendes hinzugefügt wird: „Unbeschadet der Artikel 25 und 27 kann die ersuchte Vertragspartei.....“. Mehrere Delegationen haben sich gegen diese Vorschläge ausgesprochen. In dem Bemühen, diese strittige Frage zu regeln, wurde ein Vorschlag für eine zweigleisige Kompromisslösung vorgelegt, nach der 1) die bisher abgelehnten, derzeit in eckigen Klammer stehenden Präambelabsätze im Übereinkommen beibehalten werden (nicht jedoch der Teil in den inneren Klammern) und 2) die in Absatz 2 Buchstabe b enthaltene Beschränkung der Verwendung von Informationen nicht mehr optional, sondern obligatorisch ist. Dies würde zu folgender Neufassung des Absatzes 2 des Artikels 28 führen:

- (a) Die ersuchende Vertragspartei darf Informationen oder Unterlagen, die in Erledigung ihres Ersuchens zur Verfügung gestellt werden, ohne die vorherige Zustimmung der ersuchten Vertragspartei nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwenden.
- (b) Die ersuchte Vertragspartei kann die Überlassung von Informationen oder Unterlagen in Erledigung eines Ersuchens von der Bedingung abhängig machen, dass sie vertraulich behandelt werden, wenn das Rechtshilfeersuchen ohne diese Bedingung nicht erledigt werden könnte.

Entsprechend zu ändern wären in der ersten Zeile von Absatz 3 (Änderung von „einer“ zu „der“ und „2“ zu „2 Buchstabe b“) und in Absatz 4 (anstelle von „Jede Vertragspartei ... kann von der anderen Partei verlangen, dass sie im Zusammenhang mit dieser Bedingung ...“ würde es heißen: „Die ersuchte Vertragspartei kann von der ersuchenden Vertragspartei verlangen, dass sie im Zusammenhang mit der Bedingung in Absatz 2 oder 3 ...“). Eine Delegation war gegen diese Lösung. Folglich kam es in der Angelegenheit zu keiner Beschlussfassung.

<sup>10</sup> Von mehreren Delegationen wurde vorgeschlagen, in Bezug auf Buchstabe b „may“ durch „shall“ zu ersetzen. Eine Delegation schlug vor, in Bezug auf die beiden Buchstaben a und b „may“ durch „shall“ zu ersetzen.

(3) Kann die ersuchende Vertragspartei einer Bedingung nach Absatz 2 nicht entsprechen, so setzt sie die andere Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob die Informationen dennoch zur Verfügung gestellt werden. Nimmt die ersuchende Vertragspartei die Bedingung an, so ist sie daran gebunden.

(4) Jede Vertragspartei, die Informationen oder Unterlagen unter einer in Absatz 2 genannten Bedingung zur Verfügung stellt, kann von der anderen Vertragspartei verlangen, dass sie in Zusammenhang mit dieser Bedingung Angaben über die Verwendung dieser Informationen oder Unterlagen macht.

## **Abschnitt 2 – Besondere Bestimmungen**

### *Titel 1 – Rechtshilfe bei vorläufigen Maßnahmen*

#### **Artikel 29 – Beschleunigte Sicherung gespeicherter Computerdaten**

(1) Eine Vertragspartei kann eine andere Vertragspartei um Anordnung oder anderweitige Bewirkung der beschleunigten Sicherung von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der anderen Vertragspartei befindet, und derentwegen die ersuchende Vertragspartei beabsichtigt, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu stellen.

(2) Ein Ersuchen um Sicherung nach Absatz 1 enthält Angaben in Bezug auf

- a) die Behörde, die um die Sicherung ersucht;
- b) die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung;
- c) die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat;
- d) alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standortes des Computersystems;

- e) die Notwendigkeit der Sicherung und
- f) die Absicht der Vertragspartei, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der gespeicherten Computerdaten zu stellen.

(3) Nach Eingang des von einer anderen Vertragspartei gestellten Ersuchens trifft die ersuchte Vertragspartei alle geeigneten Maßnahmen zur beschleunigten Sicherung der bestimmten Daten in Übereinstimmung mit ihrem innerstaatlichen Recht. Für die Zwecke der Erledigung eines Ersuchens wird die beiderseitige Strafbarkeit als Voraussetzung für die Vornahme dieser Sicherung nicht verlangt.

(4) Eine Vertragspartei, welche die beiderseitige Strafbarkeit als Voraussetzung für die Erledigung eines Rechtshilfeersuchens um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten verlangt, kann sich in Bezug auf andere als die in Übereinstimmung mit den Artikeln 2 bis 11 festgelegten Straftaten das Recht vorbehalten, Ersuchen um Sicherung nach diesem Artikel abzulehnen, wenn sie Grund zu der Annahme hat, dass im Zeitpunkt der Weitergabe die Voraussetzung der beiderseitigen Strafbarkeit nicht erfüllt werden kann.

(5) Darüber hinaus kann ein Ersuchen um Sicherung nur abgelehnt werden, wenn

- a) das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als eine politische oder als eine mit einer solchen zusammenhängende Straftat angesehen wird, oder
- b) die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, die Souveränität, die Sicherheit, die öffentliche Ordnung (*ordre public*) oder andere wesentliche Interessen ihres Landes zu beeinträchtigen.

(6) Ist durch die Sicherung nach Ansicht der ersuchten Vertragspartei die künftige Verfügbarkeit der Daten nicht gewährleistet oder die Vertraulichkeit der Ermittlungen der ersuchenden Vertragspartei gefährdet oder in anderer Weise beeinträchtigt, so setzt sie die ersuchende Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.

(7) Jede Sicherung, die in Erledigung des in Absatz 1 bezeichneten Ersuchens vorgenommen wird, erfolgt für mindestens 60 Tage, damit die ersuchende Vertragspartei ein Er-

suchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten stellen kann. Nach Eingang eines solchen Ersuchens werden die Daten weiterhin gesichert, bis über das Ersuchen entschieden worden ist.

### **Artikel 30 – Beschleunigte Weitergabe gesicherter Verbindungsdaten**

(1) Stellt die ersuchte Vertragspartei bei der Erledigung eines Ersuchens nach Artikel 29 um Sicherung von Verbindungsdaten bezüglich einer bestimmten Kommunikation fest, dass ein Dienstanbieter in einem anderen Staat an der Übertragung dieser Kommunikation beteiligt war, so gibt die ersuchte Vertragspartei beschleunigt Verbindungsdaten in so ausreichender Menge an die ersuchende Vertragspartei weiter, dass dieser Dienstanbieter und der Weg, auf dem die Kommunikation übertragen wurde, festgestellt werden können.

(2) Von der Weitergabe von Verbindungsdaten nach Absatz 1 darf nur abgesehen werden, wenn

- a) das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als eine politische oder als eine mit einer solchen zusammenhängende Straftat angesehen wird, oder
- b) die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, die Souveränität, die Sicherheit, die öffentliche Ordnung (*ordre public*) oder andere wesentliche Interessen ihres Landes zu beeinträchtigen.

### *Titel 2 – Rechtshilfe in Bezug auf Ermittlungsbefugnisse*

### **Artikel 31 – Rechtshilfe beim Zugriff auf gespeicherte Computerdaten**

(1) Eine Vertragspartei kann eine andere Partei um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der ersuchten Vertragspartei befindet, einschließlich Daten, die nach Artikel 29 gesichert worden sind.

(2) Die ersuchte Vertragspartei erledigt das Ersuchen unter Anwendung der in Artikel 23 bezeichneten völkerrechtlichen Übereinkünfte, Vereinbarungen und Rechtsvorschriften und in Übereinstimmung mit den anderen einschlägigen Bestimmungen dieses Kapitels.

- (3) Das Ersuchen ist beschleunigt zu erledigen, wenn
- a) Gründe zu der Annahme bestehen, dass bei den einschlägigen Daten eine besondere Gefahr des Verlusts oder der Veränderung besteht oder
  - b) die in Absatz 2 bezeichneten Übereinkünfte, Vereinbarungen und Rechtsvorschriften eine beschleunigte Zusammenarbeit vorsehen.

### **Artikel 32 – Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind**

Eine Vertragspartei darf, ohne die Genehmigung einer anderen Vertragspartei einzuholen,

- a) auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden, oder
- b) auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.

### **Artikel 33 – Rechtshilfe bei der Echtzeit-Erhebung von Verbindungsdaten**

(1) Die Vertragsparteien leisten einander Rechtshilfe bei der Echtzeit-Erhebung von Verbindungsdaten im Zusammenhang mit bestimmten Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übertragen werden. Vorbehaltlich des Absatzes 2 unterliegt die Rechtshilfe den nach innerstaatlichem Recht vorgesehenen Bedingungen und Verfahren.

(2) Jede Vertragspartei leistet solche Rechtshilfe zumindest in Bezug auf Straftaten, bei denen die Echtzeit-Erhebung von Verbindungsdaten in einem gleichartigen inländischen Fall möglich wäre.

**Artikel 34 – Rechtshilfe beim Abfangen von Inhaltsdaten**

Die Vertragsparteien leisten einander Rechtshilfe bei der Echtzeit-Erhebung oder –Aufzeichnung von Inhaltsdaten bestimmter Kommunikationen, die mittels eines Computersystems übertragen werden, soweit dies nach ihren anwendbaren Verträgen und innerstaatlichen Rechtsvorschriften zulässig ist.

*Titel 3 – 24/7-Netzwerk***Artikel 35 – 24/7-Netzwerk**

(1) Jede Vertragspartei bestimmt eine Kontaktstelle, die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und Computerdaten oder für die Erhebung von in elektronischer Form vorliegenden Beweisen für eine Straftat unverzüglich für Unterstützung zu sorgen. Diese Unterstützung umfasst die Veranlassung oder, sofern dies nach innerstaatlichem Recht und innerstaatlicher Praxis zulässig ist, die unmittelbare Durchführung folgender Maßnahmen:

- (a) fachliche Beratung,
  - (b) Sicherung von Daten nach den Artikeln 29 und 30 und
  - (c) Erheben von Beweismaterial, Erteilen von Rechtsauskünfte und Ausfindigmachen verdächtiger Personen.
- (2) a) Die Kontaktstelle einer Vertragspartei verfügt über Möglichkeiten zur schnellen Kommunikation mit der Kontaktstelle einer anderen Vertragspartei.
- b) Ist die von einer Vertragspartei bestimmte Kontaktstelle nicht Teil der für die internationale Rechtshilfe oder Auslieferung zuständigen Behörde oder Behörden dieser Vertragspartei, so stellt die Kontaktstelle sicher, dass sie sich mit dieser Behörde oder diesen Behörden schnell abstimmen kann.
- (3) Jede Vertragspartei stellt sich, dass geschultes und entsprechend ausgestattetes Personal zur Verfügung steht, um die Arbeit des Netzwerks zu erleichtern.



## **KAPITEL IV - SCHLUSSBESTIMMUNGEN**

### **Artikel 36 - Unterzeichnung und Inkrafttreten**

- (1) Dieses Übereinkommen liegt für die Mitgliedstaaten des Europarats und für Nichtmitgliedstaaten, die sich an der Ausarbeitung des Übereinkommens beteiligt haben, zur Unterzeichnung auf.
- (2) Dieses Übereinkommen bedarf der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.
- (3) Dieses Übereinkommen tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Staaten einschließlich mindestens drei Mitgliedstaaten des Europarats nach den Absätzen 1 und 2 ihre Zustimmung ausgedrückt haben, durch das Übereinkommen gebunden zu sein.
- (4) Für jeden Unterzeichnerstaat, der später seine Zustimmung ausdrückt, durch das Übereinkommen gebunden zu sein, tritt es am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag erfolgt, an dem er nach den Absätzen 1 und 2 seine Zustimmung ausgedrückt hat, durch das Übereinkommen gebunden zu sein.

### **Artikel 37 - Beitritt zu dem Übereinkommen**

- (1) Nach Inkrafttreten dieses Übereinkommens kann das Ministerkomitee des Europarats nach Konsultation der Vertragsstaaten des Übereinkommens und mit deren einhelliger Zustimmung jeden Staat, der nicht Mitglied des Rates ist und der sich nicht an der Ausarbeitung des Übereinkommens beteiligt hat, einladen, dem Übereinkommen beizutreten. Der Beschluss ergeht mit der in Artikel 20 Buchstabe d der Satzung des Europarats vorgesehenen Mehrheit und mit einhelliger Zustimmung der Vertreter der Vertragsstaaten, die Anspruch auf einen Sitz im Ministerkomitee haben.
- (2) Für jeden Staat, der dem Übereinkommen nach Absatz 1 beiträgt, tritt das Übereinkommen am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach der Hinterlegung der Beitrittsurkunde beim Generalsekretär des Europarats folgt.

### **Artikel 38 - Räumlicher Geltungsbereich**

(1) Jeder Staat kann bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde einzelne oder mehrere Hoheitsgebiete bezeichnen, auf die dieses Übereinkommen Anwendung findet.

(2) Jeder Staat kann jederzeit danach durch eine an den Generalsekretär des Europarats gerichtete Erklärung die Anwendung dieses Übereinkommens auf jedes weitere in der Erklärung bezeichnete Hoheitsgebiet erstrecken. Das Übereinkommen tritt für dieses Hoheitsgebiet am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Erklärung beim Generalsekretär folgt.

(3) Jede nach den Absätzen 1 und 2 abgegebene Erklärung kann in Bezug auf jedes darin bezeichnete Hoheitsgebiet durch eine an den Generalsekretär des Europarats gerichtete Notifikation zurückgenommen werden. Die Rücknahme wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

### **Artikel 39 – Wirkungen des Übereinkommens**

(1) Zweck dieses Übereinkommens ist es, die zwischen den Vertragsparteien bestehenden zwei- oder mehrseitigen Übereinkünfte oder Vereinbarungen zu ergänzen einschließlich der Bestimmungen

des am 13. Dezember 1957 in Straßburg zur Unterzeichnung aufgelegten Europäischen Auslieferungsübereinkommens [ETS Nr. 24],

des am 20. April 1959 in Straßburg zur Unterzeichnung aufgelegten Europäischen Übereinkommens über die Rechtshilfe in Strafsachen [ETS Nr. 30],

des am 17. März 1978 in Straßburg zur Unterzeichnung aufgelegten Zusatzprotokolls zum Europäischen Übereinkommen über die Rechtshilfe in Strafsachen [ETS Nr. 99].

(2) Haben zwei oder mehr Vertragsparteien bereits ein Abkommen oder einen Vertrag über Fragen geschlossen, die in diesem Übereinkommen geregelt sind, oder haben sie ihre Beziehungen in diesen Fragen anderweitig geregelt oder sollten sie dies in Zukunft tun, so sind sie auch berechtigt, das Abkommen oder den Vertrag oder die entsprechenden Rege-

lungen anzuwenden. Regeln Vertragsparteien ihre Beziehungen in den in diesem Übereinkommen geregelten Fragen jedoch anders als hierin vorgesehen, so tun sie dies in einer Weise, die zu den Zielen und Grundsätzen des Übereinkommens nicht in Widerspruch steht.

(3) Dieses Übereinkommen lässt andere Rechte, Beschränkungen, Pflichten und Verantwortlichkeiten einer Vertragspartei unberührt.

#### **Artikel 40– Erklärungen**

(1) Jeder Staat kann durch eine an den Generalsekretär des Europarats gerichtete schriftliche Notifikation bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde erklären, dass er von der Möglichkeit Gebrauch macht, gemäß Artikel 2, Artikel 3, Artikel 6 Absatz 1 Buchstabe b, Artikel 7, Artikel 9 Absatz 3 und Artikel 27 Absatz 9 Buchstabe e zusätzliche Merkmale als Voraussetzung vorzusehen.

#### **[Artikel 41 - Bundesstaatsklausel**

Ein Bundesstaat kann dem Generalsekretär notifizieren, dass er Verpflichtungen aus diesem Übereinkommen nur insoweit übernimmt, als sie mit den Grundprinzipien vereinbar sind, welche die Beziehungen zwischen seiner Zentralregierung und seinen Gliedstaaten oder anderen gleichartigen Gebietseinheiten regeln. Bei der Abgabe einer Erklärung legt ein Bundesstaat eine Darstellung der Art seiner föderalen Ordnung und der Folgen seiner föderalen Struktur für die Durchführung des Übereinkommens vor]<sup>11</sup>.

#### **Artikel 42 - Vorbehalte**

(1) Jeder Staat kann durch eine an den Generalsekretär des Europarats gerichtete schriftliche Notifikation bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde erklären, dass er von dem oder den in Artikel 4 Absatz 2, Artikel 6 Absatz 3, Artikel 9 Absatz 4, Artikel 10 Absatz 3, Artikel 11 Absatz 3, Artikel 14 Absatz 3, Artikel 22 Absatz 2 und Artikel 29 Absatz 4 vorgesehenen Vorbehalten Gebrauch macht. Weitere Vorbehalte sind nicht zulässig.

---

<sup>11</sup> Diese Bestimmung bleibt noch in eckigen Klammern, weil eine Delegation nicht in der Lage war, einer solchen Bestimmung im Übereinkommen zuzustimmen, und ihren Vorbehalt dagegen aufrechterhalten hat.

### **Artikel 43 – Status und Rücknahme von Vorbehalten**

(1) Eine Vertragspartei, die einen Vorbehalt nach Artikel 42 angebracht hat, kann ihn durch eine an den Generalsekretär gerichtete Notifikation ganz oder teilweise zurücknehmen. Diese Rücknahme wird mit dem Eingang der Notifikation beim Generalsekretär wirksam. Wird in der Notifikation erklärt, dass die Rücknahme eines Vorbehalts zu einem in der Notifikation angegebenen Zeitpunkt wirksam werden soll und liegt dieser Zeitpunkt später als der Zeitpunkt, an dem die Notifikation beim Generalsekretär eingeht, so wird die Rücknahme zu diesem späteren Zeitpunkt wirksam.

(2) Eine Vertragspartei, die einen Vorbehalt nach Artikel 42 angebracht hat, nimmt diesen Vorbehalt ganz oder teilweise zurück, sobald die Umstände dies erlauben.

(3) Der Generalsekretär kann sich in regelmäßigen Abständen bei den Vertragsparteien, die einen oder mehrere Vorbehalte nach Artikel 42 angebracht haben, nach den Aussichten für eine Rücknahme dieses Vorbehalts oder dieser Vorbehalte erkundigen.

### **Artikel 44 - Änderungen**

(1) Jede Vertragspartei kann Änderungen dieses Übereinkommens vorschlagen; der Generalsekretär des Europarats übermittelt jeden Vorschlag den Mitgliedstaaten des Europarates, den Nichtmitgliedstaaten, die sich an der Ausarbeitung dieses Übereinkommens beteiligt haben, sowie jedem Staat, der nach Artikel 37 diesem Übereinkommen beigetreten oder zum Beitritt eingeladen worden ist.

(2) Jede von einer Vertragspartei vorgeschlagene Änderung wird dem Europäischen Ausschuss für Strafrechtsfragen (CDPC) übermittelt; dieser unterbreitet dem Ministerkomitee seine Stellungnahme zu dem Änderungsvorschlag.

(3) Das Ministerkomitee prüft den Änderungsvorschlag und die vom Europäischen Ausschuss für Strafrechtsfragen (CDPC) unterbreitete Stellungnahme und kann nach Konsultation der Nichtmitgliedstaaten, die Vertragsparteien des Übereinkommens sind, die Änderung annehmen.

(4) Der Wortlaut jeder vom Ministerkomitee nach Absatz 3 angenommenen Änderung wird den Vertragsparteien zur Annahme übermittelt.

(5) Jede nach Absatz 3 angenommene Änderung tritt am dreißigsten Tag nach dem Tag in Kraft, an dem alle Vertragsparteien dem Generalsekretär mitgeteilt haben, dass sie sie angenommen haben.

#### **Artikel 45 - Beilegung von Streitigkeiten**

(1) Der Europäische Ausschuss für Strafrechtsfragen (CDPC) wird über die Auslegung und Anwendung dieses Übereinkommens auf dem laufenden gehalten.

(2) Im Fall einer Streitigkeit zwischen den Vertragsparteien über die Auslegung oder Anwendung dieses Übereinkommens bemühen sich die Vertragsparteien, die Streitigkeit durch Verhandlungen oder andere friedliche Mittel ihrer Wahl beizulegen, einschließlich der Befassung des Europäischen Ausschusses für Strafrechtsfragen (CDPC), eines Schiedsgerichts, das für die Streitparteien bindende Entscheidungen fällt, oder des Internationalen Gerichtshofs, je nach Vereinbarung der betroffenen Vertragsparteien.

#### **Artikel 46 – Konsultationen der Vertragsparteien**

(1) Die Vertragsparteien konsultieren einander bei Bedarf in regelmäßigen Abständen im Hinblick auf die Förderung:

- a) der wirksamen Anwendung und Durchsetzung dieses Übereinkommens;
- b) des Informationsaustauschs über wichtige rechtliche, politische und technische Entwicklungen in Bezug auf die Datennetzkriminalität und die Erhebung von in elektronischer Form vorliegenden Beweisen;
- c) der Beratung über eine mögliche Ergänzung oder Änderung des Übereinkommens.

(2) Der Europäische Ausschuss für Strafrechtsfragen (CDPC) wird regelmäßig von dem Ergebnis der in Absatz 1 bezeichneten Konsultationen unterrichtet.

(3) Der Europäische Ausschuss für Strafrechtsfragen (CDPC) fördert gegebenenfalls die in Absatz 1 bezeichneten Konsultationen und trifft die erforderlichen Maßnahmen, um die Vertragsparteien bei ihren Bemühungen um Ergänzung oder Änderung des Übereinkommens zu unterstützen. Spätestens drei Jahre nach Inkrafttreten dieses Übereinkommens führt der Europäische Ausschuss für Strafrechtsfragen (CDPC) in Zusammenarbeit mit den

Vertragsparteien eine Überprüfung aller Bestimmungen des Übereinkommens durch und empfiehlt gegebenenfalls geeignete Änderungen.

(4) Kosten, die mit der Durchführung des Absatzes 1 entstehen, werden von den Vertragsparteien in der von ihnen zu bestimmenden Weise getragen, soweit sie nicht vom Europarat übernommen werden.

(5) Die Vertragsparteien werden bei der Wahrnehmung ihrer Aufgaben nach diesem Artikel vom Sekretariat des Europarats unterstützt.

### **Artikel 47 - Kündigung**

(1) Jede Vertragspartei kann dieses Übereinkommen jederzeit durch eine an den Generalsekretär des Europarats gerichtete Notifikation kündigen.

(2) Die Kündigung wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

### **Artikel 48 - Notifikation**

Der Generalsekretär des Europarats notifiziert den Mitgliedstaaten des Europarats, den Nichtmitgliedstaaten, die sich an der Ausarbeitung dieses Übereinkommens beteiligt haben, sowie jedem Staat, der diesem Übereinkommen beigetreten oder zum Beitritt eingeladen worden ist,

- a) jede Unterzeichnung;
- b) jede Hinterlegung einer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde;
- c) jeden Zeitpunkt des Inkrafttretens dieses Übereinkommens nach den Artikeln 36 und 37;
- d) jede Erklärung nach [den] Artikel[n] 40 [und 41] oder jeden Vorbehalt nach Artikel 42;
- e) jede andere Handlung, Notifikation oder Mitteilung im Zusammenhang mit diesem Übereinkommen.

Zu Urkund dessen haben die hierzu gehörig befugten Unterzeichneten dieses Übereinkommen unterschrieben.

Geschehen zu Straßburg am ..... 2001 in englischer und französischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist, in einer Urschrift, die im Archiv des Europarats hinterlegt wird. Der Generalsekretär des Europarats übermittelt allen Mitgliedstaaten des Europarats, den Nichtmitgliedstaaten, die sich an der Ausarbeitung des Übereinkommens beteiligt haben, sowie allen zum Beitritt zu diesem Übereinkommen eingeladenen Staaten beglaubigte Abschriften.